EAI/Springer Innovations in Communication and Computing

Shalli Rani
R. Maheswar
G. R. Kanagachidambaresan
P. Jayarajan *Editors*

Integration of WSN and IoT for Smart Cities

EAI
RESEARCH MEETS INNOVATION

Springer

EAI/Springer Innovations in Communication and Computing

Series Editor

Imrich Chlamtac, European Alliance for Innovation, Ghent, Belgium

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, life style and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process.

The range of topics, focusing primarily on communications and computing engineering include, but are not limited to, wireless networks; mobile communication; design and learning; gaming; interaction; e-health and pervasive healthcare; energy management; smart grids; internet of things; cognitive radio networks; computation; cloud computing; ubiquitous connectivity, and in mode general smart living, smart cities, Internet of Things and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintain Springer's and EAI's high standards of academic excellence. The audience for the books consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity include information and communication specialists, security experts, economists, urban planners, doctors, and in general representatives in all those walks of life affected ad contributing to the information revolution.

About EAI

EAI is a grassroots member organization initiated through cooperation between businesses, public, private and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions, provide a free research and innovation platform.

Through its open free membership model EAI promotes a new research and innovation culture based on collaboration, connectivity and recognition of excellence by community.

More information about this series at http://www.springer.com/series/15427

Shalli Rani • R. Maheswar
G. R. Kanagachidambaresan • P. Jayarajan
Editors

Integration of WSN and IoT for Smart Cities

Springer

EAI
RESEARCH MEETS INNOVATION

Editors
Shalli Rani
Chitkara University Institute of Engineering and Technology
Chitkara University
Rajpura, Punjab, India

R. Maheswar
School of Electrical & Electronics Engineering (SEEE)
VIT Bhopal University
Bhopal, Madhya Pradesh, India

G. R. Kanagachidambaresan
Department of CSE
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Chennai, Tamil Nadu, India

P. Jayarajan
Department of ECE
Sri Krishna College of Technology
Coimbatore, Tamil Nadu, India

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-030-38515-6 ISBN 978-3-030-38516-3 (eBook)
https://doi.org/10.1007/978-3-030-38516-3

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Wireless sensor networks (WSNs) cover an extensive range of applications in various areas, including control networks, health care, smart living scenarios, smart industries, real-time production monitoring and many other domains. Internet of Things (IoT) has ensured smart human being life, through communications among objects, people and devices. Therefore, transfer of Internet from things (termed as people, objects and devices) towards an Internet of Things (IoT) and incorporation of WSNs in to IoT enable sensor nodes join Internet dynamically in order to cooperate and accomplish responsibilities. However, when WSNs become a part of the Internet, there is a need to carefully investigate and analyse the issues involved with WSN-IoT integration.

IOT can be defined in various ways. It involves many features of life such as connected homes, roads, devices and cities which can trace an individual's behaviour. It is expected that around 1 trillion Internet-connected devices will be accessible with mobile phones as the only one means of the applications connecting all of associated things. It is the IoT only which made billion objects to interact and communicate all over public and private worldwide networks. Around 12.5 billion things were connected in 2010-2011. The IoT approach has attracted many researchers due to its huge future-predicted impact on the daily life of people and society. Remote communication with the help of new mobile applications is made possible with the help of tiny nodes known as sensors. Therefore, WSNs have become the crucial subpart of the IoT platform. When things are connected in a network, they work together as the one scenario and provide service as a whole and not as a collection of independently working devices. This is useful for various real-world applications and services. For example, this approach would be useful for smart homes, smart transportation, smart healthcare, etc. IoT is useful for the needy and disabled people because it serves and supports many human activities at a huge scale.

Machine learning techniques, block chain services, cloud services, security paradigms, named data networking, software-defined networks have boost up the IoT technology at a large platform and have made it more sustainable. WSNs are well suitable for long-standing environmental data retrieval for IoT illustration.

The editors would like to offer an overview of recent developments in WSN and IoT integration. It will lead to introduction of various approaches like protocols, smart city scenarios, black chain technology, SDN, NDN, etc. Current research on various approaches and subareas is given to help the researchers to find out the classification for their new research areas. Beginners can make themselves aware about the current trends by the overview of the diverse approaches. It is beneficial for the students who are involved in technical studies. The aim of this book is to present some of the most relevant results achieved by applying technical approaches to the research on WSN-IOT integration. The unique aspect of the book is to present measurements, experiences and lessons obtained by reviewing recent technologies and areas of WSN and IoT.

Rajpura, Punjab, India — Shalli Rani
Bhopal, Madhya Pradesh, India — R. Maheswar
Chennai, Tamil Nadu, India — G. R. Kanagachidambaresan
Coimbatore, Tamil Nadu, India — P. Jayarajan

Acknowledgement

First and foremost, I would like to thank my husband Shvet Jain for standing beside me throughout my research career so far and editing this book. He has been my motivation for continuing to improve my knowledge and move forward in my career. He is my lifetime achievement, and I dedicate this book of mine to him. Moreover, without the prayers and best wishes of my parents, my sister and my son, all of my achievements so far and forever would never be possible.

Here, I am also thankful to my co-editors who really helped me in every aspect in the preparation of this book. Their prompt response and care to the literature and contribution is remarkable and sensational. They are great and responsible researchers indeed.

I would also like to thank the Springer staff and editors, who actually helped a lot, and without their quick and efficient efforts, it was not possible to get our book published.

Last but not least, my gratitude is due to my inspiration Dr. Archana Mantri, Pro-VC, Chitkara University, Punjab for her trust in me and for making me confident that I can put efforts to get success in each and every field.

Contents

Software-Defined Networking Framework Securing Internet of Things

Himanshi Babbar and Shalli Rani

1 Introduction to Internet of Things (IoT)

The Internet plays a very essential role in the scenario of the latest wireless telecommunications. The IoT was first coined by Kevin Ashton in the year 1998 and has been pondered as the interaction and collaboration of smart objects (things) [1]. The influence of IoT leads to the novel context of the forthcoming applications and services. There are multiple objects that serve as the basic building blocks, including sensors, mobile phones, radio frequency identification (RFID) tags, etc., which are the various key components of IoT. Therefore, to fulfill the basic necessities of users, the smart objects are able to sense, gather, and transmit the data. Internet of Things is defined as follows: it "permits the people and things to be interconnected anytime, anywhere, anyplace, anything and anytime by using any pathway or any service" [2]. The main goal of the IoT, which is shown in Fig. 1, is to generate a preferable world for the human beings in which the objects surrounding our environment know what we like and what we want, etc.

IoT is broadly classified into three layers:

- *Perception Layer:* The role of this layer is to sense and gather the data from the real life and physical world. Due to its functionality, it has become the core layer of the IoT [3]. The main key components of this layer are RFID devices, GPS, and camera-enabled devices.
- *Network Layer:* The responsibility of this layer is to interchange information and transfer data.
- *Application Layer:* This layer provides the human-to-machine interface. Nowadays, machine-to-machine (M2M) interface is the important and frequently used application form of the IoT [4].

H. Babbar · S. Rani (✉)
Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India
e-mail: himanshi.babbar@chitkara.edu.in; shalli.rani@chitkara.edu.in

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_1

Fig. 1 Internet of Things

The value that is added into the business using IoT is generated by the information that has been gathered by the devices of IoT which have gone through various five phases of IoT lifecycle:

1. *Create Phase*: in this phase, devices or sensors gather the information from the physical environment surrounding us. The data that is generated from smart devices can be used to produce understanding that can help the businesses, partners, etc.
2. *Communicate Phase*: in this phase, the events that are generated are transmitted through the network in the appropriate destination.
3. *Aggregate Phase*: data that was gathered is aggregated by the devices itself.
4. *Analyze Phase*: wherein upon the further experienced analytics, the data aggregated is needed to produce the basic patterns and hence optimize the processes.
5. *Act Phase*: where appropriate actions are being performed on the basis of information that is being generated [5].

1.1 Bits of Software-Defined Networking

With the increasing services of cloud have undertaken the researchers to think again on today's architecture of the network. The equipment used in today's network are load balancers, firewalls, Intrusion Detection System, etc.; these devices and network appliances are hard to manage and difficult to reconfigure and reinstall, so in the upcoming years, Software-Defined Networking (SDN) would be the recent and hot topic. In traditional networks, many devices of the network have routers and switches that are comprised of forwarding plane, control plane, and application plane, and these are embedded into the network device [6]. In SDN, control plane (how the packets are forwarded and where to forward the packets) and data plane (handles the packet with respect to the rules that are defined in the control plane) are decoupled from each other; by decoupling it has changed the resources of the network into programmable, automation and network control to make it more scalable and flexible enough [7].

In traditional networks, the approach followed had certain boundaries, so the solution for this is SDN. SDN has *some basic features*: (1) In the previous few years, SDN had attracted many academia and industries and had many pros due to the network virtualization. (2) The main significant characteristic of SDN is the division of control plane and data plane, as one plane handles single network components that can manage and control the different elements of the data plane [8]. (3) So, in this case, SDN furnishes the solutions to all the issues that are in the traditional network which comprises of the separation of the control plane for each device of the network. There are various *components of SDN*: OpenFlow protocol (interface between control plane and OpenFlow switch), Open vSwitch (OpenFlow-based switches), controllers in Software-Defined Networking (POX, Ryu, OpenDaylight, Floodlight), and applications of Software-Defined Networking (hub, switch, routers, firewall, and load balancer), which is explained in Fig. 2.

Software-Defined Networking (SDN) emerges as one of the noteworthy forms of networking concepts. It helps in lubricating a convenient and efficient flow of network control that facilitates the cost of investment in the meantime which is availing the huge number of users [9]. SDN has transposed the way of managing the network, and it is defined by two different tendencies: (1) SDN disassociates the control level (controllers) from the data level (forwarding plane). (2) Decoupling makes the control level programmable by the end users. In conventional networks, it is hardly possible to separate the control level from the data level. Therefore, the end users had to be dependent on the merchants for the configurations of a software network and its users. In this traditional network, data plane informs your data where it is required to go and control plane is situated inside a switch or router; in this, one device could take the decision of progressing the packet, and it also is in charge of maintaining the routing table information and required to reserve the data, and SDN was refined to design, build, and manage the networks that decouple the network layer and forwarding layer becoming directly programmable by the source automation tools [6].

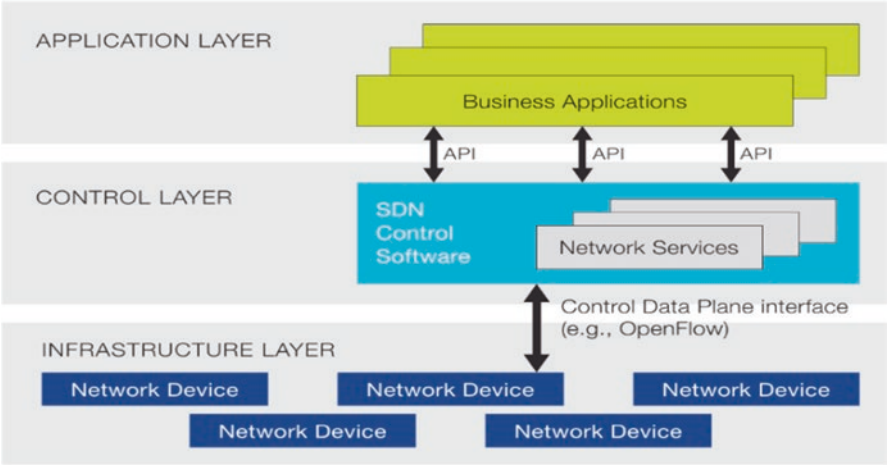


Fig. 2 Software-Defined Networking

1.2 Role of Software-Defined Networking in the Internet of Things

Nowadays SDN can be utilized as the overlay for the adoption of IoT into the real world. Any of the objects in IoT can be interconnected with another object with respect to the network cable of SDN. So, each device in the network has the IoT agent that communicates with the IoT controller as shown in Fig. 3 [10].

IoT Agent: In order to gain the objective of users, IoT agent has to be supervised to detect, accumulate, and break down the information from the physical environment. Every IoT agent needs to be enrolled with the controller of IoT having the details that incorporate the address and item's identifier and collaborate with the network protocol and the hidden system.

IoT Controller: Important choices will be taken by the agents of IoT on the basis of the data or information provided to them. These choices are reflected in the dedicated physical network via the controller of SDN. Controller of IoT, on recieving the request of connection from the agent of IoT will develop the forwarding rules on the basis of networking protocols; they utilize and collaborate these guidelines to the controller of SDN. Once the goal address is received by the controller of IoT, it is required to seek it in the network. This turns out to be simple as the agents of IoT will be registered with the controllers of IoT and they necessitate their respective location or identifier [9].

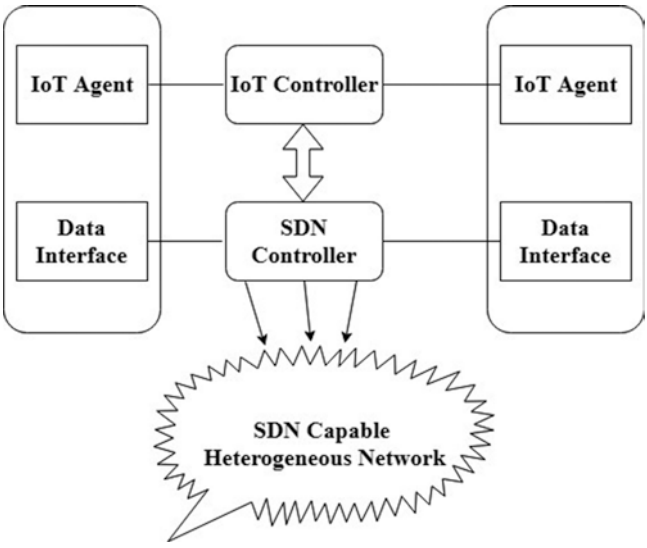


Fig. 3 SDN-based IoT architecture

SDN Controller: This controller creates the path of the network that interconnects both the objects by running an algorithm based on routing with the topology information that is produced from both IoT and levels of SDN.

1.3 Integration of SDN and IoT

IoT and SDN are the two prominent technologies that are rising toward the growth and development of society. The main goal of IoT is to interconnect the objects to the Internet, whereas SDN provides the uniformity for the management of the network by disassociating the control plane from the data plane [2]. The devices connected to the Internet are in billions, and the network management is a difficult task for the huge distribution network.

Since we all know that scalability and flexibility are the most common challenges that service providers are facing, various researchers have been exploring the various alternative solutions that include SDN which increases the bandwidth of IoTs. The most important feature of SDN is the decoupling of the control plane from the forwarding plane. In conventional networks, all the routers in the network devices apply to the high-level algorithms [11]. In SDN, the decision process is being controlled and managed by the controller of SDN, and forwarding of data is being managed by the switches. Simplification of devices of the network and central management are the two most prominent features of SDN. Since we know a massive number of devices of the network that exists, we can take advantage of the reduction in their costs. In conventional networks, each device of the network can handle all the updates by itself, but in SDN, they are managed centrally. So, network devices meet the static requirements of the network because of the environment of IoT is flexible enough as conventional networks are unable to meet the requirements of the user. Integration of SDN clarifies the simplification analysis and the decision-making processes. SDN facilitates debugging of the tools that can be used in the environment of IoT so as to increase the ability of the network in gathering the data for the purpose of debugging [2]. Therefore, the facilities availed for the integration of SDN-IoT have been diagnosed in various domains that include smart transportation, smart grid, etc. Integration of SDN and IoT provides the security in IoT because many mechanisms are being easily implemented by exploiting the features of SDN.

2 Threats and Vulnerabilities in Internet of Things

There are various challenges in IoT, and they are both technical and social to overcome the adoption of IoT explained in Fig. 4.

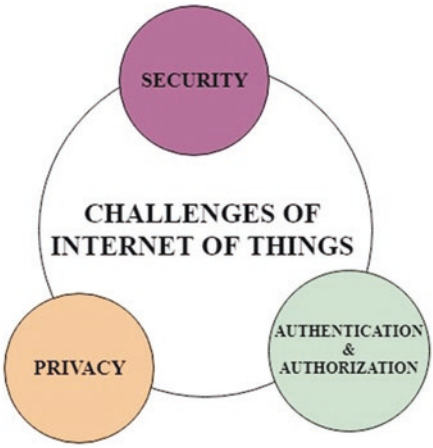


Fig. 4 Challenges of the Internet of Things

2.1 Security

Gadgets in IoT are wireless and are situated near public places. These challenges in IoT are separated into technological and security challenges [1]. The creative challenges emerge due to the heterogeneous and universal nature of IoT gadgets, while the security troubles are related to the norms and functionalities that should be maintained to accomplish a protected framework. There are *various parts to ensure security,* including:

- The item running on all IoT devices ought to be endorsed.
- When an IoT device is turned on, it ought to firstly confirm itself into the system before transmitting information [12].
- Since the IoT devices have obliged estimation of memory capacities, firewalling is significant in IoT framework to channel bundles facilitated to the devices.
- The updates and fixes on the device should be presented with the end goal that additional information exchange limit isn't consumed.

2.2 Privacy

We explained the significance of safeguarding protection in IoT. In this, we will delineate the difficulties of IoT arrangement on safeguarding protection. The difficulties can be isolated into two classifications: *information accumulation strategy* and *information anonymization.*

- *Information Accumulation Strategy:* It defines the policy in the middle of gathering the information where it imposes the type of data that is gathered and the access control of a thing to the data [2]. Using the information gathering policy, the amount of information gathered is bounded in the information accumulation

phase. Since we know that gathering and storing of personal information is secured, privacy preservation can be ensured.
- *Information Anonymization:* For ensuring the information anonymization, the most desirable techniques are the protection of cryptographic and concealment of data relations. By the diversity of the things, multiple unique cryptographic schemes may be taken into consideration.

2.3 Authentication and Authorization

Authorization is defined as the procedure that determines whether the entity or user can access the resources. For example, reading or writing of data, executing the programs, and controlling the actuators. It includes rejecting or revoking access, especially for someone or something that is malicious [13].

Authentication is defined as the procedure that recognizes the entity and is necessary for authorization. In general, authorization is not possible without authentication. How might we concede or deny access to a person or thing that we don't think about?

Each and every object in the IoT must be able to undoubtedly recognize and authenticate these objects. The undergoing process may become very challenging due to the nature of IoT and various number of entities being involved; aside from that, many of the times, objects may require to communicate with one another for the first time, and because of all of these, a mechanism was developed to mutually authenticate the entities in each and every interaction in the IoT [14].

3 Security Challenges of Software-Defined Networking

There are multiple attacks that were conducted in a very much complex way. As defined in the structure of SDN, there are challenges in security that were concluded in *two* different aspects:

3.1 Challenges Based on Hardware

Controllers are considered as the primary source for the attackers as the controller is said to be a centralized gadget, which acts as the brain of the network. There are numerous conventional approaches, and behavior of various latest attacks is efficient and effective in making the controller disabled. For example, Classic DDoS assault can choose the controller as the objective [15]. Aggressors can generate an enormous number of fraud packets and transmit them to the switches simultaneously. All the fraud packets are considered as new in switches which would later

generate the least or equal amount of the fraud transmission of requests to the controller. So, in this way, computational assets of the controller will be drained in not much stipulated time.

The switch has also been considered vulnerable in the mind of attackers. As switches have very least execution in the hardware resources, aggressors can initially assault the channel of correspondence between the controllers and switches; therefore, according to the OpenFlow protocol, the switches would be likely altered into the independent mode or the fail-secure mode [16]. This would definitely be harming the performance of the network.

3.2 Challenges Based on Protocol

There is a huge growth in the development of OpenFlow, still various aspects are there to be undertaken. The upcoming version of OpenFlow instead of the first edition creates the mutual authentication optional between the controllers and switches. So, the OpenFlow protocol may also be undertaken to induce the challenges of security at the system level [17]. Controller deals with the various modules for the effective management of network and monitoring.

4 Security Attacks in Internet of Things

As talked in the past section, IoT is classified into three layers: perception layer, network layer, and application layer. Perception layer is comprised of different types of sensor devices that include RFID, barcodes, etc. The main motive of this layer is to acquire the data from the physical environment by the use of sensors and then transmit it to the network layer. The main aim of the network layer is to send the data that is gathered from the previous layer to any specified information processing system through the Internet [4]. IoT security is one of the biggest challenges due to the diversification, complexity, etc. On the basis of these vulnerabilities, we have categorized the attack into four different categories:

- Physical attack
- Network attack
- Software attack
- Encryption attack

From each of the above-listed attacks in Fig. 5, there would be one most dangerous attack in each from all the attacks available. From the *Physical Attack*, Malicious Node Injection Attack has been considered as the most dangerous attack. This attack is transforming the data and inhibits all the services. *Network Attack*, Sinkhole Attack has been taken as the most threatening attack. In this, the attacker can install

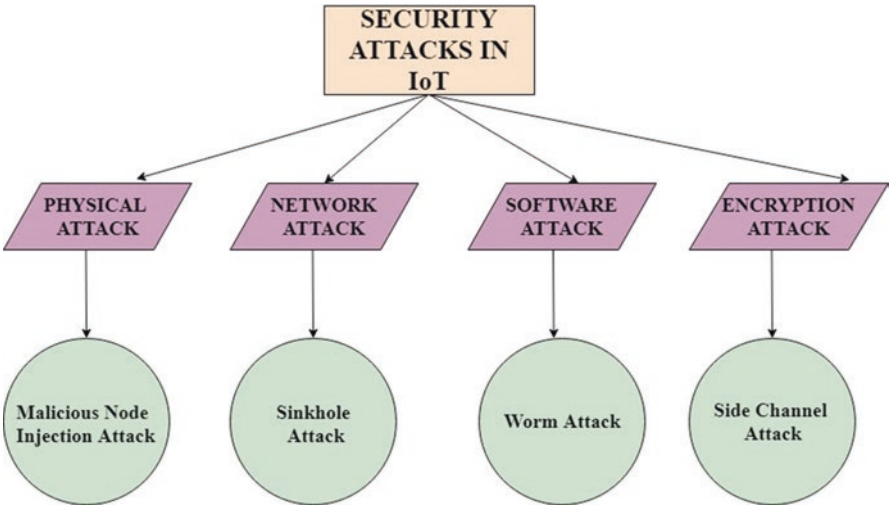


Fig. 5 Attacks in the Internet of Things

threats such as modifying and dropping the packets. *Software Attack,* Worm Attack is a risky attack. This attack is the riskiest form of attack on the Internet nowadays. It is the self-owned program which destroys the PC by the use of security holes in the networking hardware and software. It can even erase all the files from the system and even thieve all the data like passwords; passwords can be changed without informing the user. *Encryption Attack,* Side Channel Attack is the most unsafe attack and not easy to handle. It is tough to perceive as an attacker uses the side channel information to perform this attack.

Description of the attacks is given below:

- *Malicious Node Injection Attack*: This assault is also known as the man in the middle assault. The adversary can create a new malicious node among the two or more than two nodes. The attacker can set up a latest malicious node between the sender and receiver nodes by using this mechanism; it inhibits all the present data from one end to the other in the system of IoT. In this attack, assailants immunize a new malicious node among two or more nodes physically. It later changes the data that crosses the phony information to all the other nodes. So, the attacker used several nodes to execute the malicious node injection attack [10]. The enemy firstly adds the replica of the node B and then later on adds all the other malicious nodes. Both of these nodes conjointly perform the attack. Thus, the collision is being arisen at the victim node. As the attacked node is unable to transmit or receive any packet, to forestall this assault, we have used the monitoring verification (MOVE) scheme. Now they can check the node monitoring conclusion and identify correctly any malicious behavior. According to the acknowledgment, the node that was checked will assume the liability of whether the node is malicious or not.

- *Sink Hole Attack*: This type of attack tempts all the traffic from the wireless sensor network nodes and produces the metaphorical nodes. So, this attack inhibits secret information and also disproves the network service by relinquishing all the packets rather than passing them to their desired destination. In this, the enemy adjusts the node that lies in the network and executes the attack by the use of this node [10]. The adjusted node transmits the fraud information of routing to its neighboring nodes that have the least distance path to the base station and then inhibits the traffic. It then modifies the data and later drops the packets.
- *Worm Attack*: In this type of attack, the attacker has a great impact on the IoT system by injecting the malicious software there in the system which results in different outcomes. So, this type of attack affects the system by denying its services, modifying the information, and getting access to all personal information. The enemy can degenerate the system by utilizing the malicious code. In this way, these codes are dissipated through email connections, downloading all the documents from the web [4]. The worm, therefore, has the ability to reproduce itself without the utilization of human intervention. We can now utilize the indicator of the worm, IDS, etc. so as to distinguish the infection.
- *Side Channel Attack*: In this, the attacker uses the side channel information that is changed by the devices that are in encrypted form. Information is neither in the plaintext nor ciphertext form. Side channel attack stores the information about the time required to execute this operation; then attackers reuse this information to detect the encryption key. By this way, the adversaries get access to the hacked data by the use of some technique or mechanism known as electromagnetic analysis and power.

5 Software-Defined Networking-Based Ad hoc Architecture

OpenDayLight Controller is being set up as default on the equal interaction. Complete access to the switch is permitted, and controllers have similar rules. On the basis of the approach followed, we have highlighted the "Multiple SDN Controller Architecture for the Ad-Hoc Networks" [14]. It comprises of SDN-based architecture as mentioned in Fig. 6.

- Legacy interfaces: the physical layer
- Programmable layer: virtual switch compatible with SDN and controller of SDN
- Operating system and their individual applications: the layer of operating system

The proposed ad hoc architecture of SDN as given in Fig. 6 consists of the legacy interfaces which are interconnected to the virtual switch and is dominated by the controller of SDN. We all know that the controllers of SDN in every node are contrived in the equal interactions. In this case, they will not have the requirements of being interconnected through them. Simultaneously the controller of SDN can expand the security and availability among each of the nodes [18]. One of the main accomplishments of this architecture is its similarity with the SDN legacy network.

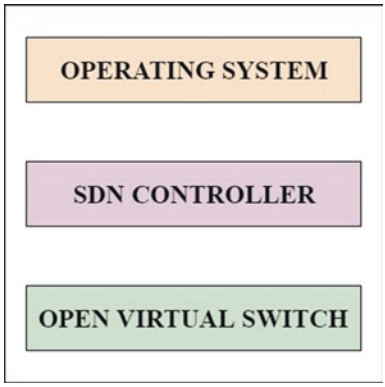


Fig. 6 SDN-based architecture

As every node in the ad hoc system has an embedded SDN-compatible virtual switch and the controller of SDN, we can essentially associate the ad hoc system to the legacy network so as to develop the domain of SDN.

In the ongoing work done so far, we have discovered that the domain of SDN is regularly constrained to the system with the infrastructure. Ad hoc users have to incorporate utilizing all the other nodes in this configuration that are associated legitimately to the area of SDN. In our proposed design, the area of SDN is upgraded so as to incorporate all the other devices of Ad-Hoc Architecture. The solution emerged from the architecture of Ad-Hoc, as shown in Fig. 7, which involves arranging the OpenFlow virtual switch in every ad hoc node. This sort of arrangement empowers the ad hoc nodes to interconnect to the network as a feature of the area of SDN [14].

6 Conclusion

IoT has emerged as one of the important topics of research. It facilitates the interconnection of various objects and sensors to integrate with one another without the need for human intervention. We have contributed to the review of the IoT security threats and vulnerabilities. In this chapter, we have proposed an SDN-based ad hoc architecture with multiple controllers. Moreover, our proposed concept can be used in the context of the ad hoc network and IoT. This is the foremost step toward the building of a secured framework of SDN based on the environment of IoT. We have made an attempt to focus on the various issues and attacks of security in the field of IoT and SDN.

Key Points to Remember

1. The Internet of Things was first coined by Kevin Ashton in the year 1998 and has been pondered as the interaction and collaboration of smart objects (things).
2. The main goal of the Internet of Things is to generate a better world for the human beings in which the objects surrounding our environment know what we like and what we want, etc.

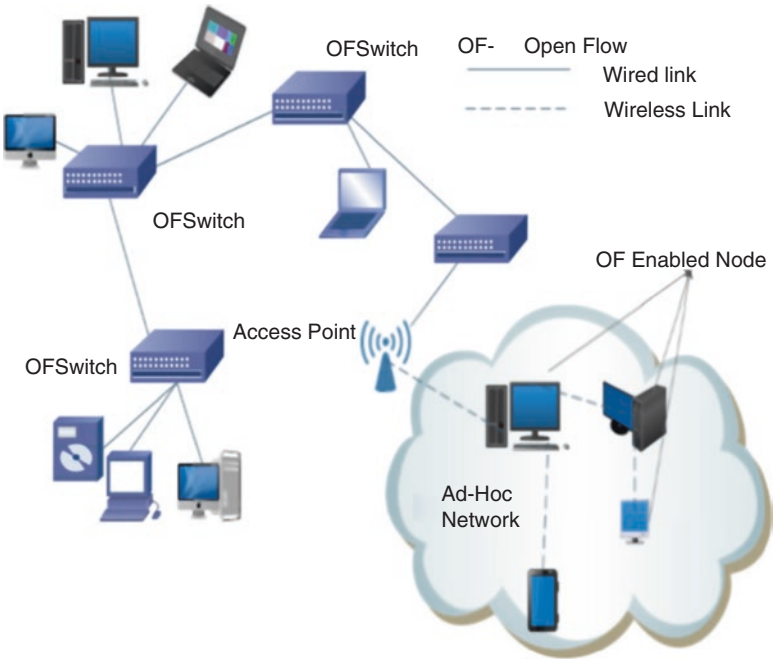


Fig. 7 SDN-based ad hoc architecture

3. In traditional networks, many devices of the network have routers and switches that are comprised of forwarding plane, control plane, and application plane, and these are embedded into the network device.
4. In SDN, the control plane (how the packets are forwarded and where to forward the packets) and data plane (handles the packet with respect to the rules that are defined in the control plane) are decoupled from each other.
5. Every IoT agent needs to be registered with the controller of IoT having the details that include address, identifier of the object, communicating network protocol, and the underlying network.
6. The main aim of IoT is to interconnect the objects to the Internet, whereas SDN provides the uniformity for the management of the network by disassociating the control plane from the data plane.
7. The facilities availed for the integration of SDN-IoT have been diagnosed in various domains that include smart transportation, smart grid, etc. Integration of SDN and IoT provides the security in IoT because many mechanisms are being easily implemented by exploiting the features of SDN.
8. *Authorization* is defined as the procedure that determines whether the entity or user can access the resources.
9. *Authentication* is defined as the procedure that recognizes the entity and is necessary for authorization.
10. IoT is categorized into three layers: perception layer, network layer, and application layer.

11. Physical Attack, Malicious Node Injection Attack has been considered as the most dangerous attack. This attack is transforming the data and inhibits all the services.
12. Network Attack, Sinkhole Attack has been taken as the most threatening attack. In this, the attacker can install threats such as modifying and dropping the packets.
13. Software Attack, Worm Attack is a risky attack. This attack is the riskiest form of attack on the Internet nowadays. It is the self-owned program which destroys the PC by the use of security holes in the networking hardware and software.
14. Encryption Attack, Side Channel Attack is the most unsafe attack and not easy to handle. It is tough to perceive as an attacker uses the side channel information to perform this attack.
15. On the basis of the approach followed, we have highlighted the "Multiple SDN Controller Architecture for the Ad-Hoc Networks."
16. The proposed architecture of SDN-Ad-Hoc consists of the legacy interfaces which are interconnected to the virtual switch and is controlled by the controller of SDN.
17. Ad hoc users have to integrate using all the other nodes in this configuration that are connected directly to the domain of SDN.

References

1. Zhang, Z.-K., Cho, M.C.Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., Shieh, S.: IoT security: ongoing challenges and research opportunities. In: IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234 (2014)
2. Sahoo, K.S., Sahoo, B., Panda, A.: A secured SDN framework for IoT. In: International Conference on Man and Machine Interfacing (MAMI), pp. 1–4 (2015)
3. Conti, M., Dehghantanha, A., Franke, K., Watson, S.: Internet of Things Security and Forensics: Challenges and Opportunities. Elsevier (2018)
4. Nawir, M., Amir, A., Yaakob, N., Lynn, O.B.: Internet of Things (IoT): taxonomy of security attacks. In: 3rd International Conference on Electronic Design (ICED), pp. 321–326 (2016)
5. Tayyaba, S.K., Shah, M.A., Khan, O.A., Ahmed, A.W.: Software defined network (SDN) based Internet of Things (IoT): a road ahead. In: Proceedings of the International Conference on Future Networks and Distributed Systems, p. 15 (2017)
6. Nunes, B.A.A., Mendonca, M., Nguyen, X.-N., Obraczka, K., Turletti, T.: A survey of software-defined networking: past, present, and future of programmable networks. IEEE Commun. Surv. Tutorials. **16**(3), 1617–1634 (2014)
7. Govindarajan, K., Meng, K.C., Ong, H.: A literature review on software-defined networking (SDN) research topics, challenges and solutions. In: Fifth International Conference on Advanced Computing (ICoAC), pp. 293–299 (2013)
8. Karakus, M., Durresi, A.: A survey: control plane scalability issues and approaches in software-defined networking (SDN). Comput. Netw. **112**, 279–293 (2017)
9. Sezer, S., et al.: Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Commun. Mag. **51**(7), 36–43 (2013)
10. Deogirikar, J., Vidhate, A.: Security attacks in IoT: a survey. In: International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 32–37 (2017)
11. Khan, F.I., Hameed, S.: Software defined security service provisioning framework for internet of things. arXiv Prepr. arXiv1711. 11133 (2017)

12. Olivier, F., Carlos, G., Florent, N.: New security architecture for IoT network. Procedia Comput. Sci. **52**, 1028–1033 (2015)
13. Hu, Z., Wang, M., Yan, X., Yin, Y., Luo, Z.: A comprehensive security architecture for SDN. In: 18th International Conference on Intelligence in Next Generation Networks, pp. 30–37 (2015)
14. Flauzac, O., González, C., Hachani, A., Nolot, F.: SDN based architecture for IoT and improvement of the security. In: IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, pp. 688–693 (2015)
15. Vandana, C.: Security improvement in iot based on software defined networking (sdn). Int. J. Sci. Eng. Technol. Res. **5**(1), 2327–4662 (2016)
16. Rawat, D.B., Reddy, S.R.: Software defined networking architecture, security and energy efficiency: a survey. IEEE Commun. Surv. Tutorials. **19**(1), 325–346 (2016)
17. Huang, H., Zhu, J., Zhang, L.: An SDN_based Management Framework for IoT Devices. IET, Limerick, Ireland. (2014)
18. Humernbrum, T., Glinka, F., Gorlatch, S.: Using software-defined networking for real-time internet applications. In: Proceedings of the International Multi-conference of Engineers and Computer Scientists, vol. 1. IET, Limerick, Ireland (2014)

Himanshi Babbar is Assistant Professor in Research in Computer Applications, working in Chitkara University, Rajpura, Punjab, India. She has 2 years of teaching experience in CGC, Landran, Mohali, Punjab. She had completed MCA (Master of Computer Applications) in Chitkara University, Punjab Campus, and is currently pursuing PhD in Computer Applications in Chitkara University, Punjab Campus. Her area of research is Software-Defined Networking. She has attended two national conferences and published many papers in national and international journals.

Shalli Rani is Associate Professor in CSE in Chitkara University (Rajpura (Punjab)), India. She has more than 14 years of teaching experience. She received MCA degree from Maharshi Dayanand University, Rohtak, in 2004; MTech degree in Computer Science from Janardan Rai Nagar Vidyapeeth University, Udaipur, in 2007; and PhD degree in Computer Applications from Punjab Technical University, Jalandhar, in 2017. Her main areas of interest and research are Wireless Sensor Networks, Underwater Sensor Networks, and Internet of Things. She has published, accepted, and presented more than 25 papers in international journals/conferences. She has worked on Big Data, Underwater Acoustic Sensors, and IoT to show the importance of WSN in IoT applications. She received the Young Scientist Award in February 2014 from Punjab Science Congress in the same field.

A Comprehensive Study of Attacks on the IoT and its Counter Measures Using Blockchain

Pardeep Kaur and Shalli Rani

1 Introduction

In 1999, the term "Internet-of-things" (IoT) was first used by Kevin Ashton. Such devices are able to assemble information more accurately and efficiently than a person, and this assembled data has possibly changed the human life-style [1]. It combines the 'Internet' with devices such as sensors, mobiles, actuators, localization systems or Radio Frequency Identification (RFID) tags called "things" having a unique address and provides a network of different devices. By 2025, the US National Intelligence Council expects that chips will resides in everything, including paper documents, furniture, and food packaging [2]. The integral elements of the IoT are Wireless Sensor Networks (WSN) and Machine-to-Machine (M2M) systems. With the arrival of smart homes, cities, and smart vehicles, the Internet of things (IoT) has developed as a territory of unbelievable effect, capability, and development, and according to the prediction of Cisco Inc., by 2020 there will be 50 billion interconnected devices [3]. Most of these devices are easily hackable because of limited computation, repository, and network capacity; therefore, they are unsafe from endpoint devices such as computers and smartphones. To protect all these devices from the different kinds of attacks, blockchain technology has come into use. Blockchain technology was used by a group of researchers to time stamp digital documents in 1991 [4]. In 2008, this technology was reinvented by Satoshi Nakamoto for bitcoin (cryptocurrency) [5]. Blockchain has been imple-

P. Kaur · S. Rani (✉)
Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India
e-mail: pardeep.kaur@chitkara.edu.in; shalli.rani@chitkara.edu.in

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_2

mented over a wide range of industries, including real estate, finance, healthcare, the government sector [6], and the IoT. This explosion occurred because applications that could only run through a central system can now run without any trusted third party through peer-to-peer connectivity with the same functionality and the same amount of certainty. Due to the fast development of smart devices, such as smart television, cars, and smart phones, with high-speed networking capacity, the IoT has achieved vast popularity and acknowledgment. It depicts a network where "things" are embedded devices, and they have sensors/chips. These sensors/chips are able to communicate through a public or private network [1], and these devices can remotely control and provide ideal functionality. The information sharing from one node to another node takes place over a network that deploys the standard protocols of communications. These smart connected devices range from small devices to broad machines, and each of these devices contains sensors or chips. For instance, according to the American College of Cardiology, Apple Watch's effectiveness at detecting heart conditions such as AFib is promising; this test is the largest ever conducted. Apple watch users who received notifications from the watch about an irregular heart beat were given an electrocardiogram device to wear. Using the ECG, the scientists were able to confirm that a third of those who received a warning from the watch actually had AFib. About 84% of notifications from the watch were confirmed to be AFib episodes since the condition can be intermittent [7]. Similarly, home devices, such as television, lights, refrigerators, and washing machines, can also be controlled remotely through the IoT. Similarly, smart cars contain many features such as an auto gear system and auto parking system. There are manifold other applications, such as industrial controlling and monitoring, location determination at hazard sites, smart badges and tag, monitoring tire pressure, monitoring soil for moisture, pesticide, herbicide, and pH levels, as well as peripheral devices, such as joystick, wireless mouse, and games. Home automation involves heating, air conditioners, security, lighting, ventilation, automatic curtains, windows, doors, locks, etc.

The IoT is not only available for personal use; it also serves in national needs. Different smart devices perform various activities, such as traceability of objects through chips so that the current location of an object can be known, interconnectivity in automobiles, placing the chips on birds helps to uncover areas for maps, monitoring surgery in hospitals, identifying climate conditions, and distinguishing proof of creatures using biochips. The information gathered through these devices is used in real time to enhance the performance of the entire framework. Distributed computing gives the virtual framework to utility processing, which incorporates examine devices, repository devices, visualization platforms, analytics tools, and customer shipments [8]. On demand customers can access the data from anywhere at any time. Smart connectivity with existing networks using the network's resources is an essential element of the IoT.

2 Security Requirement for the IoT

2.1 Privacy, Integrity, and Confidentiality of Data

In IoT networks, data travels over various devices; therefore, to ensure the confidentiality of data, cryptography techniques such as the encryption decryption mechanism of data are required. For pernicious goals, attackers may attack the data stored in IoT devices by modifying that data to violate its integrity.

2.2 Authorization, Verification, and Accounting

Authorization mechanisms ensure that information access is only provided to authorized users. Authentication is essential in IoT devices to secure the communication between two parties. The devices in the network must be verified so that privileged access can be given to specific devices. Because IoT architecture contains heterogeneous devices, the verification mechanisms must be diverse. The combination of verification and authorization provides a proper secure and trustworthy environment for interaction. Accounting represents the source utilization, and a solid mechanism for protecting the network framework is given by evaluating and maintaining records.

2.3 Services Availability

Denial-of-service attacks might block the availability of services given by IoT devices. To degrade the services provided by IoT devices to their users, at various levels attackers use different attack approaches, such as Spoofing attacks, Sinkhole attacks, Blackhole attack, Buffer reservation attack, jamming adversaries or replay attacks.

2.4 Energy Efficient

With low power consumption and short storage memory, IoT devices provide services to their users at very low cost.

By producing unnecessary artificial service requests, attackers cause network overflow to exhaust the IoT devices, resulting in an increase in power utilization [3].

3 Failure of Single Point

A regular development of heterogeneous systems on the IoT-based framework may disclose countless single-points of failure. It is necessary to develop a protected environment for a large network of IoT devices.

4 Attack at Access Level

Attackers can access IoT devices in two ways:

Passive attack: In this type, the attacker can only read the data that is sent from sender node to receiver node.
Active attack: In this type, the attacker can read as well as modify the data over the communication medium.

5 Categories of Security Issues with Their Solutions

The IoT has a wide range of heterogeneous devices from small chips to large-end users. Therefore, security and privacy issues take place at different levels [1]. Detecting attacks is essential, as it is the primary step toward constructing a harmless and trustworthy wireless network. In recent years, the IoT has been a focal point of research, and since everything is connected to the Internet, security and protection of broadcasted and stored data are the main concerns in IoT applications. As security threats, various vulnerabilities exist at different levels.

5.1 Security Issue at Low Level

Jamming Attack (Denial-of-Service)

The jamming style attacks occur due to a shared medium in wireless networks. In this type of attack, a jammer repeatedly ejects radio frequency signals to block the traffic on the network [9, 10]. A jammer remains silent when there is no action taking place over the channel but when it identifies activity on the channel it starts interference over the network and stops following MAC protocols. Before transmitting it does not wait for channels to become ideal. Sometimes, instead of injecting bits, it alternates the network between sleeping and jamming. As a result, the attacks target the reception of messages. There are four categories of jamming attack models: (a) Constant (b) Deceptive (c) Random, and (d) Reactive jammer [11].

For wireless sensor networks, a jammer is an element that is intentionally attempting to hamper communication to corrupt packages over transmission. The presence of a jamming attack can be determined by different techniques such as signal strength (ambient energy) and carrier sensing time. Both of these techniques are able to detect a constant jammer and deceptive jammer but are not able to detect random and reactive jammers effectively. Xu et al. [11] proposed a technique to identify jamming attacks through the procedure of successful Packet Delivery Ratio (PDR). The PDR is either calculated by the sending node or by the receiving node in communication. The PDR on the sender side is evaluated by keeping track of acknowledgements received from the receiver. On the other hand, the PDR is evaluated by the ratio of packages that pass the Cyclic Redundancy Check (CRC) to the number of packages that reach the receiver side. There are two detection algorithms: (a) Consistency check signal strength can be achieved by evaluating PDR between each node with its neighboring nodes and then checking whether this PDR value is consistent with signal strength. (b) Consistency check location information uses the PDR value to indicate the link quality and provide location information of the WSN. The jamming status of a node can be concluded by checking whether the node's calculated PDR value is consistent with the given location of its neighboring nodes. A High PDR value means neighboring nodes are close to that particular node, and if all neighboring nodes have low PDR values, it means the node is affected by a jamming attack.

Another anti-jamming technique is dependent upon the integration of error-correction codes with cryptographically strong interleaves (i.e., attackers are not able to estimate the interleaving function). Existing anti-jamming systems depend upon a broad utilization of spread-spectrum techniques utilized at the bit level to protect data packages. This kind of technique independently assures bits from jammers and are satisfactory for sound communication in which the jammer blocks the communication channel so that packages would not reach their destination in the appropriate time. The interconnecting nodes use a high-gain spread sequence to reduce the energy of jammers. In a "non-error-correction" encoded data package, a single bit error causes deprivation to the loss of the full package generating a CRC error [12].

Insecure Initialization

For appropriate functionality of an integrated system without breach security and privacy of network services, a secure method is required to initialize and configure the IoT framework at the physical level. Due to the broadcast behavior in wireless networks at the medium access control (MAC) layer or network layer, communication over the channel is generally vulnerable to intrusion by unauthorized receivers. That is why security becomes an essential issue as well as a challenge. Cryptographic technologies are the center attraction of security issues; however, they also have some limitations including computational complexity because it is tough to perform resource constrained wireless networks and proper arrangement of secret keys [13].

The existing physical layer security mechanism was introduced by Pecorella et al. [14], and these mechanisms are categorized into four parts on the basis of physical characteristics such as secrecy transmission capability, channel fingerprint, spectrum spreading of signal power, and cooperative. The physical layer technique is used to upgrade secrecy for WSN in which an unauthorized user is unfamiliar with the communication channel or the communication channel of an authorized user is less noisy than for an unauthorized user. The secrecy transmission rate is the rate at which secrecy data is transferred from sender to receiver, and both of them are assured that there is no eavesdropper within the specific area. The maximum secrecy rate is called its secrecy capacity.

Using the physical layer security technique makes it more challenging for attackers to analyze the broadcasted data [13]. Signal processing methods play an essential role in developing physical-layer secrecy in multiantenna wireless systems. In the data transmission phase, artificial noise and secrecy precoding transmission mechanisms are appropriate ways to expand the signal quality difference at the intruder [15].

Low Level Sybil Attack

Sybil attacks are popular in peer-to-peer networks where the communicating medium is broadcasting and are generated because of malicious Sybil nodes, which operate a huge number of forged identities. By using random medium access control (MAC) protocols a Sybil node might throw a channel demand message of high rate to an access point to mimic a huge number of clients so that the IoT application's performance can be degraded. As a result, appropriate nodes in the same network are refused access once the Sybil node has dominated an access point's channel schedule [16]. One approach to execute a Sybil attack is to have the Sybil node directly interact with appropriate nodes, and when this appropriate node broadcasts a message to the Sybil node, the existing malicious node reads the information. A second approach is that no appropriate node directly interacts with Sybil nodes. Messages broadcasted to a Sybil node are transmitted through one of these malicious nodes, and that intermediator malicious node pretends to pass on the information to a Sybil node [17].

In Sybil attacks, a malicious node illegally claims a huge number of forged identities and exhausts resources over the network. In a Rich-scattering environment, to detect Sybil attacks, Hong et al. [15] introduced a channel-based authentication method that uses the uniqueness of channel responses in indoor and urban environments. The Sybil indicator includes a test measurement that is selected on the basis of attack procedure, number of claimed identities, and synchronous access points. The test examines various parameters such as number of channel estimates, total users, Sybil users, access point, bandwidth, and signal power. Demirbas and Song [18] find Received Signal Strength Indicator (RSSI) to be a reliable and time-varying solution to Sybil attacks because it does not burden WSN with keys pair. When the destination node receives a message from the sending node, the receiver

joins the sender identity with RSSI of the message. When other messages using the same RSSI associate with various sender identities, the receiver will be able to detect the Sybil attack.

Spoofing Attacks

Spoofing attacks such as IP address spoofing attack and address routing protocol are genuine risks and occur when a malicious party mimics another user in a network to eject attacks so that it will be able to read stored or transmitted data from the sender to the intended receiver. It is necessary to identify the existence of spoofing attacks and remove them from the network. Using cryptographic verification is the conventional way to deal with such attacks [19].

Full-scale cryptography authentication is not enough for identity verification; it needs a proper key-management system, further infrastructure and computational load. K-mean cluster analysis is the mechanism for identifying spoofing attacks along with locating the address of the performers of the attacks. The position of the attacker can be identified by using localization algorithms, which are based on area or point. The functionality of the K-means spoofing identifier is calculated in terms of detection rates and receiver operating characteristic curves. Normally, the gap among the original node and spoofing node can be predicted with a median error of 10 feet [19]. Another approach, proposed by Xiao et al. [20], is a rich scattering environment, the physical layer technique for upgrading authentication. This technique uses hypothesis test and channel frequency response measurements to distinguish between unauthorized and authorized users. Another approach proposed by Li et al. [21] is the idea of a forge-resistant link related to transmitted packages and when forge-resistant consistency verifies, which allows other network items to identify abnormal functionality.

Sleep Deprivation Attack

Sleep deprivation attack is a destructive attack and especially appears in a link layer, where a pernicious node insists for appropriate nodes to waste their power by restricting the sensor nodes from going into low power sleep mode. The main aim of this attack is to enlarge the power consumption of the target node. In the 6LoWPAN environment, when a huge number of activities are performed at a time it causes reduction of battery life.

Rivest et al. [22] introduced a system of cluster-based layered technique to design a lightweight Insomnia Mitigating Intrusion Detection System (IMIDS) that can mitigate this kind of attack without utilizing MAC protocols, such as G-MAC, S-MAC, B-MAC, and T-MAC. The goal of this system is to increase the lifetime of the WSN, and this system framework can productively relieve sleep deprivation assault in WSN. Computer Simulation conclusions in MATLAB display the viability of the introduced model in finding sleep deprivation attacks. Bhattasali and

Chaki [23] solve the problem of WSN by utilizing multiagent and semantic techniques. Network security consists of two categories: prevention-based techniques and detection-based techniques. At the point when an interruption happens, prevention-based techniques are regularly the main line of defense against assaults. After the failure of prevention-based techniques, then the detection-based technique is used to identify and exclude the attacker. The detection-based technique is further categorized: misuse detection and anomaly detection. After attack, misuse detection is used to define a changed pattern from the original pattern. Anomaly detection uses a set of typical profiles and distinguishes uncommon deviations from the ordinary conduct as anomalies.

5.2 Security Issues at the Intermediate Level

At the IoT network layer and transport layer, intermediate-level security issues take place that are primarily concerned with session management, routing, and interaction between nodes.

Fragmentation Caused Replay or Duplication Attacks

The fragmentation procedure is a breakdown of an IP datagram into small packages so that they can be easily transferred over different networks from a sender and assembled on the receiver side. A datagram receipt consists of the sender's address, receiver's address, size of datagram, and tag of datagram. Several styles exist where attackers can use fragmentation to percolate, causing denial of service or replay attack to networks. Only a sender and receiver is required for fragmenting and reassembling of packages. Thus, in-between routers and switches should not include the fragmentation process. If the IP package is modified in between sender and receiver, a security hole exists. An attacker can block the successful transmission of packages at the destination node. Additionally, an attacker can manipulate the datagram receipt based on which sensor nodes will suffer from re-booting, performance can be stopped or shutdown, because of re-sequencing of packages re-assembling buffer overflowed at receiver side, exhausting processing sources, etc. Some IP package fragmentation attacks include ping of death, jolt, fragrouter, new teardrop, and tiny fragmentation. [24].

Kim [24] introduced a replay attack protection technique. This technique adds a timestamp for unidirectional fragmented packages and a nonce for bidirectional fields to the datagram receipt. Without any serial number, timestamp and nonce provide security against replay attacks. The main aim of the timestamp filed is to fit a datagram within a single frame by dividing it into small packages. All packages, except the last one, are a multiple of eight bytes. The nonce field consists of an arbitrary number of at least 6 bytes that is chosen by the sender of the requesting

message. The main aim of nonce is to ensure that packaging is a fresh reaction to a request sent previously by the node.

Hummen et al. [25] proposed two other approaches: content chaining scheme and split buffer. In the content chaining approach, a node is able to cryptographically check that accepted fragments at the receiver end belong to the same package on a pre-fragment basis. In the split buffer approach, the appropriate sender directly competes with an attacker to assemble buffer sources and splits the assembled buffer into fragment-size buffer slots. The buffer slot will be filled when a complete package has been delivered or overload condition is reached. If overload condition is reached, then the node has the capability to take the decision of which package to discard, and this decision depends upon per-package scores. Packages with lower score will be discarded, and those with highest score will be accepted.

Buffer Reservation Attack

The buffer reservation attack reserves the memory space of the receiving node for a time period of package reassembly timeout. If all fragments are delivered successfully, the attacker benefits from the recipient of a fragmented package not being able to determine that most of the space has been misused by the attacker. The receiving node in the network is the buffer space used to store the fragmented packages for assembly, and the attacker can misuse this space by sending inadequate packages to the target node. The space is occupied by these inadequate packages, causing the overflow condition. Now the targeted node has to discard some packages.

The attacker can block this space at very low cost. Hummen et al. [25] proposed a scheme that increases this cost for the attacker so that the attacker has to send inadequate fragmented packages continuously in short bursts to keep the network busy and reserve space at the target node and the appropriate node would not be able to reserve space for package assembly at the receiver end, causing the buffer reservation attack to suffer from a flooding attack. Thus, the attacker gains no advantage by sending unfragmented packages to the target node.

Another approach sets the reassemble timeout of fragmented packages to 60 seconds to handle fragment loss during communication. The goal of this timeout is to decrease the space occupied by incomplete reassemble fragments. When this time runs out, the receiving node will drop all the incomplete fragments so that memory can be free for new fragmented packages.

Insecure Neighbor Discovery

In IoT development architecture, each device has to be especially distinguished over the network. It is necessary to secure the particular channel through which information is to transfer to a specific destination in the end-to-end message communication. The sensors in WSN have less power, are less expensive, of small size, and are capable of doing small computations. Thus, these sensors are penetrable to different

attacks, such as man in middle of communication of two nodes, tracing of router, and duplicate address identification, and these are neighbor discovery attacks. If the neighbor discovery signals penetrate toward wormholes (discussed later), the appropriate nodes will get the wrong routing information about their neighbors. This might prompt the decision of a non-existence route [26].

To secure neighbor discovery packages directly, a security framework with modules is explained by Riaz et al. [27], and it can be achieved by using an IP security authentication header with a pair of symmetric keys. This pair of keys is only known to participation nodes of the network. However, it stills faces some security issues, and to overcome this problem it uses a public key signature for verification of neighbor discovery packages. When one node finds its neighbor node, before set up communication keys, first it will verify that discovered node by applying some verifications methods.

Sinkhole Attack and Blackhole Attack

A sinkhole is a kind of denial of service (DoS) attack engaged by an inner attacker to disturb the functionality of a wireless sensor network. Basically, a sinkhole attack happens when a bargained node executes two pernicious acts. The first act is, by advertising a favorable path, the sinkhole attracts valid traffic from its surrounding nodes by modifying the rank of messages in the destination information object (DIO) message. The rank field describes the positivity of the node to its neighbors. The bargained node creates false routing rumors that it has power and spreads it to neighboring nodes. When the bargained node broadcasts its low rank then all traffic moves toward this node, causing its neighbor to choose it as a parent, and it becomes the cluster header of each round. The second act is, when all nodes start transferring packages to this malicious cluster header, it starts dropping only selected packages. A sinkhole attack slows down the process of message sending from the sender node to the receiver node to reduce the end-to-end delivery functionality. In a blackhole attack, the procedure is the same, except that the malicious cluster header drops all the packages.

Weekly and Pister [28] found two methods to overcome the sinkhole problem. The first is rank verification and the second is parent failover. These methods allow complete packages to be sent to their destination.

The rank verification method necessitates that bargained nodes lower their rank by 1 and all the edges in the graph should be of equal weight. Moreover, together these techniques are more effective than if they are applied individually. The method is based on a one-way hash function such as SHA1 [29] and a hash chain. This technique can help to acquire high quality end-to-end performance by upgrading the density of routers in the network. The root node begins with any random number and calculates its hash. When this hash is broadcasted, the DIO rank is accordingly increased or replaced. In the network, before forwarding, the appropriate nodes execute further hashing, but on the other hand the bargained node starts communicating with the hash value. After some time, to assure that the routing tree has

converged, for verification by individual nodes, the root node executes a broadcast of the random value selected at first to all the nodes in the network. If a discrepancy occurs at a node, it means an inauthentic parent rank value.

In the end-to-end acknowledgement method or parent failover method, when the root node first transmits the DIO message, it inserts an unheard noise set (UNS) attribute to this message. This UNS is approved by the root node so that no one can change the transmitted data. The UNS is used to identify the bargained node by a sinkhole in the network. After an interval of 10 seconds, non-root nodes transfer data. If the root receives this data less than 30%, this node will be added by the root to the UNS. Carefully choose the threshold value. When a node receives the DIO message with itself involved in the UNS, the node blacklists its parent for consequent intercommunication, so that no node would ever select it as parent.

Firoz et al. [30] introduced two approaches for blackhole attack: local decision and global verification. Every node in the network notices the communication behavior of its neighbor by eavesdrop data packages transferred by its neighbors, and a node identifies a mistrustful node based on the data collection of the communication behavior of its neighbor nodes. After finding a mistrustful node, the checkout procedure starts, and, here, a validating node validates a mistrustful node. Verification is started by a query from the root node to find out if it received packages.

Wormhole Attacks and Rushing Attack

In networks, sensors use radio channels to transfer data/information from a sender to an intended destination. Malicious nodes intercept the packages and pass them through to some other location in the same network and retransfer them, and this penetrating process makes a wormhole in the sensor network [26]. If a fast transmission path lies in-between the two ends of a wormhole, the penetrated packages can propagate faster than the normal multi-jump route, causing a rushing attack [31].

The previous approaches require that the node should be prepared with special hardware, such as a synchronized clock or antenna. Wang and Bhargava [26] presented a method to protect a network from such wormhole attacks, MDS–VOW (Multi-Dimensional Scaling – Visualization Of Wormhole). In this method, special hardware does not need to be attached to sensors, and it selects and combines mechanisms from sociology, PC illustrations, and logical representation. By using multiple dimension scaling, MDS–VOW retraces the network to find the positions of fake identities.

RPL Routing Attack

Due to the increasing demand for wireless sensors with short memory and low power, IPv6 Routing protocol was deployed by IETF [32] ROLL Working Group to provide routing solutions. The IPv6 Routing Protocol for Low-power and Lossy

Networks (RPL), constructs and maintains directed acyclic graphs (DAG) routed to at least one base station. The base station compiles the information evaluated by other participating nodes in the network and controls these nodes. Thus, the destination node in the network is the base station. An attacker enters into the base station or attacks the nodes near the base station and can modify, intercept, forge, replay, and create messages so that they can interfere with the function of the whole network by divert routing toward a large path so that the node batteries are exhausted. If the attack impact is major then it will lead to reconstructing of the entire DAG and may exhaust the node's batteries. An attacker can achieve this by modifying the version number of the Destination Oriented Directed Acyclic Graph (DODAG) or by modifying the DODAG node's rank value.

The term rank value defines the node's level in the graph. If the rank is low, the node is close to the base station, or if its rank is high, the node is far from the base station. Sibling nodes of a particular node also have the same rank value, as a node will forward more messages to the closest one. If a node sets one node as a base station, a loop can occur in the network. If the network find such loops, and sometimes it is difficult to solve loops, then the whole graph might reconstruct, and this construction starts when the base station transfers DIO messages with an upgraded version number.

To block loop generation in the network, the RPL follows the rank rules that in the network a child node should always have greater rank than its parent. The DIO message has the version number as a component, which is correlated to the network. At each time, the version number is augmented monotonically by the network root, and to revalidate the integrity and enable worldwide occurrence, the root of DODAG chooses to form a new version of the DODAG. The version number is channeled unchanged down the DODAG as nodes join the new DODAG. For verification version numbers and ranks, the proposed security system is known as Version Number and Rank Authentication (VeRA) [33] and uses the hash function such as SHA [29] and MAC function such as digital signature RSA [33] and HMAC [34]. According to RPL protocol, the rank value of a child node is greater than the selected DODAG parent node to stop generation of loops, and the rank value of sibling should be equal to that node. RPL provides cryptography methods for securing control messages, but the network is still able to be attacked because sensor objects are not manipulation resistant. In RPL, through control messages, the child gets the parent's information messages, causing it to follow a poor quality route because it is not able to check the service provided by the parent node, and it may be possible that there is a malicious node.

Sybil Attacks at the Intermediate Layer

When attackers generate fake identities, IoT devices are penetrable to Sybil attack so that system efficiency will be compromised. Due to Sybil attack, the IoT system may generate wrong reports, which is like cheating a user, the privacy of the system can be lost, and the effectiveness of the network reduced. Users might receive spam

messages or mails. These Sybil identities attract other users by sending spam advertisements and mails to other users to steal other client's private data. Sybil identities disperse malware and phishing sites. In a dispersed vehicular correspondence framework [35] and portable social frameworks [36], Sybil identities produce one-sided choices with "legible" accounts. Without a successful Sybil detection system, the aggregate outcomes can be effectively controlled by the attackers. Since most Sybil identities behave like ordinary clients, it is difficult to distinguish them [37]. Usually, the Sybil identities exist in sensing and social domains, such as Online voting systems [38] or mobile sensing systems [39].

Yu et al. [40] presented SybilGuard as a novel decentralized protocol against Sybil attackers by limiting the size and number of the Sybil group. This protocol depends upon the "social network", where a connection among two users defines a human-established trust relationship like a friend relationship. Sybil users can create many accounts in one network but there are few true relationships. The attack edges connect the honest region (which contains all honest users) to the Sybil region (which contains all malicious users). For 99.8% of the honest users, SybilGuard assures that the size and count of Sybil groups are bounded, and then only these honest nodes will be accepted in the same network by 99.8% of all other honest nodes. These attack edges effect both distributed and peer-to-peer systems including the IoT. The protocol assures that the count of Sybil identities are independent from attack edges, but it depends upon trust edges among Sybil nodes and honest nodes.

Du et al. [41] analyzed various Sybil attacks with their solutions in the IoT. Sybil attacks are divide into three categories based on Sybil attacker's capabilities: Sybil Attack-1, Sybil Attack-2, and Sybil Attack-3. The Sybil attack's solutions are: (a) social graph-based Sybil detection (SGSD), (b) behavior classification-based Sybil detection (BCSD), and (c) mobile Sybil detection (MSD). In Sybil Attack-1, Sybil identities strongly connect with Sybil identities and there are limited relations between Sybil identities and honest identities. In Sybil Attack-2, attackers exist in a social domain. Sybil Attack-2 builds social connections with Sybil identities and true identities. The aim of Sybil Attack-2 is to steal the user's personal information to violate the user's privacy by modifying their personal details. In Sybil Attack-3, Sybil attackers exist in a mobile domain. Basically, Sybil Attack-3 has the same aim as Sybil Attack-2. Due to the dynamic nature of a mobile network, Sybil identities cannot connect with others for a long time period. The aim of SGSD is to label nodes "Sybil" or "honest". Consequently, there are basically two types of SGSD: (a) social network-based Sybil detection (SNSD) [40] and (b) social community-based detection (SCSD) [42]. Analyses of the Orbit Showtime Network (OSN) in [43] compares true and Sybil client's behavior by their clicking habit and browser history and distinguishes them [43]. According to the client's behavior categorization and learning, the BCSD [44] can identify Sybil Attack-2. The aim of MSD [45] is to either identify Sybil Attack-3 or to limit Sybil attacker's behaviors by three ways: (a) Friend Relationship-Based Sybil Detection (FRSD) (b) Cryptography-Based Mobile Sybil Detection, and (c) Feature-Based Mobile Sybil Detection.

Verification and Secure Communication

For secure communication in various IoT devices, verification and access control are essential activities. Due to weak physical security, mobility and dynamic network topology of low power and small storage devices in IoT networks are penetrable to several attacks [46]. Any ambiguity in security at the network layer might expose the network to a large number of dangers [47, 48]. Moreover, because of the constrained resources nature of the smart object, the overhead of Datagram Transport Level Security (DTLS) needs to be reduced and standard protocols established, but direct solutions cannot be used in 6LoWPAN/CoAP networks [49].

To achieve security in wireless networks, the IoT devices and clients are authenticated through key management systems [41]. With the origination of IPv6, a unique ID is assigned to each and every device in the entire world. It is easy to detect what data is sent or received by which device at what time, etc. To ensure data exchanges, IPv6 protocol stacks use IP security [50]. Today, in the evolution of the Internet, the IPv6 protocol and the LoWPAN adaption layer play an important role. Myriad sensing applications have come into existence on the basis of end-to-end communication and secure group communication among the internet administrator and sensing devices. These types of communications are only executable if proper security processes are adhered to in LowPAN [49]. For proper security in the network layer, Granjal et al. [50] proposed an authentication header [51] and encapsulating security payload (ESP) [52] on wireless sensor networks that provides security for IPv6 communications. Security headers with the cryptographic algorithms are particularly used with the IP security architecture while providing fundamental security guarantees independently of the applications running on sensor nodes. For the network layer, security schemes are mapped to adapt to the requirements of various wireless sensor network applications.

Transport Level End-to-End Security

For end-to-end communications between sensor objects and other internet objects, a wireless sensor network application requires these devices to be interconnected with internet hosts. By using a pre-shared key distributed to participating nodes in advance and datagram transport layer security (DTLS) (advanced version of transport layer security (TLS)) [53], devices that depend upon constrained application protocols (CoAP) [49] can protect their communications [54]. At transport-layer, TLS provides end-to-end security and plays an important role. With the aim of minimum communication errors, the constraints such as microprocessor, energy, and memory evaluate how much energy is required for low-energy wireless communications and provide small packages with low communication speeds. The aim of transport level end-to-end security is to send data from a sender to a desired receiver; therefore, it requires authentication mechanisms so that data can be transmitted over a network in a secure manner without violating privacy [55].

There are three key security management and verification approaches for end-to-end communication with other devices: (a) In a Pre-shared key approach, devices save preconfigured keys. (b) In a Raw Public key approach, identification devices have at least one public key. (c) In certification mode, certification authority devices get public keys [55].

For end-to-end secure communication among IoT devices, Kothmayr et al. [56] proposed a scheme using two-way authentication based on RSA [57] that used a public key cryptography algorithm dependent upon existing Internet standard protocols such as Datagram Transport Layer Security (DTLS) protocol. The verification can be executed either by fully authenticated DTLS handshakes pre-shared keys or by a trusted platform module (TPM) [58] using RSA. The RSA certificates are transmitted in X.509 format with the help of RSA. The proposed architecture is an appropriate solution for the IoT because it provides confidentiality, integrity, verification with low energy, end-to-end potential, and memory overhead.

When Hyper Text Transfer Protocol (HTTP) clients approach the Constrained Application Protocol (CoAP) server at the back end, the proxy is required to translate packages. At the application layer, a mapping is required between HTTP and COAP so that no malicious code will be added. One solution is to use a Transport Layer Security pre-shared key (TLS-PSK) [59] for transport between routers, in which DTLS packages are encoded into TLS packages and TLS packages are encoded into DTLS packages. Each stream of data has its own TCP connection and protected TCP header.

Another approach is integrated transport layer security (ITLS) [60]. A package sent by a sender is encrypted with a pair of keys. The proxy uses the primary key to decrypt a package and then forward that package to the intended destination. DTLS does not support multicast; therefore, two participating nodes using DTLS first discuss a session key for communication. The key is evaluated by a pre-shared key and a pair of nonce generated by the server and client.

The requirements to fulfill the multicast for CoAP are defined in [61]. Another framework, BlinkToSCoAP [63], implements lightweight versions of DTLS, CoAP, and 6LoWPAN protocols over a tiny operating system. BlinkToSCoAP messages interchange among two Zolertia Zl devices, permit evaluation of energy consumption, memory footprint, and package overhead and potential. The obtained outcome demonstrates that securing CoAP with DTLS in the IoT is absolutely achievable without bringing about much overhead.

Session Establishment and Resumption

At transport layer, a session can be hijacked with a forged message, which can cause replay attacks, denial-of-service (DOS), wiretapped secret-key attacks, man in the middle attacks, etc. [62, 63]. An attacking node plays the role of a victim node to continue the session among two nodes. By changing the serial number, communicating devices have to re-transmission the message [1].

Peretti et al. [62] suggested a mutual authentication based on cryptographic module and session key distribution for a secure session management that is robust to various attacks. In this scheme, first an arbitrary number is selected, then encoding is applied on that number to produce a session key; afterwards, that key is used for encoding of another arbitrary number. This encoded value will be used for verification. Without repetition of parameters, a new session key can be generated for each session. Another verification method is the Edge-Fog-Cloud network architecture; at the Edge of the network Fog user's smart cards/devices are mutually verified with the Fog servers at the Fog layer. This scheme is known as Octopus and needs a roamer user in the network, who holds one long-lived master secret key so that they can communicate with any of the Fog servers in the network with the proper verifiable method [63]. Without any extra overhead and re-enrolment, the fog users can mutually authenticate with this new Fog server. For each user the Fog server stores only one secret key and fog users have no concern with public-key architecture. In this method, the fog user has to perform a few hash functions and symmetric cryptography.

Cloud-Based Privacy Violation

Network-based arrangements inside the IoT depend on cloud organizations. This methodology permits the advantageous and dependable communication of networks [64]. Due to the source constraints of IoT devices, the entire data related to a user is stored in clouds. These clouds can be used at anytime from anywhere. Cloud services are cheap compared to building one's own storage mechanisms. The input, output, and computation function are nearly correlated to the IoT user's privacy, which should not be presented to malignant IoT clients and pernicious cloud servers [65]. IoT attacks can breach a user's privacy and location privacy that is stored in the cloud. A pernicious cloud service could manipulate confidential data that is transferred from a sender to receiver or may modify data stores in clouds.

To overcome the concerns such as a pernicious cloud service provider that manipulates confidential data or an attack on the cloud, Henze et al. [64] proposed D-CAM, which uses the hash chain and digital signatures to tackle the issues of distributed and secure design, authorization and management borders in a cloud-based IoT network. To control messages, the cloud with D-CAM provides highly available and scalable storage.

5.3 Security Issues at High Level

Constrained Application Protocol Security with Internet

The application layer is penetrable to various attacks. The CoAP is a synchronized web transfer protocol constructed by IETF using HTTP for use with constrained networks and constrained sources, such as low power and short memory. CoAP gives a request/response communication system among end user applications by

running over User Datagram Protocol (UDP) for both synchronized and unsynchronized acknowledgement. In a client-server system, to provide resource-oriented communication, CoAP uses HTTP commands such as PUT, POST, GET, and DELETE. The main purpose of designing a UDP-based application layer protocol is to overcome TCP overhead and bandwidth needs. Each header of the two bits package describes the Quality of service rank, what type of message the package contains, and the state of the package. The CoAP messages use a particular format described in RFC-7252 [66] for secure communication. The multicast support in CoAP requires verification methods and proper key management [67].

CoAP does not involve any inbuilt security functions; it was designed for machine-to-machine and IoT devices interactions. To protect CoAP-based networks and to assure end-to-end protection among two end users located in different networks, Datagram Transport Layer Security (DTLS) is used. DTLS fulfills all the requirements of an IoT environment, such as key management, cryptographic algorithms, integrity of data, and verification of data. At the application layer, during transition these protocols do not allow access to data at the gateway. One solution to secure LLN from various attacks is to use tunnels such as Virtual Private Network (VPN) [67]. At the network layer, VPN is used to interconnect two independent networks through a tunnel to hide the actual receiver and messages. The tunnel ends at the gateway such as the 6LoWPAN Border Router (6LBR) in another network. Support from the operating system is not important for utilizing the DTLS-DTLS tunnel method; however, it needs changes in the network stack of the back end system. Another approach proposed in [68] provides a protection system promoting internet-integrated wireless sensing applications and LoWPANs.

Middleware Security

In the IoT worldview, owing to the enormous number of technologies that take part in the exchange of data, some type of middleware layer is employed. The Naming Addressing Profile server (NAPS) connects various platforms as a middleware in the IoT environment. At the back end NAPS provides the services of collecting sensor's data, filtering data on the basis of content, and matching [69].

These devices are deployed across various platforms and middleware is used in the IoT for communication between different devices, networking, verification, to handle all the data transfer over a platform, for service support, protection, security, encryption, etc. Conzon et al. [70] proposed VIRTUS as a middleware solution to implement authentication and encryption for distributed application running in the IoT environment by using open standard protocols such as XMPP [71] and OSGi [72] for private networks only. By utilizing the standard security highlights given by the XMPP protocol, the middleware provides a solid and protected communication medium for distributed applications, ensured with both encryption and verification systems. Because of the scalability problem, for Java the OSGi scheme is a productive unit management framework and gives the primary standardized solution that enables applications to be made out of small, recyclable, and collective elements. In

order to support the dynamic modules combination to simplify the configuration and the deployment, OSGi gives structuralism to runtime units' management and has been exploited in VIRTUS to deal with automatic supervising of dependencies and updates. The XMPP protocol is open for everyone, it is free, provides long-time security, being decentralized means anyone can individually manage the network by using its XAPP server, and being extensible means anyone can insert their features into the existing core features.

6 Blockchain

A blockchain is a chain made up of blocks, where every block consists of a public ledger or history of all the transactions made in a distributed manner and a copy of this ledger is shared among all the participating nodes in the network. Instead of a central server there is a peer-to-peer connectivity and each and every transaction is confirmed by consensus of a majority of participating nodes. Once information is entered into the public ledger it is almost impossible to delete it. Blockchain [73] is the technology behind the most famous digital currency—bitcoin [5], and it was introduced by Satoshi Nakamoto to solve the problem of double spending [74].

7 Blockchain Concept

Blockchain came into existence to solve the conventional problem of lack of trust in central authority. Blockchain technologies consist of cryptography algorithms, such as Security hash algorithm 256, mathematical puzzle, economic model, networks, and distributed consensus algorithms, for example, Proof-of-stake and Proof-of-work. Some essential elements of blockchain technology are: decentralized, transparent, open source, immutable, and anonymity [3].

7.1 Decentralized

Nodes are connected in a peer-to-peer manner in a blockchain network so that they can share their data directly with others. Distributary data can be stored and updated.

7.2 Anonymity

Trust issues between node to node in a blockchain network are solved by keeping transactions anonymous; only the node's public key address needs to be known.

7.3 Transparent

The recorded, stored, and updated data is transparent to every node in a blockchain network. It helps to understand when which transaction takes place, with whom it takes place, and who knows about the data.

7.4 Open Source

Anyone can join a blockchain network because it is open to each person.

7.5 Immutable

Once data is packed in a blockchain, it is impossible to tamper with it, unless at the same time an attacker or any other node can take control of over 51% of the network.

8 The Need of Blockchain in the IoT

The updated digital world still depends upon a trusted third party to send or receive their data. Most access solutions such as an email service provider that is a certification authority send notifications to us that an email has been delivered successfully or an email address is invalid. It could be any social network such as Facebook, Instagram or it could be a bank sending time-to-time notifications about a person's account balance or transactions and thus they have collected a user's personal data. The conventional truth of the digital universe is it depends on a trusted third party for the security and protection of our digital resources. In some companies such as Fitbit, the data they gather is public by default. Now the problem is hackers can hack these resources; they can modify these resources. That is why blockchain has come into use for security and privacy in every field, including the IoT. Blockchain has the potential to covert the third-party dependent world into independent by empowering a distributive consensus in which at any time in the future every single online transaction involving past and present digital assets can be verified without violating the protection of the involved digital resources and participating parties.

9 Types of Blockchain

9.1 Public Blockchain

In public blockchain each node can verify every transaction and by voting can take part in the consensus process. Examples of public blockchain are bitcoin and Ethereum [75].

9.2 Consortium Blockchain

Partially decentralized, open or private data. In this blockchain the node that has authority can be chosen in advance. An example of a consortium blockchain is hyper ledger [76].

9.3 Private Blockchain

Because accessing data for nodes will be restricted by authority, only selected nodes can participate in this blockchain.

10 Workings

The name 'blockchain' indicates that it is a chain of sequenced blocks in a chronological order. Every individual block consists of a unique hash, transactions that occur at the same time, the hash of the previous block that is mainly responsible for the chain, and the size of the block depends upon the transaction size. The first block of the chain is known as the genesis block as it does not contain any previous hash. Instead of a trusted third party, blockchain uses cryptography to execute a transaction between two willing parties. As shown in Fig. 1, each transaction is secured with a digital signature using a private key and shared public key [77]. The node that first receives the transaction confirms the digital signature with the help of the "public key" of the sending owner of the respective transaction.

In a network, Bob (a node) initializes a transaction request that he wants to send money to Alice (another node) and broadcasts this request over the network. The other nodes in the network verify this request by checking the history of whether the node that generated the request has enough balance to send money. If the transaction is valid then other nodes add this transaction into the public ledger. Then, nodes collect transactions that occur at the same time in a block and broadcast this block over the network. A problem exists here because nodes can also collect unconfirmed transactions and insert them into their block and can broadcast that created block over the network as a suggestion for the next block in the network. The order in which transactions are generated is different from the order in which they are received by different nodes in the network. How is it decided which block should be selected next for the chain? A number of blocks are generated by different nodes at the same time. To solve this problem Satoshi Nakamoto introduced a mathematical puzzle [5]. Each and every block is only accepted into the chain if it is able to solve the answer to this special mathematical puzzle.

This whole procedure is called "proof of work". The miner has to show that he has enough computing resources and is able to solve the mathematical problem for

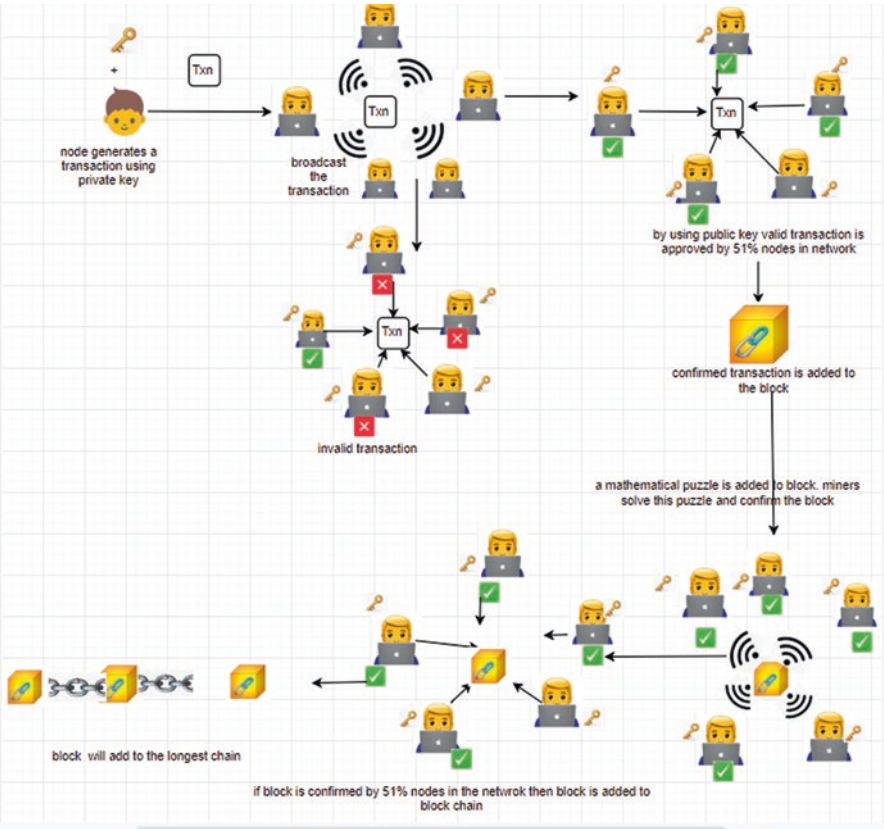


Fig. 1 Workings of blockchain

generating a new block. Moreover, a node has to evaluate a "nonce" that is hashed with hashes of the last blocks and both transactions generate a hash with four leading zeros. The standard work needed is exponential in the count of zero bits required and by executing a single hash authentication procedure. The complexity of the mathematical puzzle is adjusted such that on average a node takes 10 minutes in a blockchain network to make a true answer and is able to add a new block in the chain. The first successful user to solve the puzzle will broadcast the block over the network. Sometimes, more than one block will be solved, leading to several branches in the chain. To order blocks in the chain according to agreement, nodes have to donate their computing resources to solve the puzzle and generate blocks. The nodes that donate their resources are called "miners" and they are awarded for their efforts (Fig. 2).

The longest chain is considered the only appropriate chain in the network. A node can generate a block not only by solving a mathematical puzzle but also there is a mathematical race with honest nodes in the network. Therefore, it is very difficult for an attacker to generate a fraudulent transaction. If a miner mines a block

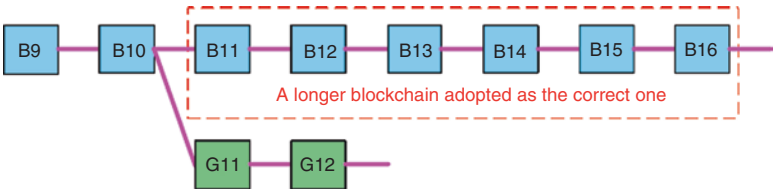


Fig. 2 Select longest chain [78]

with fraudulent transactions then he can lose his computing resources; therefore, every miner mines a block with valid transactions only. As blocks in the blockchain are linked cryptographically together, the whole procedure becomes more challenging.

11 Blockchain Solution for the IoT

As we have discussed, there are several types of attacks in the IoT environment. Blockchain provides a better, more robust and distributed peer-to-peer mechanism to prevent attacks, identify incompatibility and forks, and automatically resolve them without any help from a trusted central server. According to a client's requirement in the case of energy, the integration of the IoT with blockchains takes into consideration a shared market in which machines can buy and sell vitality energy automatically. For example, TransActive Grid [79] is exploring various avenues regarding the idea of a shared market for a sustainable power source in an area of Brooklyn, NY [80]. Solar panels record their overabundance yield on a blockchain, and sell it to neighboring nodes through smart contracts.

11.1 Identity of IoT Devices

IoT devices have relationships with persons, and these persons could be users, manufacturers, administrators or suppliers. Management of this relationship is a difficult task because ownership of IoT devices changes during their lifetime from manufacturer to suppliers, then supplier to retailer, retailer to consumer, thus affecting their identity procedures such as verification and authorization of data. When devices are delivered at a destination through shipping, at the destination the owner sends a signed message to a smart contract to inform everyone that the IoT device has successfully reached the destination. Now this signed transaction plays the role of a verifiable cryptographic receipt of the delivery party's claim that IoT devices were received. On the other end, the receiving party also posts that it is in possession of the IoT devices. When devices get resold, the ownership of devices will be changed and revoked. The whole procedure includes a number of stakeholders and

checks. To keep track of IoT devices, each and every stakeholder in this network maintains their own database, and the input from other parties in the same blockchain updates this database. Other challenges are management of IoT device attributes, such as type, location features, make, manufacturer, deployment, serial number, Global Positioning System coordinates, and capabilities, and relationships, such as deployed by, dispatched by, utilized by, updated by device-to-service, device-to-device, and device-to-human [6]. Blockchain has the capability to effectively resolve these kinds of issues. Blockchain provides a faithful, honest, reliable, authentic environment for observation and trace ownership of goods and assets. When IoT devices register in a blockchain network, then it provides an identity, attributes set, and complex relations to connect, and these attributes and relationships can upload, store, and update distributary on the blockchain network. TrustChain [81] is capable of generating such transactions among unknowns without any trusted central control. TrustChain is a permission-less tamper-proof warehouse to store transaction details regarding ownership of IoT devices. TrustChain generates a temporally immutable chain that is parallel to the original chain for each owner to keep their records; thus, every client can create their own genesis block.

11.2 Address Space

Blockchain is more scalable than IPV6 for IoT devices because blockchain supplies 4.3 billion addresses, and this count is extremely greater than IPV6. The address space of blockchain is 160-bit. A blockchain address is 20 bytes or a 160-bit hash of the public key generated by the Elliptic Curve Digital Signature Algorithm (ECDSA) [82]. Blockchain is able to produce and allocate addresses offline for around 1.46×1048 IoT devices. The probability of address collision is approximately 1048, which is considered sufficiently secure to provide a GUID (Global Unique Identifier). GUID requires no registration or verification when assigning and allocating an address to an IoT device [6].

11.3 Storing Data

Constantly, every second, a huge amount of data is collected and analysis results in economic growth. Data can be public or private. On the basis of this collected data, various organizations predict the future and much more. Each block contains a number of transactions, and each transaction contains one hash value. Storing each hash value requires a large amount of space; therefore, blockchain provides a solution to huge data by storing data in a Merkle tree root form. It combines the hashes of two transactions to make a single hash unless and until one single hash of each block is generated.

11.4 Public Ledger

In every sector, including finance or social networking, a user's sensitive and personal data is stored at a central server and users have no control over that stored data and are not able to use them. They do not know who uses their data or where it is used. Moreover, several types of attacks on central authority can modify or destroy data. Instead of storing data at a central server, blockchain stores data in a chain of blocks and a copy of each blockchain is provided to each user in the network, meaning each user maintains their database individually. When any transaction occurs in the network database of each user, they will be updated automatically. An attack on blockchain would only reach 10 or 20 copies because it is nearly impossible to attack a billion copies of blockchain. When an attacker makes some changes in one block then he has to recalculate the PoW for that block and blocks after that block because each block uses the previous hash and with the change of even a single bit the hash changes. Additionally, in blockchain, only the longest chain is considered a valid chain in the network.

12 Conclusion

IoT devices are used throughout the entire world. Each place surrounding us is sensing enabled by wireless sensor networks, and these IoT devices need to communicate with each other in a synchronized manner. On one hand, there are many benefits of these devices in real life, but on the other hand, these devices are vulnerable to various attacks. Managing such devices properly is a big challenge. When the whole procedure depends on a single central authority, an attack on this single center or any technical challenge may cause this central point to fail. In order to prevent such situations, blockchain has come into existence with peer-to-peer connectivity. There is no central server, and each participating node directly communicates with other nodes. Anonymity, transparency, immutability, decentralization, etc., make blockchain perfect to use in the case of IoT devices.

References

1. Ashton, K.: That 'internet of things' thing. RFID J. **22**(7), 97–114 (2009)
2. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
3. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. **82**, 395–411 (2018)
4. Haber, S., Stornetta, W.S.: How to time-stamp a digital document. In: Conference on the Theory and Application of Cryptography, pp. 437–455. Springer, Berlin/Heidelberg (1990)
5. Nakamoto, S.: A peer to peer electronic cash system, Bitcoin Organization (2008) http://bitcoin.org/bitcoin

6. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. Ieee Access. **4**, 2292–2303 (2016)
7. Apple Watches are surprisingly good at detecting heart conditions says recent Stanford study. https://www.techspot.com/news/79227-apple-watches-surprisingly-good-detecting-heart-conditions-recent.html
8. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (IoT): a vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
9. Wood, A., Stankovic, J., Son, S.: JAM: a jammed-area mapping service for sensor networks. In: 24th IEEE Real-Time Systems Symposium, pp. 286–297 (2003)
10. Xu. W., Wood, T., Trappe, W., Zhang, Y.: Channel surfing and spatial retreats: defenses against wireless denial of service. In: Proceedings of the 2004 ACM Workshop on Wireless Security, pp. 80–89 (2004)
11. Xu, W., Trappe, W., Zhang, Y., Wood, T.: The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 46–57. ACM (2005)
12. Noubir, G., Lin, G.: Low-power DoS attacks in data wireless LANs and countermeasures. ACM SIGMOBILE Mob. Comput. Commun. Rev. **7**(3), 29–30 (2003)
13. Chae, S.H., Choi, W., Lee, J.H., Quek, T.Q.: Enhanced secrecy in stochastic wireless networks: artificial noise with secrecy protected zone. IEEE Trans. Inf. Forensics Secur. **9**(10), 1617–1628 (2014)
14. Pecorella, T., Brilli, L., Mucchi, L.: The role of physical layer security in IoT: a novel perspective. Information. **7**(3), 49 (2016)
15. Hong, Y.W.P., Lan, P.C., Kuo, C.C.J.: Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches. IEEE Signal Process. Mag. **30**(5), 29–40 (2013)
16. Xiao, L., Greenstein, L.J., Mandayam, N.B., Trappe, W.: Channel-based detection of sybil attacks in wireless networks. IEEE Trans. Inf. Forensics Secur. **4**(3), 492–503 (2009)
17. Newsome, J., Shi, E., Song, D., Perrig, A.: The sybil attack in sensor networks: analysis & defenses. In: Third International Symposium on Information Processing in Sensor Networks, 2004. IPSN 2004, pp. 259–268. IEEE (2004)
18. Demirbas, M., Song, Y.: An RSSI-based scheme for sybil attack detection in wireless sensor networks. In: 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06), pp. 5. IEEE (2006)
19. Chen, Y., Trappe, W., Martin, R.P.: Detecting and localizing wireless spoofing attacks. In: 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 193–202. IEEE (2007)
20. Xiao, L., Greenstein, L., Mandayam, N., Trappe, W.: Fingerprints in the ether: using the physical layer for wireless authentication. In: 2007 IEEE International Conference on Communications, pp. 4646–4651. IEEE (2007)
21. Li, Q., Trappe, W.: Light-weight detection of spoofing attacks in wireless networks. In: 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp. 845–851. IEEE (2006)
22. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM. **21**(2), 120–126 (1978). https://doi.org/10.1145/359340.359342
23. Bhattasali, T., Chaki, R.: A survey of recent intrusion detection systems for wireless sensor network. In: International Conference on Network Security and Applications, pp. 268–280. Springer, Berlin, Heidelberg (2011)
24. Kim, H.: Protection against package fragmentation attacks at 6lowpan adaptation layer. In: 2008 International Conference on Convergence and Hybrid Information Technology, pp. 796–801. IEEE (2008)
25. Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., Wehrle, K.: 6LoWPAN fragmentation attacks and mitigation mechanisms. In: Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 55–66. ACM (2013)

26. Wang, W., Bhargava, B.: Visualization of wormholes in sensor networks. In: Proceedings of the 3rd ACM Workshop on Wireless Security, pp. 51–60. ACM (2004)
27. Riaz, R., Kim, K.H., Ahmed, H.F.: Security analysis survey and framework design for ip connected lowpans. In: 2009 International Symposium on Autonomous Decentralized Systems, pp. 1–6. IEEE (2009)
28. Weekly, K., Pister, K.: Evaluating sinkhole defense techniques in RPL networks. In: 2012 20th IEEE International Conference on Network Protocols (ICNP), pp. 1–6. IEEE (2012)
29. Eastlake, D., Jones, P.E: RFC3174-US Secure Hash Algorithm 1(SHA1). (2001). https://tools.ietf.org/html/rfc3174
30. Ahmed, F., Ko, Y.B.: Mitigation of black hole attacks in routing protocol for low power and lossy networks. Secur. Commun. Netw. **9**(18), 5143–5154 (2016)
31. Hu, Y., Perrig, A., Johnson, D.: Rushing attacks and defense in wireless Ad Hoc network routing protocols. In: Proceedings of the ACM Workshop on Wireless Security (WiSe) (2003)
32. Handley, M., Bonaventure, O., de Louvain, U.C.: Internet Engineering Task Force (IETF) A. Ford Request for Comments: 6824 Cisco Category: Experimental C. Raiciu (2013)
33. Somani, U., Lakhani, K., Mundra, M.: Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In: 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), pp. 211–216. IEEE (2010)
34. Krawczyk, H., Bellare, M., Canetti, R.: HMAC: keyed-hashing for message authentication (1997). https://tools.ietf.org/rfc/rfc2104.txt
35. Lin, X.: LSR: mitigating zero-day Sybil vulnerability in privacypreserving vehicular peer-to-peer networks. IEEE J. Sel. Areas Commun. **31**(9), 237–246 (2013)
36. Liang, X., Lin, X., Shen, X.: Enabling trustworthy service evaluation in service-oriented mobile social networks. IEEE Trans. Parallel Distrib. Syst. **25**(2), 310–320 (2014)
37. Zhang, K., Liang, X., Lu, R., Shen, X.: Sybil attacks and their defenses in the internet of things. IEEE Internet Things J. **1**(5), 372–383 (2014)
38. Tran, D., Min, B., Li, J., Subramanian, L.: Sybil-resilient online content voting. In: Proceedings of USENIX Network Systems Design and Implementation (NSDI), pp. 15–28 (2009)
39. Reddy, Y.: A game theory approach to detect malicious nodes in wireless sensor networks. In: Proceedings of the 3rd International Conference on Sensor Technologies and Applications (SENSORCOMM), pp. 462–468 (2009)
40. Yu, H., Kaminsky, M., Gibbons, P., Flaxman, A.: SybilGuard: defending against Sybil attacks via social networks. IEEE ACM Trans. Netw. **16**(3), 576–589 (2008)
41. Du, W., Deng, J., Han, Y.S., Chen, S., Varshney, P.K.: A key management scheme for wireless sensor networks using deployment knowledge. In: IEEE INFOCOM 2004, vol. 1. IEEE (2004)
42. Xue, J., et al.: VoteTrust: leveraging friend invitation graph to defend against social network Sybils. In: Proceedings of IEEE Conference on Computer Communications (INFOCOM), pp. 2400–2408 (2013)
43. Wang, G., et al.: You are how you click: clickstream analysis for Sybil detection. In: Proceedings of 22nd USENIX Security Symposium, pp. 241–255 (2013)
44. Yu, H., Shi, C., Kaminsky, M., Gibbons, P., Xiao, F.: DSybil: optimal Sybil-resistance for recommendation systems. In: IEEE Symposium on Security and Privacy, pp. 283–298 (2009)
45. Piro, C., Shields, C., Levine, B.N.: Detecting the sybil attack in mobile ad hoc networks. In: 2006 Securecomm and Workshops, pp. 1–11. IEEE (2006)
46. Mahalle, P.N., Anggorojati, B., Prasad, N.R., Prasad, R.: Identity authentication and capability based access control (iacac) for the internet of things. J. Cyber Secur. Mobil. **1**(4), 309–348 (2013)
47. Granjal, J., Monteiro, E., Silva, J.S.: Network-layer security for the Internet of Things using TinyOS and BLIP. Int. J. Commun. Syst. **27**(10), 1938–1963 (2014). https://doi.org/10.1002/dac.2444
48. Granjal, J., Monteiro, E., Silva, J.S.: Enabling network-layer security on IPv6 wireless sensor networks. In: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, pp. 1–6 (2010). https://doi.org/10.1109/GLOCOM.2010.5684293

49. Brachmann, M., Garcia-Morchon, O., Kirsche, M.: Security for practical coap applications: issues and solution approaches. In: GI/ITG KuVS Fachgesprch Sensornetze (FGSN). Universitt Stuttgart (2011)
50. Granjal, J., Monteiro, E., Silva, J.S.: Enabling network-layer security on IPv6 wireless sensor networks. In: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, pp. 1–6. IEEE (2010)
51. Kent, S.: RFC4302-ipauthenticationheader (2005). https://tools.ietf.org/html/rfc4302
52. Kent, S.: RFC4303-IP Encapsulating Security Payload (ESP) (2005). https://tools.ietf.org/html/rfc4303
53. Shelby, Z., Hartke, K., Bormann, C. The constrained application protocol (CoAP) (2014). https://tools.ietf.org/html/rfc7252
54. Dierks, T.: The transport layer security (TLS) protocol version 1.2 (2008). https://tools.ietf.org/html/rfc5246
55. Granjal, J., Monteiro, E., Silva, J.S.: End-to-end transport-layer security for Internet-integrated sensing applications with mutual and delegated ECC public-key authentication. In: 2013 IFIP Networking Conference, pp. 1–9. IEEE (2013)
56. Kothmayr, T., Schmitt, C., Hu, W., Brnig, M., Carle, G.: {DTLS} based security and two-way authentication for the Internet of Things. Ad Hoc Netw. **11**(8), 2710–2723 (2013). https://doi.org/10.1016/j.adhoc.2013.05.003
57. Young, M., Boutaba, R.: Overcoming adversaries in sensor networks: a survey of theoretical models and algorithmic approaches for tolerating malicious interference. IEEE Commun. Surv. Tutorials. **13**(4), 617–641 (2011). https://doi.org/10.1109/SURV.2011.041311.00156
58. Huang, X., Xiang, Y., Bertino, E., Zhou, J., Xu, L.: Robust multi-factor authentication for fragile communications. IEEE Trans. Dependable Secure Comput. **11**(6), 568–581 (2014)
59. Reardon, J., Goldberg, I.: Improving Tor using a TCP-over-DTLS tunnel. In: Proceedings of the 18th Conference on USENIX Security Symposium, pp. 119–134. USENIX Association (2009)
60. Kwon, E.K., Cho, Y.G., Chae, K.J.: Integrated transport layer security: end-to-end security model between WTLS and TLS. In: Proceedings 15th International Conference on Information Networking, pp. 65–71. IEEE (2001)
61. Rahman, A., Dijk, E.: Group communication for coap. Group (2011)
62. Peretti, G., Lakkundi, V., Zorzi, M.: BlinkToSCoAP: an end-to-end security framework for the Internet of Things. In: 2015 7th International Conference on Communication Systems and Networks (COMSNETS), pp. 1–6. IEEE (2015)
63. Park, N., Kang, N.: Mutual authentication scheme in secure internet of things technology-forcomfortablelifestyle. Sensors. **6**(1), 20–20 (2016)
64. Henze, M., Wolters, B., Matzutt, R., Zimmermann, T., Wehrle, K.: Distributed configuration, authorization and management in the cloud-based internet of things. In: 2017 IEEE Trustcom/BigDataSE/ICESS, pp. 185–192. IEEE (2017)
65. Zhou, J., Cao, Z., Dong, X., Vasilakos, A.V.: Security and privacy for cloud-based IoT: challenges. IEEE Commun. Mag. **55**(1), 26–33 (2017)
66. Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., Alonso-Zarate, J.: A survey on application layer protocols for the internet of things. Trans.. IoT Cloud Comput. **3**(1), 11–17 (2015)
67. Scott, C., Wolfe, P., Erwin, M.: Virtual private networks, ser. Animal Series. O'Reilly, Bejing (1999)
68. Granjal, J., Monteiro, E., Silva, J.S.: Application-layer security for the WoT: extendingCoAPtosupportend-to-endmessagesecurityforinternet-integrated sensing applications. In: International Conference on Wired/Wireless Internet Communication, pp. 140–153. Springer, Berlin/Heidelberg (2013)
69. Liu, C.H., Yang, B., Liu, T.: Efficient naming, addressing and profile services in Internet-of-Things sensory environments. Ad Hoc Netw. **18**, 85–101 (2014)
70. Conzon, D., Bolognesi, T., Brizzi, P., Lotito, A., Tomasi, R., Spirito, M.A.: The virtus middleware: an xmpp based architecture for secure iot communications. In: 2012 21st International Conference on Computer Communications and Networks (ICCCN), pp. 1–6. IEEE (2012)

71. XMPP Standards Foundation. XMPP. [Online]. http://xmpp.org/
72. OSGi Alliance. OSGi main. [Online]. http://www.osgi.org
73. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain technology: beyond bitcoin. Appl. Innov. **2**(6-10), 71 (2016)
74. Double-Spending—Bitcoin WiKi, Mar. (2016). [Online]. Available: https://en.bitcoin.it/wiki/Double-spending
75. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper. **151**(2014), 1–32 (2014)
76. Cachin, C.: Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310, pp. 4 (2016)
77. Understanding Public Key Cryptography. [Online] (2005). Available: https://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx
78. Zheng, Z., Xie, S., Dai, H.N., Wang, H.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **2016**, 1–25 (2016)
79. TransActive Grid, Mar. (2016). [Online]. Available: http://transactivegrid.net/
80. Rutkin, A.: Blockchain-based microgrid gives power to con-sumers in New York (2016). [Online]. Available: https://www.newscientist.com/article/2079334-blockchain-based-microgrid-gives-power-to-consumers-in-new-york/
81. Otte, P., de Vos, M., Pouwelse, J.: TrustChain: a Sybil-resistant scalable blockchain. Futur. Gener. Comput. Syst. (2017) https://doi.org/10.1016/j.future.2017.08.048
82. Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ECDSA). Int. J. Inf. Secur. **1**(1), 36–63 (2001)

Pardeep Kaur is a Research Scholar in CSE at Chitkara University (Baddi (Himachal Pardesh)), India. In 2016, she received her Bachelor degree in CSE from Shaheed Udham Singh College of Engineering & Technology, Mohali. In 2019, she completed a 2 month internship on the project 'E-Voting system using blockchain' at the National Chung Cheng University, (Chiayi (Taiwan)). Her current areas of interest are blockchain and the Internet of Things.

Shalli Rani is Associate Professor in CSE at Chitkara University (Rajpura (Punjab)), India. She has 14+ years teaching experience. She received her MCA degree from Maharishi Dyanand University, Rohtak in 2004, her M.Tech. degree in Computer Science from Janardan Rai Nagar Vidyapeeth University, Udaipur in 2007, and her Ph.D. degree in Computer Applications from Punjab Technical University, Jalandhar in 2017. Her main areas of interest and research are Wireless Sensor Networks, Underwater Sensor networks and the Internet of Things. She has published/accepted/presented more than 35 papers in international journals/conferences. She has worked on Big Data, Underwater Acoustic Sensors, and the IoT to show the importance of WSN in IoT applications. She received a young scientist award in Feb. 2014 from Punjab Science Congress, in the same field.

Caching Policies in NDN-IoT Architecture

Divya Gupta, Shalli Rani, Syed Hassan Ahmed, and Rasheed Hussain

1 Introduction

Nowadays, the Internet is the most popular tool all over the world. With the advancements in technology over time, the evolution in traditional Internet has been realized. The evolution in Internet is mostly due to changes in user requirements, number of users and applications, usage patterns, and nature of applications. The connection of large amount of physical objects to an Internet at an unprecedented rate leads to the generation of new paradigm known as the Internet of Things (IoT) [14]. The vision of IoT is to transform traditional objects to smart by enabling them to hear, think, see, and talk together to perform jobs. The interconnection of such a huge number of heterogeneous devices results into increased magnitude of no. of objects found in current Internet, which may include devices such as sensors or systems including HVAC monitoring or learning thermostats, each individually acting as a host or router in a spontaneous network such as ad hoc networks or wireless sensor networks (WSN). Generally, all the things are tiny devices with limited resources in terms of battery life, memory, and processing speed. The set of protocols, e.g., 6LoWPAN, have been proposed by the Internet Engineering Task Force

D. Gupta · S. Rani (✉)
Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India
e-mail: divya.gupta@chitkara.edu.in; shalli.rani@chitkara.edu.in

S. H. Ahmed
Department of Computer Science, Georgia Southern University, Statesboro, GA, USA
e-mail: sh.ahmed@ieee.org

R. Hussain
Institute of Information Security and Cyber-Physical Systems, Innopolis University, Innopolis, Russia
e-mail: r.hussain@innopolis.ru

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_3

(IETF), Institute of Electrical and Electronics Engineering (IEEE), and IP-based standardized bodies to make WSN work coherently with Internet connections and other network types [5]. Host-centric approach where devices need to share IP addresses before communication starts posing a challenge in deploying IP-based IoT solutions for a large number of devices. However, more than half of Internet traffic is mainly produced by content-centric applications such as iTunes, YouTube, Facebook, Twitter, WhatsApp, Amazon, Netflix, etc. [30]. Moreover, users of such applications are concerned about requested data irrespective of location from where data is being generated. Each day evolution of content-centric applications failing Internet design as it was not designed for distribution network. To this reason, researchers explored information-centric networking (ICN) as a clean slate, innovative approach to transform Internet [4]. Unlike host-centric approach of IP-based communication model, ICN provides content as a first-class citizen of the whole network. Nodes in ICN network need to specify what they want and not where it should be.

In this arena, named data networking (NDN) has rapidly gained interest and come as a promising candidate due to its simple, beyond end-to-end connection communication. The benefits associated in terms of reliable, efficient data delivery, content security, and in-network caching have raised NDN as a forthcoming networking solution for Internet of Things (IoT) challenges. With NDN, the consumer demands the content by sending content name in network, which further routes requests toward nearby copies of demanded content using content names (not IP addresses). This makes use of in-network caching an important feature for NDN as it not only will reduce content retrieval latency but also support less network bandwidth utilization as well as reduced network traffic. The analysis reports in [34] present less utilization of 2.02 hops on an average for 30% of request packets using content-centric in-network caching. Since caching is not a new tool introduced by ICN and is already employed by current Internet to reduce network bandwidth, it lacks in identification of identical objects which makes it difficult to take caching advantages. Although caching techniques and methods for cache optimization have been discussed and studied earlier, new features of NDN-IoT caching such as transparency, ubiquity, and granularity have made use of earlier caching techniques unable to be directly implemented on NDN-IoT. To make best use of in-network caching in NDN-IoT, many caching techniques have been proposed by networking community in the past years. In this paper we discussed several NDN-IoT caching algorithms with overview to their strategies, advantages, parameters evaluated, and simulators used for study.

In particular, our contribution to this paper is the following: Sect. 2 listed various challenges related to caching in IoT using IP architecture. Section 3 presented support of NDN in IoT to meet various challenges mainly focusing on caching. Section 4 provides overview on the NDN study. Further to detail, the various caching schemes introduced by different research groups/individuals in the field of NDN-IoT have been listed in Sect. 5. The research issues related to NDN-IoT caching have been presented in Sect. 6, and finally Sect. 7 concludes the paper.

2 Caching in IoT: A Challenge

The communication in TCP/IP demands availability of both consumer and provider at the same time. However, to provide energy efficiency in IoT, resource-constrained nodes might go in sleep mode. Moreover, IoT's dynamic and mobile environment provides no guarantee of stable connections among communication authorities. Consequently, energy-efficient data dissemination in IoT mostly relies on caching and proxing. In proxing, any node acting as proxy may request data and can store response for request temporarily on behalf of sleeping node until it wakes up. The cached content can be served to other nodes that are requesting the same content and sharing the same proxy so as to reduce response delay and better network bandwidth utilization. With its usefulness, IoT suffers several limitations to caching implemented by CoAP and HTTP at the application layer [32]. To list few, (i) in order to utilize caching facility, each client has to explicitly choose proxy node (forward or reverse) as caching points deployed earlier may or may not be optimal anymore. The client node makes use of resource discovery mechanism to choose proxies which add in to system complexity. (ii) In a highly dynamic environment with intermittent connectivity, pre-configured (pre-selected) proxies may go out of reach. With change in network topology, the client has to re-configure proxies or has to stop using caching capability of network. (iii) The protection of application data becomes very hard in the case of loss of end-to-end connection between cache and proxy. For efficient and flexible caching for an IoT environment, the network architecture must support caching inside the network without any configuration requirement for an application. Further to this, the network layer should be aware of all application layer resources, and the caching feature has to be incorporated under forwarding layer so as to maximize cache utilization by each interest packet traversing through the network. In addition, the secure and trustworthy in-network cache demands some fundamental changes in IoT security model.

3 NDN in IoT

To meet challenges faced by host-centric IoT communications, a new IP-independent communication model known as named data networking (NDN) has emerged recently under the roof of information-centric networking (ICN). NDN has rapidly gained interest and came as a promising candidate due to its simple, robust, beyond end-to-end connection communication. Researchers explored NDN as a clean slate, innovative approach to transform Internet [4]. Unlike, host-centric approach of IP-based communication model, NDN provides content as a first-class citizen of the whole network. Nodes in NDN network need to specify what they want and not where it should be. For this reason, NDN has been introduced as one of the future

Table 1 IoT requirements and native NDN support

S. no.	IoT challenges	NDN support
1	Scalability	Hierarchical application-specific names
2	Robustness	In-network storage, anycasting, interest aggregation
3	Security	Data authentication, content integrity, per packet signature, encryption possibility
4	Reliability	Multi-path routing, retransmission of interest from the actual consumer, intermediate node retry
5	Heterogeneity	Customized forwarding and caching strategies, unbounded namespace
6	Mobility	Receiver-driven connectionless communication, location-independent names, any node data retrieval
7	Energy efficiency	Aggregation, in-network storage, anycasting

Internet architecture (FIA) taken from the broader field of content-centric networking (CCN) [43] proposed by Van Jacobson at Xerox PARC [8]. In NDN, content is mapped using names instead of mapping to host location resulting in better performance, security, and network scalability. In addition, support for multicasting, in-network caching, and scalability is present as incorporated features of NDN. The NDN for IoT is preferred due to its low power and complexity requirements, and benefits of incorporating NDN in IoT have been highlighted by many researchers in literature [1]. The support of NDN to fit inherent requirements of IoT is shown in Table 1. Shang et al. [31] specified how NDN addresses IoT challenges and way for implementing IoT using NDN. A lot of work has been done in the past focusing on the incorporation of NDN into IoT for different applications and addressed several challenges being offered by NDN-IoT integration. Out of all, some works use NDN/CCN hierarchal naming feature for deploying sensors and collecting data from a specific application. The implementation of IoT using small packet size offered by NDN as well as in-network caching is highly beneficial in terms of deployment of energy-efficient IoT systems. The NDN's in-network caching feature is most preferred and beneficial for utilizing maximum network performance in terms of reduced response delay, low bandwidth, reduced network traffic, and congestion control and energy efficient for resource-constrained devices. Therefore, NDN architecture is considered as a promising solution for addressing features, challenges, and requirements of IoT system as well as for resolving issues related to IP-based IoT networks.

4 Overview of NDN

This section presents the basics of NDN in terms of discussion related to its architecture, data structures associated with each NDN router, as well as forwarding mechanism of named networks.

4.1 NDN Architecture

In today's world, the Internet architecture centers on network layer. Both NDN and IP share a common narrow-waist architecture [4] (refer to Fig. 1). Corresponding layers perform the different functions even though they share the same layer. The network layer in NDN supports scalability, efficiency, security, and reliability. In traditional IP-based standards, data is exchanged after connection is established between end-to-end nodes resulting in state-full routing but stateless forwarding [40]. It does not provide any facility to recover from the link failures; rather it tends to establish a new connection with the node. NDN stack introduced security and forwarding as two new layers in NDN stack. The strategy layer in NDN provides state-full forwarding as nodes themselves choose alternate path to forward packets if some kind of failure occurs. Irrespective of channel security provided by IP where data is forwarded on a secured channel, NDN provides content security by signing data packets with producer key to provide authentication as well as secure communication [17]. NDN is a purely receiver-driven communication model [4] which provides simple and robust communication by taking into account two types of exchange packets, interest packet and data packet, which themselves carry hierarchical, application-specific content names. The communication in NDN gets started by the consumer who sends an interest packet. It carries the requested content name, which is then forwarded by intermediate nodes until it reaches the destination node or requested content is not received. The provider node responds via data packet by sending the requested content back to the consumer. Data packets usually carry the requested name and content signed by producer key to provide authentication to data when received by the consumer. Data packet travels back on the same path followed by the interest packet [2]. Figure 2 represents the interest packet and data packet format in NDN.

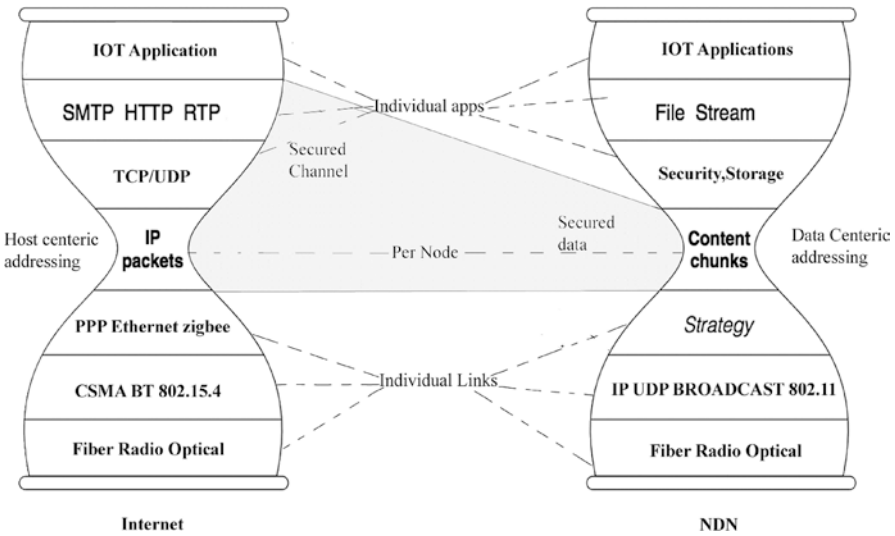


Fig. 1 NDN hourglass architecture

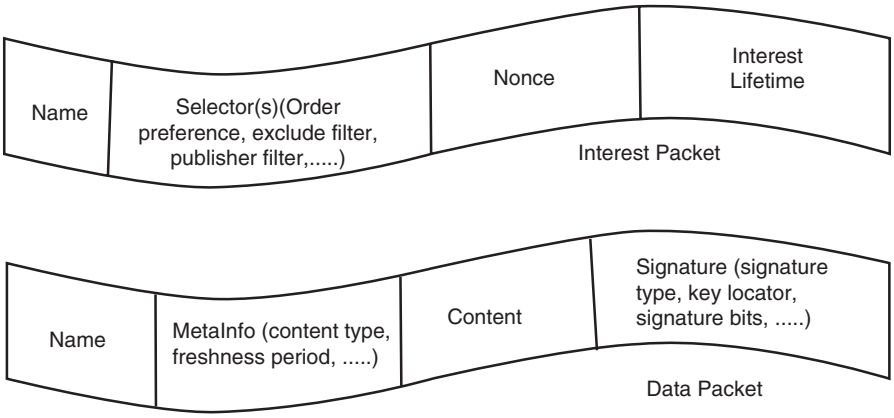


Fig. 2 NDN packet format

4.2 NDN Routing Data Structure

Nodes present in network carry out the routing of interest packets and data packets in NDN where each node acts as a router to route the packet upstream and downstream based on some forwarding strategies. To route the packets to the next intermediate node, each node in NDN maintains three data structures [42].

Content store (CS) Content store act as a cache and store the data packets in order to fulfill any future requests if comes for same content. The amount of data cached per node depends upon the size of cache. Regardless of IP-based point-to-point communication where packet losses its value once transferred, NDN provides in-network caching by caching data at each node in NDN network. The data packets stored in CS help to reduce network latency by providing data closer to the consumer, and packets need not to travel upstream to the producer. This results in less utilization of upstream bandwidth as well as congestion control in network. The decision of whether caching or not and, if yes, where to store in the case of cache full generates a need of caching strategies for NDN communication based on requirement of applications.

Pending interest table (PIT) PIT holds record of all interest transmitted by node and for which data has not yet been delivered. After CS lookup (if content is not found in cache), interest packets travel toward PIT where an entry is created recording its name and incoming/outgoing interfaces. Data packet has to follow reverse path followed by interest packet when it becomes available. PIT management is a vital factor in NDN as data packets are sent back to the original consumer without any further processing at intermediate nodes. The entry from PIT purged if data is received by node or if PIT timer expires even if data is not received. The PIT in NDN router holds a pending interest for a specific time and sends NACK in case interest is not being satisfied due to some link failure and congestion or if no corresponding entry is found in FIB. The original consumer on receiving a NACK

may decide to retransmit the request to other interfaces to find another path. NDN avoids loops as data packets follow the reverse path traversed by interest packet and Nonce in PIT helps routers to identify and discard looping interest packets if any allowing them to use multiple paths freely toward the same producer. The PIT in NDN serves other purposes as multicast delivery by sending data to all interfaces who requested for it, congestion control by sending at most one data packet per interest, and managing router load by limiting the size of PIT.

Forwarding information base (FIB) FIB maintains outgoing interfaces and forward packets based on some strategies. After PIT lookup (adding interface in PIT), interest travels toward FIB which contains prefixes of names and list of interfaces representing the possibilities where the producer could be. Regardless of IP-based communication where there is a single interface per prefix name, NDN provides multiple output interfaces per prefix. The FIB looks for the longest prefix match and, after the match, decides on which interface of that respective prefix packet has to be forwarded. As a number of interfaces present for a single prefix match, forwarding of packet to which particular interface leads to generation of a number of forwarding strategies based on requirement of application.

4.3 NDN Forwarding

The forwarding process at each node when it receives a packet from any intermediate node is shown in Fig. 3.

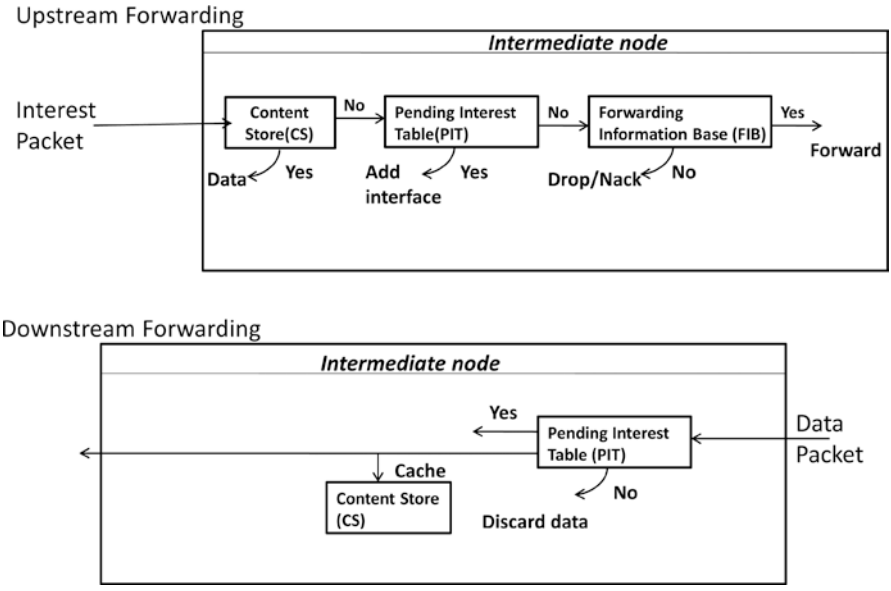


Fig. 3 Packet lookup, storage, and forwarding process

Upstream forwarding Upon receiving an interest by intermediate node, it first checks its content store. If a matching name is found in CS, then content is sent back to the consumer in the form of data message by the intermediate node, and interest packet need not to travel upstream further. If a matching name does not exist in CS, then PIT gets checked by node. If found in PIT with the same name and different Nonce (random number generated per interest packet), then the node does not forward packet upstream as already some other consumer has requested for the same content earlier and the node aggregates interface of this consumer in previous PIT entry with the same interest name and will send data to both consumers when it becomes available. If found with the same name as well as Nonce, the packet is treated as retransmitted packet and got discarded. If not found in PIT, the node adds new entry with content name, Nonce, incoming interface (the interface from which interest packet is received by the node), and outgoing interface in its pending interest table and forward packet to FIB. If a matching prefix is found in FIB, the packet is forwarded to the associated outgoing interface based on forwarding strategies; otherwise the packet is discarded.

Downstream forwarding The data packet is sent back on the same path travelled by the interest packet. On receiving a data packet by any intermediate node, it first checks for the content name in its PIT; if not found, the packet is simply discarded; otherwise, the packet is sent downstream on the interface from where the interest packet was received. The data packet is stored by node in its CS to fulfill future requests for the same content if any comes and removes the entry from PIT. The entry from PIT is purged if data is received by the node or if PIT timer expires even if data is not received. PIT timer is a predefined time for which an entry must exist in PIT and is referred to as PIT entry lifetime (PEL).

5 Caching in NDN-IoT

Intrinsically, the present Internet is intended to send all requests for the same content toward original source that increases network congestion, network load, response latency, bandwidth consumption, and retrieval delay. Moreover, the present Internet does not provide any support for data dissemination as well as for quick content retrieval. To overcome the issues related to present Internet, content-centric networking was proposed. Caching the content within the network at intermediate nodes called in-network caching is fundamental and an important feature of content-centric, peer-to-peer network model of NDN. For NDN-based IoT, content caching is highly demanded for dissemination of information toward edges with low cost. Some IoT applications demand fresh content with some time constraint, and some require content to be replaced with availability of new versions. For example, the value of room temperature needs continuous monitoring and updation. Therefore, caching is implemented at the network layer to directly deal with named information. Content caching in NDN comes with various benefits. By caching contents from different producers, the content gets dislocated from the original source, and hence,

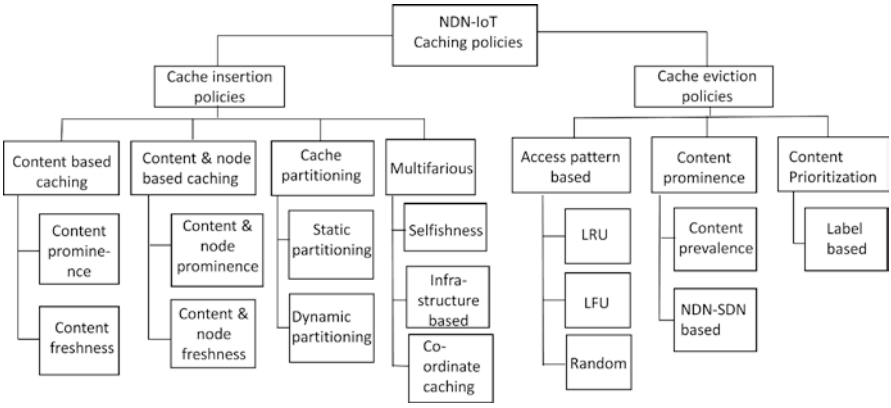


Fig. 4 Classification of different NDN-IoT caching policies

location-independent delivery of content is achieved. Energy-efficient communication is supported for resource-constrained devices, and support for mobility is attained. It leads to better network performance by storing multiple copies of the same content at different locations and thus avoids single point of failure. Subsequently, it provides significant benefit to control network congestion by reducing overhead at producer. Further, it helps a lot to reduce network traffic load and content retrieval delay. For efficient content caching in network, cache decision policies are used to determine whether the content will be cached at intermediate nodes or edge nodes or somewhere else. The implementation of different caching policies is followed by several caching algorithms. The caching algorithms must be intelligent enough to answer the following two questions: Where to cache the content? Which content will be replaced first in case of cache full? Based on the solution to the abovementioned questions, we have classified NDN-IoT caching policies into two broad categories: cache insertion policies (decide if the content is to be cached in network or not) and cache eviction policies (decide replacement of content at router cache) (refer to Fig. 4). In addition to the merits offered by caching, it also undergoes through various complications and restrictions for design of NDN-IoT-based caching policies. In the following subsection, we will discuss several cache insertion policies along with cache eviction policies.

5.1 Cache Insertion Policies

These policies mainly refer to the strategies adopted by caching equipments for caching the contents according to some properties such as content, content and node popularity, freshness, etc. The Cache All [19] (also refers to Leave Copy Everywhere (LCE) and Cache Everything Everywhere (CEE)) is inbuilt cache insertion policies in design of NDN. With the aim to reduce retrieval latency as well as traffic load in network, the response for request is cached by all the intermediate nodes in the path

between the sender and receiver. The scheme is simple but has resulted in redundancy in network due to multiple copies of the same content. Some existing cache insertion policies to reduce redundancy for better utilization of caching resources are Leave Copy Down (LCD), Leave Copy with Probability (LCProb), and Leave Copy with Uniform Probability (LCUnip). LCD reduces the redundancy by allowing only few intermediate nodes to cache content based on cache hit. Using LCProb [44], the content can be cached using the probability of 1/hop count, and LCUnip [41] allows content to be cached using uniform probability.

For NDN-IoT environment, efficient design of caching policies must take into account the content properties and node properties. The properties for content that need to cache may include content freshness, popularity, timings, and particular source, whereas properties for node that intend to cache content can include battery power, memory, processing time, and distance from producer. Based on the following observations, we have further classified cache insertion policies into four subcategories:

(i) Content-based caching – Based on the properties of content, these policies decide which content should be cached and what not.
(ii) Content- and node-based caching – Based on the properties of content and node, these policies decide whether node should cache the content or not.
(iii) Cache partitioning – Based on the type of IoT application, these policies decide whether there is a need to assign specific cache slot or not.
(iv) Multifarious –These policies include all the algorithms designed on the basis of different parameters such as network/node infrastructure, node selfishness, as well as combined coordinated caching approaches.

As depicted in Fig. 4, cache insertion policies are further categorized into content-based caching, content- and node-based caching, cache splitting, and multifarious. To get deeper view of caching literature, we have further classified these schemes into several categories such as content-based caching has been classified on the basis of content freshness and prominence and content- and node-based caching into freshness and prominence of both content and node and cache partitioning is further categorized on the basis of either static or dynamic splitting and multifarious caching into selfishness, infrastructure-based, and coordinate caching.

Content-based caching for NDN-IoT Mostly IoT applications before caching put some restrictions based on content type. Some need content with some freshness, while other may demand content with prominence. In this following subsection, we will present NDN-IoT-based caching policies for making caching decision dependent on properties of content.

Content prominence For implementing content prominence caching, each router in network maintains access frequency of prominent contents with the help of previous request statistics. With the aim to minimize traffic load and number of access hops travelled by request packet in dynamic network, Li et al. [23] proposed caching

schemes to cache frequent content on selected routers. The proposed schemes show significant improvement over existing schemes such as CEE, LCD, LCProb, and LCUnip. Further as an improvement to previous work, Li et al. [22] extended their work by presenting three coordinated caching schemes for inserting contents in cache and proved better results if compared to LCE.

Wu et al. [37] proposed fame-based coordinated caching plan known as effective multipath caching (EBC) for wiping out excess data traffic from the core network so as to reduce inter-ISP traffic and retrieval latency. This policy plans to place replica based on the present request statistics as well as utilized the worldwide popularity of content for caching placement decision. The proposed scheme outperformed CEE and LCProb policies. The storage cost, processing time, and communication cost are the main overhead associated with content prominence-based coordinated caching policies. Further, to reduce both inter-domain and intra-domain traffic of NDN network, the author proposed distributed caching with coordination (DCC) [38]. In DCC, worldwide popularity of content is calculated using sum of weighted popularity of the same content at different routers and is considered as a measure for cache decision. The proposed scheme performed well as compared to CEE and random cache. Cho et al. [9] proposed caching policy known as WAVE in which whole information is segmented into small chunks and is stored in a balanced manner among network routers based on popularity of contents. For this policy, the quantity of chunks stored by each router is recommended by its upstream router with the help of cache recommended flag bit in each data packet to make cache decisions. The policy results in less duplication with high cache hit ratio.

Baugh et al. [7] proposed per-face popularity (PFP) caching policy to protect popular cache items from cache pollution attacks and to build high cache robustness. They have normalized per-face contributions so that interest requests arriving from any face have no influence on popularity than different faces. Based on this, only items with some legitimate popularity remain as content of cache, spoke across all routers. The simulation results proved its effectiveness for cache pollution attacks against various standard techniques such as LCE, LRU, and FIFO in terms of cache hit and in preserving popular items.

Further to present performance comparison of different caching policies, Hail et al. [16] applied always and probabilistic caching with probability = 0.5 for NDN-IoT environment. For replacement of cache, LRU and random replacement algorithms were utilized. Simulations were carried out with total 36 nodes (4 consumer nodes, 6 random producers) in ndnSIM and ns-3. Results proved higher cache hit, reduced retrieval latency, and retransmissions when both probabilistic and LRU were used in combination. The combination ensures availability of latest content in network as an important IoT requirement. To judge caching benefit, always caching with probability = 1 [6] was evaluated on RIOT OS. The results from both policies go in favor of caching content for IoT network even for small devices with small CS and memory.

Content freshness Some IoT applications demand fresh content with some time constraint, and some require content to be replaced with availability of new versions. For example, the value of room temperature needs continuous monitoring and timely updation. Therefore, caching policies dealing with content freshness are important for NDN-IoT applications. In this manner, Quevedo et al. [27] proposed caching policy to facilitate applications demanding content with specific freshness index. Any consumer inquiring the content needs to send interest packet with desired freshness value. For this, a new field named as freshness parameter has been added to interest packet with some modifications. The availability of freshness parameter ensures quality of data being fetched as well as control of consumer on data. By adding a ratio of active time of restrictive in freshness consumer to active time of less restrictive in freshness consumer, caching performed better for IoT applications that need recent data.

Content- and node-based caching for NDN-IoT For NDN-IoT environment, efficient design of caching policies must take into account the content properties and node properties. The properties for content that need to cache may include content freshness, popularity, timings, and particular source, whereas properties for node that intend to cache content can include battery power, memory, processing time, and distance from producer. In the following subsection, we will discuss caching policies that consider both content and node properties.

Caching based on content prominence and node properties Vuralet et al. [35] proposed caching policy considering both content and node parameters. The routers in network were responsible for computation of content probability using content properties such as freshness, rate of request, and node properties such as location of node, battery power, and rate of request. The above scheme was implemented in MATLAB with 40GB link for multimedia applications. As extensive calculations are required, this scheme was less preferred for IoT networks with high mobility due to the presence of resource-constrained IoT devices. The scheme could be implemented on static networks as devices in such networks do not face any battery or power issues for complex calculations.

Caching based on content freshness and node properties Hail et al. [15] presented a probability-based caching policy for IoT applications known as pCASTING considering both content and node properties. The freshness of content and battery of node were considered as parameters for making cache decisions. The scenario of 60 nodes with 1 producer and 8 consumers was simulated in ndnSIM and ns-3. The effectiveness of proposed caching was evaluated against several existing cache policies such as CEE, caching with probability, and no caching. The scheme presents significant improvement in terms of cache hit and number of packet received. However, from the results, proposed policy observed more retrieval delay than CEE but less than the other two.

Cache splitting As each router in network utilizes capacity constraint, so to maximize the network performance in terms of cache hit ratio, the idea was to isolate

reusable contents from non-reusable one. To achieve high cache performance, the cacheable contents of some applications such as audio, video, pictures, websites, etc. were stayed away from being supplanted by noncacheable contents such as messages, emails, telephony apps, etc. Cache splitting was examined under network traffic for implementation of idea. Each CS from all nodes has been divided into two different traffic divisions, i.e., constant bitrate (CBR) utilized for multimedia streaming applications and non-CBR for the rest of applications.

Static and dynamic partitioning From this view, Rezazad et al. [29] proposed two kinds of cache splitting: static and dynamic splitting. Static partitioning divides cache among fixed, non-sharable slots and dynamic divides cache among fixed but sharable slots. With dynamic cache, any traffic division may use another division's cache if not needed at that time by its respective class. The authors of the scheme implemented the concept of dynamic partition using cache miss equation which is mainly utilized for splitting databases. The scheme was proposed to reduce cache miss probability for all NDN traffic types, and results proved less cache miss using dynamic partitioning. Further to exploit the full potential of network's inbuilt caching capability, Wang et al. [36] proposed collaborative in-network caching scheme with content-space partitioning and hash routing (CPHR). After successful partitioning of contents and allotment of contents to caches, CPHR become able to constrain the path extend by hash routing. They have formulated cache partitioning issue to optimal network hit ratio and proposed heuristic approach as solution. CPHR presents significant overall hit ratio (about 100%) when evaluated against LRU.

Multifarious caching In this section, we offer a comprehensive summary of caching schemes that don't target a selected methodology (i.e., content-based, node-based caching and cache partitioning) however gift caching for IoT from alternative views. We tend to categorize these NDN-based caching ways for IoT into selfishness, infrastructure-based caching, and coordinate caching policies. Although NDN-based caching node design bestowed isn't specifically for IoT, we embrace it to address the disaster management of IoT network.

Selfishness Hu et al. [18] projected a Not So Cooperative Cache (NSCC) policy where a self-seeking node can cache only if caching results in reduced access price of its own by obtaining the information from either its native local or neighbor cache. The policy mainly concerns on seeking which contents to cache, so as to provide low access price for every node. To achieve this, every self-seeking node in NSCC holds four elements, interest/data processor, request rate measure, reckon cache, and native cache. Interest/data processors are responsible for processing interest packets and for keeping track of content's native prominence. Request rate measuring is the one that shares this native prominence with alternative NSCC nodes as well as learns widespread prominence contents of other nodes. The request rate measuring system provides a read of content's prominence to the reckon cache. The reckon cache mainly focuses to seek out what content ought to be cached by local/alternate nodes. To seek out the world object placement at NSCC nodes,

reckon cache uses a scientific theory approach (each node acts severally and avariciously caches most well-liked contents) developed by [21]. Native cache holds the contents urged by reckon cache. The results of simulations proved that the projected theme (greedy NSCC nodes) achieves higher cache hit ratio if compared to NSCC nodes.

Infrastructure based The authors in [24] proposed a plan of overlay shared caching by introducing content management layer in fixed and mobile converged (FMC) specification. The producer of content or network supplier will be responsible for the management/control of this layer. CM layer decides wherever content will be cached about victimization and information management policies. Unified Access Gateway (UAG) node in FMC network is designed to cache and forward contents to a requesting node. A cache controller (CC) in integration to UAG provides optimum caching and pre-fetching plans. A value-added config packet is present within the CCNx to hold data concerning caching and cache replacement theme. Updated CCNx provides transparency in overlay caching and for pre-fetching method. Cache controller sends config packet to cache node and that reciprocally sends interest packet to overlay cache which in turn responds with the desired data packet. Higher system performance is achieved due to less packets received by the original server as additional packets are responded by overlay caching.

Coordinated caching Some authors have facilitated caching with the routing, forwarding, PIT, or security to extend the NDN Forwarding Daemon (NFD) performance. In this manner, Choi et al. [10] have planned coordinated routing and caching (CoRC) theme to attenuate the impact of scalable routing and to extend the in-network caching potency. Dehghan et al. have analyzed TTL-based caching schemes with PIT based on two different categories, wherever the timer might be set just the once or be reset with each individual content request.

Yao et al. [39] have projected a caching arrange obsessed on CCN mobility prediction. This paper is placed within the CCMP possibility that caches the thought contents at heaps of transportable nodes which will visit an analogous hot spot territories occasionally. PPM (prediction by partial matching) is used to anticipate the quality nodes' probability of achieving various problem space regions obsessed on their past directions. A cache eviction obsessed on content prominence to make sure solely prominent contents are cached is likewise projected.

Shi et al. [33] proposed cache aware routing setup in mobile social network (MSN) captivated with ICN for transportable structure. A concept referred to as interest routing (IR) is devised among nodes. To trade contents with the content requester, data routing (DR) setup is employed, imaginary subject to the counseled intimacy approximations among nodes. An in-network caching (IC) policy is devised to react to the approaching further requests, and it will receive the less reaction immobility than the traditional transportable MSN routing plans. The projected scheme shows better performance in terms of less network burden and high message delivery magnitude over different existing ones.

5.2 Cache Eviction Policies

The cache eviction approach is mandatory for taking decision regarding evacuation of the current cache contents to make room for fresher ones. Trade methodologies are necessary for carrying out effective cache mechanism. This approach evacuates the obsolete cache information and gives area to the new approaching data. Based on this, we have categorized cache eviction policies into access pattern-based caching, content prominence, and content prioritization. To get deeper insight of different eviction approaches, we have further classified these policies such as access pattern-based policies into Least Recently Used (LRU), Least Frequently Used (LFU), random, and Less Flexibility First (LFF) based on their usage frequency. Subsequently, content prominence is further classified on the basis of content prevalence and NDN-SDN and content prioritization on label basis.

Access pattern-based caching In this subsection, we will discuss cache eviction policies that are used as most frequent replacement processes. A most common used eviction approach is Least Recently Used (LRU) [25] where least recently utilized content is substituted by newly arrived content. This approach is commonly used due to increased cache hit ratio by storing most recent data for more time. Another most often utilized cache eviction policy is Least Frequently Used (LFU) [13] due to the fact of its arrangement of evacuating the less frequently utilized contents first. The LFU works by storing popular objects for more time to achieve high interest satisfaction. Each node with LFU keeps track of the requests being satisfied by a particular data object, and the item with lowest frequency is substituted. The decision-making time for these techniques depends on the content material substitution and content arrival on router. For complex data structures, the use of random cache eviction is recommended [26]. In random eviction policy, the item to be replaced is selected randomly on the arrival of new content. With random policy nodes do not need to manage request state information which saves both memory and cost. The authors in [18] proposed Least Value First (LVF) [3], a new cache eviction policy where replacement of content is subjected to content retrieval delay, content prominence, and content age. The results of experiments proved the effectiveness of the proposed policy over FIFO and LRU in terms of cache hit, network delay, and hit timings (Table 2).

Content prominence In a mobile network with low intermittent connectivity, caching plays a vital role for better network performance. The current NDN-IoT environment has shown progressive move toward caching utilizing both cache insertion and eviction. In the past years, content prominence has been utilized for the design of various cache policies. Access pattern-based cache eviction policies are not fit for utilizing content popularity in NDN networks. The design of efficient caching eviction algorithms based on content prominence is highly recommended for NDN-IoT. To address issue related to performance of cache in NDN-IoT network, Ran et al. [28] proposed cache eviction scheme based on content prevalence.

Table 2 Summary of selected caching strategies in NDN-IoT

Caching category	Caching subcategory	Authors	Caching strategy	Eviction policy	Architecture	Comparison	Simulators
Cache insertion policies							
Content based	Prominence	Li et al. [22, 23]	AsymOpt	None	NDN	CEE, LCD, LCProb and LCUnip	GT-ITM toolkit
		Wu et al. [37, 38]	Distributed coordination caching	LRU	NDN	CEE, Rand-cache	Ambilence, GEANT
		Baugh et al. [7]	Per face popularity (PFP)		ICN	LCE, FIFO, LRU, LFU	ndnSIM
	Probability	Hail et al. [16]	Dynamic probability	LRU, Rand-Cache	NDN	Always and probabilistic caching	ndnSIM, ns-3
		Baccelli et al. [6]	Constant probability		CCN	Always and no caching	RIOT OS
	Freshness	Quevedo et al. [27]	Different freshness	LRU	CCN	IP	ndnSIM, ns-3
Content and node based	Prominence and node property	Vural et al. [35]			NDN-IoT		MatLAB
	Freshness and node property	Hail et al. [15]	pCASTING	LRU	NDN	CEE, probabilistic and no caching	ndnSIM, ns-3
Cache splitting	Static and dynamic splitting	Rezazad et al. [29]	Cache miss	LRU, Rand-cache	NDN	Shared CS	Java
	Content splitting	Wang et al. [36]	CPHR	Perfect-LFU	ICN	LRU	NS3
Cache eviction policies							
Content based	Prominence	Ran et al. [28]	CCP-CPT	Not applicable	NDN	LRU, LFU	ndnSIM
		Kalghoum et al. [20]	NC-SDN	Not applicable	NDN-SDN	LFU, LRU, FIFO	ndnSIM, ns-3
	Prioritization	Dron et al. [12]	Infomaximizing	Not applicable	NDN	LRU, IC	ns-3

The content prominence (CCP) for cache eviction policies has been facilitated at each node by maintaining a data structure holding content names with its prominence. For the same, they added a table called Content Prevalence Table (CPT) in content store to record information such as content name, cache hit, and present and previous prominence. The CCP periodically calculates the prominence of content based on content access rate and cache hit and replaces content with minimum prominence during cache eviction. The experimental results proved better performance of proposed policy if compared to LRU and LFU. However, updating CCP periodically consumes a lot of CPU time and memory and was not recommended for large-scale networks with resource-constrained devices. In order to minimize resource consumption at routers, Dai et al. [11] proposed the use of space-efficient bloom filter technique for calculating online content prominence.

Kalghoum et al. [20] have proposed a cache eviction algorithm dependent on SDN (software-defined networking) called NDN-SDN. The proposition depends on the content prominence figuring done by the changes to clarify a cache substitution technique. The NDN-SDN integration builds the hit proportion and diminishes the bandwidth consumption, subsequently upgrading the NDN network execution.

Content prioritization To reduce content retrieval latency in NDN network, content prioritization has shown progress toward NDN caching just like content prominence. The arrangement relies on assigning priority to different contents for making decisions related to information exchange. Content priority is of high relevance in a dynamic environment due to short connectivity time between nodes for information exchange. During connection, nodes always exchange high-priority data with each other and therefore high latency suffered by low-priority data. However, how to assign priority to content is a big question. For deciding content priority, demand of content and common exchanged information among nodes could be used as a priority measure. Dron et al. [12] recommended a cache eviction policy based on content prioritization with listing benefits of assigning names for caching content in ad hoc networks. To categorize, all content in cache is labeled either hot for high priority or cold for low priority. The authors have facilitated use of knapsack problem to decide content label based on its items' maximum utilization feature. The items corresponding maximum utilization are denoted as hot. The proposed scheme has shown outstanding performance in relation to LRU and intention caching for content retrieval latency and network bandwidth utilization.

6 Research Issues for Caching in NDN-IoT

From the discussions of various caching schemes above, the studies have shown that cache space is very limited as compared to the request coming in and out of routers or workstations. The management of cache space becomes really important when

different traffic compete for its utilization. Although researchers in the past have worked a lot in this domain pertaining to efficient caching mechanism for NDN-IoT environment, this area is still open for addressing issues of the domain. The caching mechanism focusing on content prominence for utilizing cache space has mainly classified content into either popular or nonpopular. These approaches mainly consider high popular content for cache insertion and low popular for cache eviction. However, calculating popularity of content with high accuracy is highly resource-consuming and is inefficient for environment with resource-constrained devices. Moreover, cache eviction policies are used to substitute old content with new one depending upon different parameters like prominence, priority, freshness, etc. There is always a trade-off between routers' processing capability and complexity of eviction policies. The design of simple policies with less complexity is the need of NDN-IoT environment due to processing constraints at router level. Managing replicas of content at different routers results in increased cost for various networks like NDN and ad hoc network. Some networks have facilitated routing algorithms with the use of on-path caching. The design of routing algorithms providing cache facility without routing information is a challenge. Another research challenge for caching is to deal with unpopular contents as their presence adds no benefit to caching but results in decreased network performance.

7 Conclusion

The communication in networks has shown a remarkable shift from host-centric communication to content-centric communication with the support of content-centric networking architectures like NDN. These architectures have proved their native support for efficient and fast content delivery and solution to traffic explosion problems without the use of IP addresses and are recommended to be used with many IoT applications. In NDN-IoT environment, transparent, ubiquitous, and fine-grained in-network caching is a fundamental aspect which guarantees efficient and timely retrieval of content. In the recent years, caching has emerged as a hot topic in this field. In this paper, several NDN-IoT caching algorithms with their strategies, advantages, parameters evaluated, and simulators used for study have been discussed. From the study, we conclude that reducing the cache redundancy based on different factors (such as content properties, content and node, splitting, replacement policies, etc.) is the best way to improve network performance in terms of high cache hit, reduced retrieval latency, low bandwidth utilized, and less network traffic. Moreover, cooperative caching mostly results in better performance than non-cooperative due to less cache redundancy. However, better results get achieved at the cost of additional complexity by adding new fields with caching information. Therefore, design of a caching algorithm with high cache hit, reduced content retrieval latency, less hops traversed, and of course low cost is still a challenge for the research community and needs further investigation.

References

1. Aboodi, A., Wan, T.C., Sodhy, G.C.: Survey on the incorporation of ndn/ccn in iot. IEEE Access. **7**, 71827 (2019)
2. Ahmed, S.H., Bouk, S.H., Yaqub, M.A., Kim, D., Song, H., Lloret, J.: Codie: controlled data and interest evaluation in vehicular named data networks. IEEE Trans. Veh. Technol. **65**(6), 3954–3963 (2016)
3. Al-Turjman, F.M., Al-Fagih, A.E., Hassanein, H.S.: A value-based cache replacement approach for information-centric networks. In: 38th Annual IEEE Conference on Local Computer Networks-Workshops, pp. 874–881. IEEE (2013)
4. Amadeo, M., Campolo, C., Iera, A., Molinaro, A.: Named data networking for iot: an architectural perspective. In: 2014 European Conference on Networks and Communications (EuCNC), pp. 1–5. IEEE (2014)
5. Amadeo, M., Campolo, C., Quevedo, J., Corujo, D., Molinaro, A., Iera, A., Aguiar, R.L., Vasilakos, A.V.: Information-centric networking for the internet of things: challenges and opportunities. IEEE Netw. **30**(2), 92–100 (2016)
6. Baccelli, E., Mehlis, C., Hahm, O., Schmidt, T.C., Ẅahlisch, M.: Information centric networking in the iot: experiments with ndn in the wild. In: Proceedings of the 1st ACM Conference on Information-Centric Networking, pp. 77–86. ACM (2014)
7. Baugh, J.P., Guo, J.: A per-face popularity scheme to increase cache robustness in information-centric networks. Procedia Comput. Sci. **134**, 267–274 (2018)
8. Jacobson, V., Smetters, D.K., Thornton, J.D., Plass, M.F., Briggs, N.H., Braynard, R.L.: Networking named content. In Proceedings of the 5th international conference on Emerging networking experiments and technologies (pp. 1–12). ACM (2009)
9. Cho, K., Lee, M., Park, K., Kwon, T.T., Choi, Y., Pack, S.: Wave: popularity-based and collaborative in-network caching for content-oriented networks. In: 2012 Proceedings IEEE INFOCOM Workshops, pp. 316–321. IEEE (2012)
10. Choi, H.G., Yoo, J., Chung, T., Choi, N., Kwon, T., Choi, Y.: Corc: coordinated routing and caching for named data networking. In: Proceedings of the Tenth ACM/IEEE Symposium on Architectures for Networking and Communications Systems, pp. 161–172. ACM (2014)
11. Dai, H., Wang, Y., Wu, H., Lu, J., Liu, B.: Towards line-speed and accurate on-line popularity monitoring on ndn routers. In: 2014 IEEE 22nd International Symposium of Quality of Service (IWQoS), pp. 178–187. IEEE (2014)
12. Dron, W., Leung, A., Uddin, M., Wang, S., Abdelzaher, T., Govindan, R., Hancock, J.: Information-maximizing caching in ad hoc networks with named data networking. In: 2013 IEEE 2nd Network Science Workshop (NSW), pp. 90–93. IEEE (2013)
13. Garetto, M., Leonardi, E., Martina, V.: A unified approach to the performance analysis of caching systems. ACM Trans. Model. Perform. Eval. Comput. Syst. **1**(3), 12 (2016)
14. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M.: Internet of things (iot): a vision, architectural elements, and future directions. Futur. Gener. Comput. Syst. **29**(7), 1645–1660 (2013)
15. Hail, M.A., Amadeo, M., Molinaro, A., Fischer, S.: Caching in named data networking for the wireless internet of things. In: 2015 International Conference on Recent Advances in Internet of Things (RIoT), pp. 1–6. IEEE (2015)
16. Hail, M.A.M., Amadeo, M., Molinaro, A., Fischer, S.: On the performance of caching and forwarding in information-centric networking for the iot. In: International Conference on Wired/Wireless Internet Communication, pp. 313–326. Springer (2015)
17. Hamdane, B., Serhrouchni, A., Fadlallah, A., El Fatmi, S.G.: Named-data security scheme for named data networking. In: 2012 Third International Conference on the Network of the Future (NOF), pp. 1–6. IEEE (2012)
18. Hu, X., Papadopoulos, C., Gong, J., Massey, D.: Not so cooperative caching in named data networking. In: 2013 IEEE Global Communications Conference (GLOBECOM), pp. 2263–2268. IEEE (2013)

19. Iqbal, J., Giaccone, P.: Interest-based cooperative caching in multi-hop wireless networks. In: 2013 IEEE Globecom Workshops (GC Wkshps), pp. 617–622. IEEE (2013)
20. Kalghoum, A., Gammar, S.M., Saidane, L.A.: Towards a novel cache replacement strategy for named data networking based on software defined networking. Comput. Electr. Eng. **66**, 98–113 (2018)
21. Laoutaris, N., Telelis, O., Zissimopoulos, V., Stavrakakis, I.: Distributed selfish replication. IEEE Trans. Parall. Distr. Syst. **17**(12), 1401–1413 (2006)
22. Li, J., Wu, H., Liu, B., Lu, J.: Effective caching schemes for minimizing inter-isp traffic in named data networking. In: 2012 IEEE 18th International Conference on Parallel and Distributed Systems, pp. 580–587. IEEE (2012)
23. Li, J., Wu, H., Liu, B., Lu, J., Wang, Y., Wang, X., Zhang, Y., Dong, L.: Popularity-driven coordinated caching in named data networking. In: Proceedings of the Eighth ACM/IEEE Symposium on Architectures for Networking and Communications Systems, pp. 15–26. ACM (2012)
24. Li, Z., Point, J.C., Ciftci, S., Eker, O., Mauri, G., Savi, M., Verticale, G.: Icn based shared caching in future converged fixed and mobile network. In: 2015 IEEE 16th International Conference on High Performance Switching and Routing (HPSR), pp. 1–6. IEEE (2015)
25. Liu, J., Wang, G., Huang, T., Chen, J., Liu, Y.: Modeling the sojourn time of items for in-network cache based on lru policy. China Commun. **11**(10), 88–95 (2014)
26. Psounis, K., Prabhakar, B.: A randomized web-cache replacement scheme. In: Proceedings IEEEINFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No. 01CH37213), vol. 3, pp. 1407–1415. IEEE (2001)
27. Quevedo, J., Corujo, D., Aguiar, R.: Consumer driven information freshness approach for content centric networking. In: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 482–487. IEEE (2014)
28. Hua Ran, J., Lv, N., Zhang, D., Yuan Ma, Y., Yong Xie, Z.: On performance of cache policies in named data networking. In: 2013 International Conference on Advanced Computer Science and Electronics Information (ICACSEI 2013). Atlantis Press (2013)
29. Rezazad, M., Tay, Y.: A cache miss equation for partitioning an ndn content store. In: Proceedings of the 9th Asian Internet Engineering Conference, pp. 1–8. ACM (2013)
30. Saxena, D., Raychoudhury, V., Suri, N., Becker, C., Cao, J.: Named data networking: a survey. Comput. Sci. Rev. **19**, 15–55 (2016)
31. Shang, W., Bannis, A., Liang, T., Wang, Z., Yu, Y., Afanasyev, A., Thompson, J., Burke, J., Zhang, B., Zhang, L.: Named data networking of things. In: 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 117–128. IEEE (2016)
32. Shang, W., Yu, Y., Droms, R., Zhang, L.: Challenges in iot networking via tcp/ip architecture. Technical Report NDN-0038. NDN Project (2016)
33. Shi, J., Wang, X., Huang, M.: Icn-based cache-aware routing scheme in msn. Ad Hoc Netw. **75**, 106–118 (2018)
34. Tyson, G., Kaune, S., Miles, S., El-Khatib, Y., Mauthe, A., Taweel, A.: A trace-driven analysis of caching in content-centric networks. In: 2012 21st International Conference on Computer Communications and Networks (ICCCN), pp. 1–7 (2012)
35. Vural, S., Navaratnam, P., Wang, N., Wang, C., Dong, L., Tafazolli, R.: In-network caching of internet-of-things data. In: 2014 IEEE International Conference on Communications (ICC), pp. 3185–3190. IEEE (2014)
36. Wang, S., Bi, J., Wu, J., Vasilakos, A.V., et al.: IEEE/ACM Trans. Networking. **24**(5), 2742–2755 (2015)
37. Wu, H., Li, J., Wang, Y., Liu, B.: Emc: the effective multi-path caching scheme for named data networking. In: IEEE International Conference on Computer Communications and Networks (ICCCN), pp. 580–587. IEEE (2013)

38. Wu, H., Li, J., Pan, T., Liu, B.: A novel caching scheme for the backbone of named data networking. In: 2013 IEEE International Conference on Communications (ICC), pp. 3634–3638. IEEE (2013)
39. Yao, L., Chen, A., Deng, J., Wang, J., Wu, G.: A cooperative caching scheme based on mobility prediction in vehicular content centric networks. IEEE Trans. Veh. Technol. **67**(6), 5435–5444 (2017)
40. Yi, C., Abraham, J., Afanasyev, A., Wang, L., Zhang, B., Zhang, L.: On the role of routing in named data networking. In: Proceedings of the 1st ACM Conference on Information-Centric Networking, pp. 27–36. ACM (2014)
41. Zhang, G., Li, Y., Lin, T.: Caching in information centric networking: a survey. Comput. Netw. **57**(16), 3128–3141 (2013)
42. Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Crowley, P., Papadopoulos, C., Wang, L., Zhang, B., et al.: Named data networking. ACM SIGCOMM Comput. Commun. Rev. **44**(3), 66–73 (2014)
43. Zhang, L., Estrin, D., Burke, J., Jacobson, V., Thornton, J.D., Smetters, D.K., Zhang, B., Tsudik, G., Massey, D., Papadopoulos, C., et al.: Named data networking (ndn) project. Relatório Tecnico NDN-0001, Xerox Palo Alto Research Center-PARC 157, 158 (2010)
44. Zhang, M., Luo, H., Zhang, H.: A survey of caching mechanisms in information-centric networking. IEEE Commun. Surv. Tutor. **17**(3), 1473–1499 (2015)

Divya Gupta is Assistant Professor in CSE with Chitkara University (Rajpura (Punjab)), India. She has more than 6 years of teaching experience. She received her master's degree in Computer Science and Engineering from Lovely Professional University, Phagwara, in 2012. Currently she is pursuing her PhD degree in Chitkara University. Her research area includes named data networking (NDN).

Shalli Rani is Associate Professor in CSE with Chitkara University (Rajpura (Punjab)), India. She has more than 14 years of teaching experience. She received her MCA degree from Maharshi Dayanand University, Rohtak, in 2004;M Tech degree in Computer Science from Janardan Rai Nagar Vidyapeeth University, Udaipur, in 2007; and PhD degree in Computer Applications from Punjab Technical University, Jalandhar, in 2017. Her main areas of interest and research are wireless sensor networks, underwater sensor networks, and the Internet of Things. She has published/accepted/presented more than 35 papers in international journals/conferences. She has worked on Big Data, underwater acoustic sensors, and IoT to show the importance of WSN in IoT applications. She received the Young Scientist Award in February 2014 from Punjab Science Congress, in the same field.

Syed Hassan Ahmed (S'13-M'17) completed his BS in Computer Science from Kohat University of Science and Technology (KUST), Pakistan, and masters combined with PhD degree from School of Computer Science and Engineering (SCSE), Kyungpook National University (KNU), Republic of Korea. In summer 2015, he was also a visiting researcher at the Georgia Tech, Atlanta, USA. Collectively, Dr. Hassan has authored/co-authored over 100 international publications including journal articles, conference proceedings, book chapters, and 02 books. From the years 2014 to 2016, he consequently won the Research Contribution awards by SCSE at KNU, Korea. In 2016, his work on robust content retrieval in future vehicular networks led him to win the Qualcomm Innovation Award at KNU, Korea. Currently, Dr. Hassan is a Postdoctoral Fellow in the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, USA, and his research interests include sensor and ad hoc networks, cyber-physical systems, vehicular communications, and future Internet.

Rasheed Hussain received his BS in Computer Software Engineering from N-WFP University of Engineering and Technology, Peshawar, Pakistan, in 2007 and MS and PhD degrees in Computer Engineering from Hanyang University, South Korea, in 2010 and 2015, respectively. He also worked as a Postdoctoral Research Fellow at Hanyang University, South Korea, from March 2015 till August 2016. He is currently working as Assistant Professor in the Institute of Information Sciences at Innopolis University, Innopolis, Russia. He is also working as Consultant for Innopolis University and Guest Researcher in the Department of Informatics at University of Amsterdam (UvA), Netherlands. His main research interests include information security and privacy, applied cryptography, and vehicular ad hoc networks. He is a member of the IEEE.

A Systematic Literature Survey: Development of Smart City Based on Various Internet of Things Architectures

Kirti, Gagandeep, and Anshu Singla

1 Introduction

The present scenario in which we reside is no doubt a very urbanized one. But it does not provide a very reliable and methodological way of living. So, this paper provides an insight as to how the urban cities could be transformed into technical uptowns or smart cities. The authors have used IoT to the rescue for this purpose. The Internet of Things is the terminology for making devices such as electrical appliances, actuators, and sensors that communicate with each other via the Internet. This amalgamation of IoT with internetworking makes the idea of a smart city a commercially viable one. In smart city various technologies like information and communication are utilized in order to provide public services which are way more interactive and feasible. Recent studies show that more than 6 billion individuals will be living in the urban community by 2050. So it is required to inculcate smart IoT vision to build smart city architecture. This vision includes smart waste management, smart hospitals, smart air monitoring, smart parking, smart building, and air monitoring system. There have been many proposals on transforming a city into a smart one by incorporating the abovementioned parameters. In this paper, the authors have reviewed technologies that can be used to convert these smart ideas into action. To study the implementation of these ideas, the authors reviewed papers of the last 7 years of how these technologies are prioritized. Different web applications hinged on wireless sensor networks have practiced in applications associated

Kirti · A. Singla (✉)
Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab, India
e-mail: kirti@chitkara.edu.in; anshu.singla@chitkara.edu.in

Gagandeep
CT Institute of Engineering, Management and Technology, Lambri, Punjab, India

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_4

to smart cities. Remote sensor systems have just been connected in various applications identified with savvy city like conditions for observing the urban surrounding to inculcate smart living. In this unique circumstance, web of things (IoT) [1], the authors take a perspective assumption that it is a dynamic part by interfacing and empowering gadgets to the web. In addition, tech-savvy accessories can give information and in addition get data for better familiarity with their environment. Collecting data from different provenances with the objective of learning extraction is a noteworthy test of relevant city utilities. As a reality check, the day is approaching that information will be expensive than the gadgets. The prime source for information procurement is IoT, WSN, cell phones, and a general group of people. Since all the gadgets produce diverse kinds of information, their distinctive configuration results in distinctive rates of information flow, thereby making it heterogeneous. This heterogeneity of the data requires a system that brings together a virtual space where this information source may fit. There exists a complex relationship between the diverse information collection created from different applications identified with a savvy city. Heterogeneity of information originates from the heterogeneity of sensors producing this information. Sensor heterogeneity is additionally a cause that influences to build an interoperable framework that can amalgamate with new sensors required for smart city applications. There is abundance of applications of IoT that can be deployed to make a city smart as shown in Fig. 1.

IOT is not a self-contained technology but rather composed of many components. These components are the building blocks of IOT. These components are (a) hardware, (b) software, and (c) network architecture.

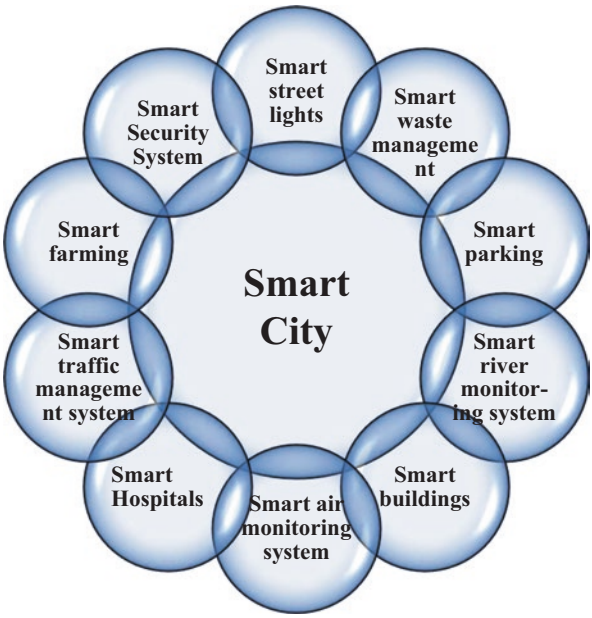


Fig. 1 Applications of IoT to make a city smart

Sensors being omnipresent in mobiles to smart homes, smart agricultural fields to smart retail stores, and smart cars to smart cities all are getting connected to each other and acquaint using the Internet. Even the security systems are moving toward smart security systems. In addition to CCTVs, sensors and the Internet can be used to achieve inclined level of sharp security structure of the warehouse. In this paper, the authors have implemented physical intrusion detection system (IDS) which is a smart security system that can be used to detect the encroachers in zone where humans are prohibited.

The rest of the paper is arranged as follows: Sect. 2 elucidates the literature of work done since 2013 to shift from urban to smart cities exploiting IoT. Section 3 delivers the brief idea of the physical intrusion detection system. Section 4 explicates the related work of physical intrusion detection since 2013. Section 5 explains the experimental setup done for the physical intrusion detection. In Sect. 6, result analysis has been performed. At last in Sect. 7, the authors have concluded the paper.

2 Literature Review

The various IOT architectures that exist in literatures are discussed below and shown in (Table 1). In 2013, Kyrazias et al. proffered two novel smart applications based on IoT [2]. The motive of the first application is efficient utilization of energy using the resources such as electricity as well as heat meters. The motive of the second application is to promote eco efficiency using traffic sensors which will give driving guidance. The authors emphasize the requirement of approaches that consolidate privacy, security, and trust as inbuilt support.

In 2013, Vlacheas et al. propounded a framework called cognitive management to address the matter of how miscellaneous objects can be connected in one environ-

Table 1 Brief description of work done in IoT architectures to make cities smart since 2013

References	Year	Description
[2]	2013	Propounded two novel applications: heat management and cruise control
[3]	2013	Propounded cognitive management framework
[4]	2014	Elucidates architecture deployment in Santander city
[5]	2015	Propounded multilevel smart city architecture
[6]	2016	Proffer smart city architecture
[7]	2016	Proffer City of Things testbed
[8]	2017	Radiofrequency identification-based authentication architecture
[9]	2017	Propounded Efficient Algorithm for Media-based Surveillance System
[10]	2018	Proffered unified framework
[11]	2018	System incorporates unmanned aerial vehicle
[12]	2018	Propounded great alternative region-based approach
[13]	2019	Propounded framework to upgrade the conveyance utility
[14]	2019	Delivered architecture to oversee the construction of huge monuments
[15]	2019	Propounded an architecture to deliver control methodology for premises

ment [3]. The authors use the proximity and cognition as a parameter to select the objects autonomically in a smart way. In this paper, the main priorities of the authors are to obscure heterogeneity, to provide flexibility, to utilize cognitive schemes, and to provide proximity. The main focus of this paper is virtual objects (RWO, any real-world object) in framework that changes dynamically.

In 2014, Sanchez et al. elucidated the architecture deployed at Santander city [4]. The authors also present the design of IoT architecture at a large scale in real world. The authors address the issues encountered while deploying urban city-scale architecture deployment. The authors describe the detailed vision of actual deployment of architecture model at Santander city. The authors also discuss the features supported by the deployed architecture design in Santander city.

In 2015, Gaur et al. propounded an architecture based on Dempster-Shafer uncertainty theory and web technologies [5]. The propounded smart city architecture is a multilevel architecture that utilizes a huge amount of information collected using web technologies semantics and Dempster-Shafer theory. The authors use the sensor fusion and reasoning mechanism to fetch the information from different domains. The authors elucidated the propounded multilevel architecture in the context of real-world scenarios. The authors use Dempster-Shafer theory to fetch sensor information to understand the activities of people.

In 2016, Chakarbarty et al. proffer a secure smart city architecture that incorporates four subblocks [6]. The first block represents black network (integrity, privacy, confidentiality), the second block represents trusted SDN controller (availability), and the third and fourth blocks represent the unified registry (authentication, authorization, mobility) and key management (external key management), respectively. These subblocks yield the security to reduce the vulnerabilities in IoT systems. The security provided by deploying this architecture is an extended form of security provided by standard IoT protocols.

In 2016, Latr et al. proffer City of Things IoT testbed located at Antwerp, Belgium [7]. This IoT testbed enables the validation and deployment of smart city at various levels such as user and technical. This testbed is a consolidating approach and thus can be applied on various layers such as data, network, etc. which make it eligible to support various wireless devices. At the network layer, it enables fast prototyping, while at the data layer, it provides the capability of fetching data quickly. At the user level, it provides the capability to give their input.

In 2017, Gope et al. proffer a confirmation design for disseminated IoT in view of radiofrequency identification (RFID) [8]. The authors use lightweight mechanism to reduce the time complexity. The authors use hashing to ensure security. The authors proffer the RFID authentication protocol which takes into account all the attributes necessary for RFID. The authors segregate the RFID to small subnetworks called RFID clusters. The main elements of the proffered architecture are reader, database, cloud, and RFID tags.

In 2017, Gupta et al. propounded an algorithm for smart city called EAMSuS (Efficient Algorithm for Media-based Surveillance System) in IoT [9]. The authors integrate the two-algorithm developed for security and wireless sensor network's

packet routing. The authors use the novel format to compress the video, named HEVC (High Efficiency Video Coding). The authors applied the cryptography to ensure security and confidentiality while transmitting packets. The authors also ensure that their algorithm reduces the space as well as the time complexity of sensor nodes (Table 1).

In 2018, Dutta et al. proffer a framework called unified framework [10]. The motive of developing this unified framework is to associate data, people, and services together into one framework. The authors also established prototypes named smart classroom and noise as well as air monitoring approach to ensure the efficiency of propounded unified framework. The authors segregate the applications into further three subcategories: category (a) IoT-based, category (b) smartphone- and IoT-based, and category (c) smartphone-based. The authors use the fog computing to mitigate the data traffic overload.

In 2018, Varela et al. proffer a system that consolidates into unmanned aerial vehicle (UAV) which enables monitoring of air pollutants' criteria [11]. The data fetched using the proposed system is then transmitted using the radiofrequency to base stations which process the received information and send it further to the Internet. UAV is an open-source platform that comprises large range communication as well as specialized sensors.

In 2018, Tao et al. propounded a great alternative region (GAR)-based approach to detect the pernicious nodes by employing network monitors [12]. The GAR approach is based on the network topology. The authors propounded a heuristic scheme to detect the location of compromised nodes. GAR are used as contender for network monitor location. The authors use the K-center to position the monitor to detect pernicious nodes. The authors use genetic algorithm to optimize the positioning of network monitors.

In 2019 [13], Claudio et al. have propounded an IoT framework that upgrades the conveyance utility for the betterment of citizens. The propounded framework consolidates the miscellaneous components like actuators and sensors in one schema. The authors have proffered the comprehensive case study about the framework. According to the author's study, it is possible to deploy a dynamic infrastructure considering all the important factors like security and safety measures.

In 2019 [14], Addabbo et al. delivered the IoT-based architecture to oversee the construction of huge monuments. The delivered architecture is formulated from the amalgamation of moderate power sensors and long range spectrum. The deployed is enabled to examine if there is any crack in the buildings. The authors have practiced the developed architecture in two cities: (a) medieval city and (b) city of Siena.

In 2019 [15], Zhao et al. propounded a novel architecture that proffers control methodology for premises. The propounded architecture comprises an agent as well as link models, which makes it preferable in comparison to the traditional one. Even before the establishment of the premises, control methodology can be set up in advance. The aforementioned characteristic makes it superior as well as eases the installation process.

3 Physical Intrusion Detection System

Intrusion detection system (IDS) is used for surveillance of the noxious traffic in the wireless sensor network nodes or the whole network. It acts as the security guard in defending the network from intruders [16]. Any intruder can harm the network nodes to such a great extent that sensors can communicate with each other. Moving further, to check the presence of a physical invader in the security zone of a warehouse, most of the organizations rely on CCTVs.

But it is required to move ahead of this as CCTVs can be easily tampered by human beings. So, to acquire human intervention-free security and more technology-based security, IOT is the most suitable solution. Physical IDS (PID) can be created using sensor-embedded technology, which will help us to attain the desired security goals. The basic difference between IDS and the physical IDS that we are going to propose is that the latter one will be able to detect the physical traducer if present in the warehouse. Constant eye-check can be made on the warehouse even without being tangibly present over there. Various sensors will be placed all over the warehouse, and they will continue to sense after specific refresh rates. Their data will be visualized by any authorized person who will have the access to the interface from anywhere. That person can control their working just through their mobile, tablet, etc. In fact, immediate actions can also be taken at that spot. The sensors will communicate with each other using the wireless protocols. Their data processing and visualization of data all will be buttoned up using the IOT technologies which are microcontrollers, cloud computing, and Big Data analysis. In crux, it can be said that physical IDS is one step ahead of the CCTVs and fingerprint technology.

4 Related Work of PID

In 2013 [17], Kasinathan et al. propounded a unified key to discover the denial-of-service attacks in networks that are based on 6LoWPAN. The authors have also deployed the Suricata, the signature-based network to discover the attack in PID system. In 2014 [18], Chen et al. propounded a PID architecture rooted upon event processing scheme considering the security stipulations. The authors have also propounded the deployment details for the event processing scheme established by Esper. In 2015 [19], Pongle et al. propounded a PID system that can discover the variations in the adjacent nodes in the network and can send the details to the unified modules. According to the authors, space complexity has been mitigated with the propounded approach. In 2015 [20], Cervantes et al. propounded a PID system for discovering specifically the sinkhole attack. In the propounded approach, if the node is suspected with sinkhole attack, the node broadcasts the attack to each and every node in the network. In 2016 [21], Arrington et al. propounded a PID system to keep a hawk eye on the smart home by practicing the behavior-based modeling.

Table 2 Brief description of work done on PID system since 2013

References	Year	Description
[17]	2013	To discover the denial-of-service attack
[18]	2014	PID architecture rooted upon event processing scheme
[19]	2015	PID system that can discover the variations in the adjacent nodes in the network
[20]	2015	PID system for discovering specifically the sinkhole attack
[21]	2016	To detect encroachment by practicing the behavior-based modeling
[22]	2017	Propounded approach is hinged upon the radio signal-based scheme allied to connect components
[23]	2018	Propounded a PID system employing the amalgamation of fog as well as cloud computing with IoT
[24]	2018	Employed the renowned classification algorithm named naive Bayes for PID system
[25]	2018	Employed the data mining in PID system to detect the encroachment
[26]	2019	Exploited the deep learning concept to establish PID system
[27]	2019	Propounded a heuristic approach to establish a PID system exploiting the random neural network in amalgamation with IoT
[28]	2019	Exploited the nature-inspired genetic algorithm to find out if there is legitimate entry or not

The algorithms that are rooted upon immunity have been practiced by authors to accomplish the goal (Table 2).

In 2017 [22], Roux et al. propounded a futuristic approach to unearth whether the users are licit or forbidden. The propounded approach is hinged upon the radio signal-based scheme allied to connect components. To differentiate between the licit and forbidden users, the authors have employed the machine learning algorithm. In 2018 [23], Pacheco et al. propounded a PID system employing the amalgamation of fog as well as cloud computing with IoT. According to the authors, the aforementioned amalgamation not only makes the PID system extensive but also makes it approachable and economical. The system is hinged upon the abnormality action to discover if the system has been invaded. In 2018 [24], Mehmood et al. employed the renowned classification algorithm named naive Bayes for PID system. The authors have exploited the PID system as multiagent in the entire network to discover if there is any encroachment. In 2018 [25], Subasi et al. employed data mining in PID system to detect the encroachment. According to the authors, in grid environs the deployed random forest delivers recommended results in comparison to k-nearest neighbor, support vector machine, and artificial neural network. In 2019 [26], Daming et al. exploited the deep learning concept to establish a PID system that can find out if there is any encroachment. The authors have instigated the modeling approach of feature extraction as well as the migration learning. According to the authors, the exploited scheme reduces the time complexity of detection. In 2019 [27], Qureshi et al. propounded a heuristic approach to establish a PID system exploiting the random neural network in amalgamation with IoT. The authors have collated the pro-

pounded approach with state-of-the-art machine learning algorithms. According to the authors, the accuracy of established PID system to discover encroachment has been enhanced by 10%. In 2019 [28], Mansor et al. exploited the nature-inspired genetic algorithm to find out if there is legitimate entry or not.

5 Experimental Settings

This fragment will describe the mechanism for creating the physical IDS and implementing it on the warehouse for detecting any encroachment. The microcontroller that has been used is Arduino Uno. Arduino/Genuino Uno is a microcontroller board rooted on the ATmega328P. It has 14 digital input/output pins, out of which 6 can be used as PWM outputs and 6 can be used as analog inputs. It also has 16 MHz quartz crystal, a power jack, an ICSP header, a USB connection, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started.

In this system, all the sensors read up the data, i.e., sense the data. The sensed data have been then sent to the Arduino board. The ATmega328 microcontroller then processed the data. The code has been written in Arduino IDE and has been sent to Arduino board using USB. Arduino then executed the instruction written in the code and data has been sent to private cloud interface. But, how? The answer is as follows: Firstly, the Wi-Fi module, i.e., ESP8266, is connected to the Arduino and checked whether it is connected to the board or not. Then it displays this on the terminal screen accordingly. If connected, then it will check whether the module is connected to the Wi-Fi or not. It has been checked by the sequence of some "AT" (attention) commands. After being connected to the Wi-Fi, now it will create a string in which the data of all the sensors is connected together to form a single data packet. Then, this packet is sent to the private cloud interface for displaying and continuous monitoring of data. The data is sent at regular intervals. The private cloud interface gets its page refreshed after every 17 seconds which means that after every 17 seconds, the data is refreshed over the interface. Now, the question is where this huge amount of data is stored and how this data is analyzed. The answer is through the use of cloud computing and Big Data analysis. The cloud's service model Infrastructure as a Service is used a database. Here all the data is stored that is being sent from sensors through Arduino and ESP8266. In interface a table is maintained in which the data of every sensor is displayed. The output is in numerical form in interface. The temperature and humidity (DHT-11) and MQ-6 gas sensor columns show the respective values sensed by sensors. The output of the ultrasonic sensor (HC-SR04) and PIR motion sensor (HC-SR01) is string which is displayed in the form of 0 and 1 over the interface. The PIR value 0 signifies that no motion is detected and the value 1 signifies that motion is detected. The ultrasonic value 0 shows that door is closed and 1 shows that door is open. To analyze this whole data, we have feature of plotting this value in the form of charts. The temperature and

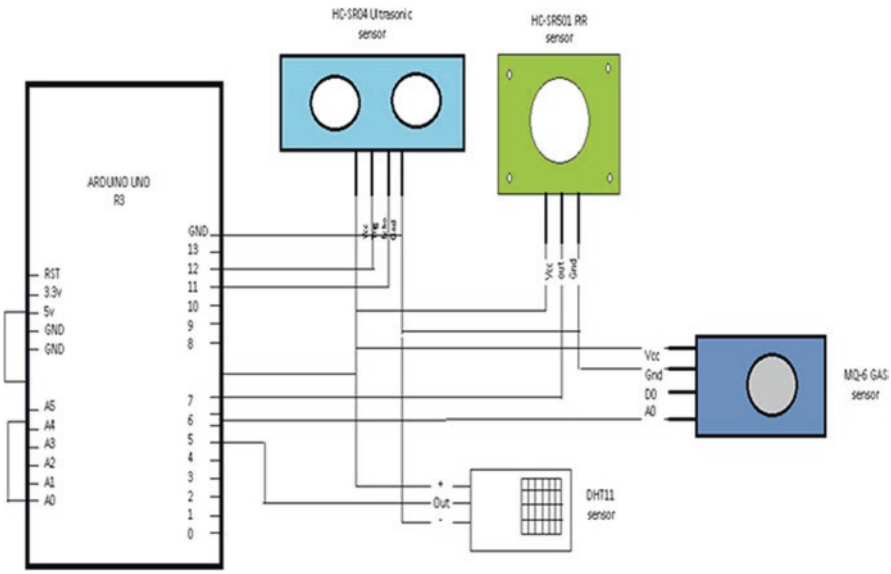


Fig. 2 Circuit diagram for deployed intrusion detection system

humidity and gas (ppm) values are plotted. Through this graph we can analyze the data and see the significant changes.

In this way, any person over any location can monitor the area. This will help in taking the immediate measures and some emergency helps like police, ambulance, etc. This is a cost-efficient system as once installed sensors will continue to work for a long time and less human interference will be there. We can achieve more accurate results and immediate measures can be easily taken. Overall, this provides organized, competent security system. The circuit of deployed method is complex to some extent but not hard to understand. The circuit diagram is shown in Fig. 2.

The control room contains the Arduino and Wi-Fi module which is ESP8266. All other sensors like ultrasonic sensor, PIR sensor, MQ-6 gas sensor, and DHT-11 sensors are connected to the control room using cables as shown in Fig. 3. Figure 4 shows the prototype of the warehouse where all the sensors are embedded to keep an eye on the security of it.

6 Result and Discussion

The output of this physical IDS can be vigilant over the private cloud interface. Of course, the user has to enter his credentials required for ingression into the interface. The user can continuously keep his hawk eye whenever the values change over the interface.

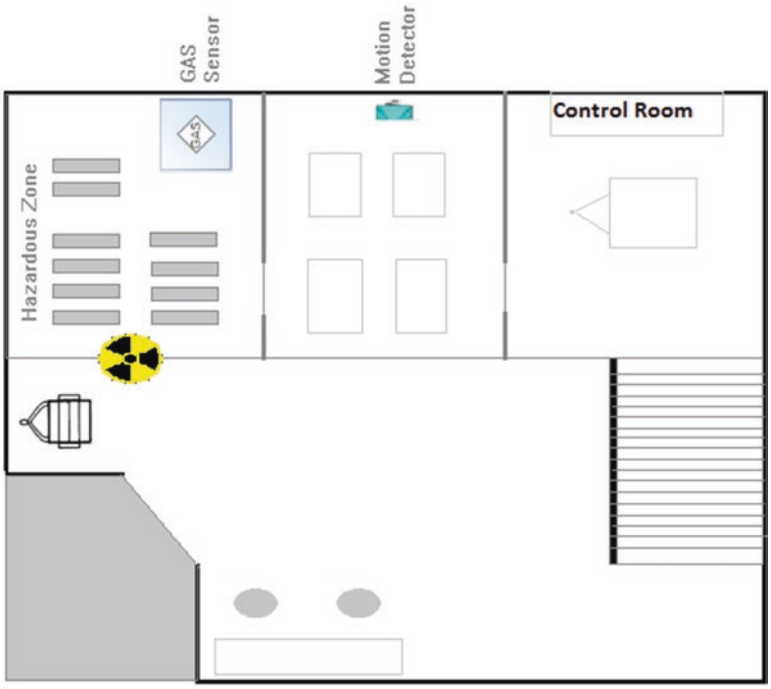


Fig. 3 Top view of the intrusion detection system

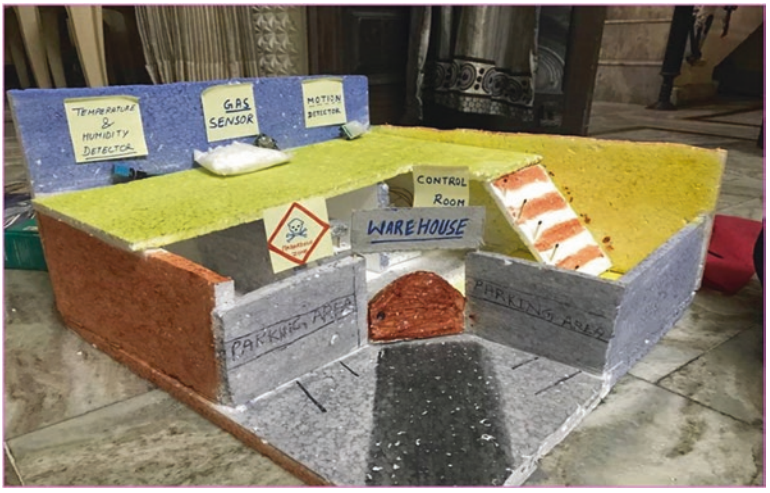


Fig. 4 Prototype of intrusion detection system

Table 3 Data sent over cloud interface by intrusion detection system

Transaction ID	Temperature	Humidity	PIR	Ultrasonic	MQ – 6	Timestamp (server)
11	26	29	0	0	0	2019-08-20 21:38:45
12	26	29	0	0	0	2019-08-20 21:39:03
13	26	29	0	0	0	2019-08-20 21:39:21
14	26	29	0	0	0	2019-08-20 21:39:39
15	26	29	1	1	0	2019-08-20 21:39:57
16	26	29	1	1	0	2019-08-20 21:40:15
17	26	29	1	1	0	2019-08-20 21:40:33
18	26	29	1	1	0	2019-08-20 21:40:51

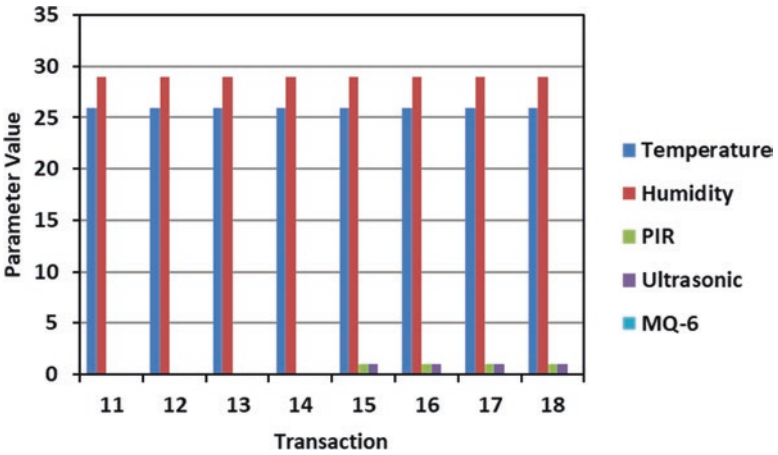


Fig. 5 Graphical representation of data sent over cloud interface

Table 3 depicts the data sent over cloud interface through intrusion detection system. The value of temperature and humidity at that time is shown; value 1 under PIR means motion is detected and 0 means no motion detected. The ultrasonic sensor and MQ-6 values 0 means gate of warehouse is closed and no gas leaked, respectively. Whenever the gate opens, the value of the ultrasonic sensor changes to 1 which means the gate is open and someone entered the warehouse.

For qualitative analysis, the graphs for the above transactions are shown in Fig. 5. Representation shows that there is motion in transactions 15, 16, 17, and 18 and the gates of the warehouse are open as well, which means there may be some intruders there.

7 Conclusion

The motive of this paper is to view the various trends to deploy the smart city using IoT. Here the authors have reviewed the different architecture exploit to create smart city in recent years. The authors analyze the various characteristics of IoT and how

to use them in different domains. In this paper, firstly the motivation to research in IoT field has been explained. Secondly, the authors have deployed the intrusion detection system for warehouse. The physical intrusion detection system will be the effective system for providing security that requires less human interference and more technology-equipped system. The Internet will boost up the process, and the look-out of the area can be done from anywhere. It will be cost-effective, and long-term usage would be achieved. This will drive the security systems to another height and will help people to be stringed together with the pace changing technology. Everything will be digitalized and most probably accurate results will be achieved. Even, this system can be extended with more sensors for big warehouse and other storage areas also. Thus, a systematic, consistent, higher-quality security system can be maintained with the help of new embedded technology Internet of Things. By using this paper, the researchers can discern how the new architecture for sustainable smart city in the future can be designed.

References

1. Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-Khah, M., Siano, P.: Iot-based smart cities: a survey. In: 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), pp. 1–6. IEEE (2016)
2. Kyriazis, D., Varvarigou, T., White, D., Rossi, A., Cooper, J.: Sustainable smart city IoT applications: heat and electricity management & eco-conscious cruise control for public transportation. In: 2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), pp. 1–5. IEEE (2013)
3. Vlacheas, P., Giaffreda, R., Stavroulaki, V., Kelaidonis, D., Foteinos, V., Poulios, G., et al.: Enabling smart cities through a cognitive management framework for the internet of things. IEEE Commun. Mag. **51**(6), 102–111 (2013)
4. Sanchez, L., Muñoz, L., Galache, J.A., Sotres, P., Santana, J.R., Gutierrez, V., et al.: SmartSantander: IoT experimentation over a smart city testbed. Comput. Netw. **61**, 217–238 (2014)
5. Gaur, A., Scotney, B., Parr, G., Mcclean, S.: Smart city architecture and its applications based on IoT. Procedia Comput. Sci. **52**(Iupt), 1089–1094 (2015)
6. Chakrabarty, S., Engels, D.W.: A secure IoT architecture for smart cities. In: 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 812–813. IEEE (2016)
7. Latre, S., Leroux, P., Coenen, T., Braem, B., Ballon, P., Demeester, P.: City of things: an integrated and multi-technology testbed for IoT smart city experiments. In: 2016 IEEE International Smart Cities Conference (ISC2), pp. 1–8. IEEE (2016)
8. Gope, P., Amin, R., Islam, S.H., Kumar, N., Bhalla, V.K.: Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. Futur. Gener. Comput. Syst. **83**, 629–637 (2018)
9. Memos, V.A., Psannis, K.E., Ishibashi, Y., Kim, B.G., Gupta, B.B.: An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. Futur. Gener. Comput. Syst. **83**, 619–628 (2018)
10. Dutta, J., Roy, S., Chowdhury, C.: Unified framework for IoT and smartphone based different smart city related applications. Microsyst. Technol. **25**(1), 83–96 (2019)
11. Hernández-Vega, J.I., Varela, E.R., Romero, N.H., Hernández-Santos, C., Cuevas, J.L.S., Gorham, D.G.P.: Internet of Things (IoT) for monitoring air pollutants with an Unmanned

Aerial Vehicle (UAV) in a smart city. In: Smart Technology, pp. 108–120. Springer, Cham (2018)
12. Arasteh, H., Hosseinnezhad, V., Loia, V., Tommasetti, A., Troisi, O., Shafie-Khah, M., Siano, P.: Iot-based smart cities: a survey. In: 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC), pp. 1–6. IEEE (2016, June)
13. Badii, C., Bellini, P., Difino, A., Nesi, P.: Sii-Mobility: an IoT/IoE architecture to enhance smart city mobility and transportation services. Sensors. **19**(1), 1 (2019)
14. Addabbo, T., Fort, A., Mugnaini, M., Panzardi, E., Pozzebon, A., Vignoli, V.: A city-scale IoT architecture for monumental structures monitoring. Measurement. **131**, 349–357 (2019)
15. Zhao, Q., Jiang, Z.: Insect Intelligent Building (I 2 B): a new architecture of building control systems based on Internet of Things (IoT). In: International Conference on Smart City and Intelligent Building, pp. 457–466. Springer, Singapore (2018)
16. Anand, A., Patel, B.: An overview on intrusion detection system and types of attacks it can detect considering different protocols. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **2**(8), (2012)
17. Gupta, A., Pandey, O.J., Shukla, M., Dadhich, A., Mathur, S., Ingle, A.: Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks. In: 2013 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1–7. IEEE (2013)
18. Jun, C., Chi, C.: Design of complex event-processing IDS in internet of things. In: 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, pp. 226–229. IEEE (2014)
19. Pongle, P., Chavan, G.: Real time intrusion and wormhole attack detection in internet of things. Int. J. Comput. Appl. **121**(9), 1 (2015)
20. Cervantes, C., Poplade, D., Nogueira, M., Santos, A.: Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp. 606–611. IEEE (2015)
21. Arrington, B., Barnett, L., Rufus, R., Esterline, A.: Behavioral modeling intrusion detection system (bmids) using internet of things (iot) behavior-based anomaly detection via immunity-inspired algorithms. In: 2016 25th International Conference on Computer Communication and Networks (ICCCN), pp. 1–6. IEEE (2016)
22. Roux, J., Alata, E., Auriol, G., Nicomette, V., Kaâniche, M.: Toward an intrusion detection approach for IoT based on radio communications profiling. In: 2017 13th European Dependable Computing Conference (EDCC), pp. 147–150. IEEE (2017)
23. Pacheco, J., Hariri, S.: Anomaly behavior analysis for IoT sensors. Trans. Emerg. Telecommun. Technol. **29**(4), e3188 (2018)
24. Mehmood, A., Mukherjee, M., Ahmed, S.H., Song, H., Malik, K.M.: NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks. J. Supercomput. **74**(10), 5156–5170 (2018)
25. Subasi, A., Al-Marwani, K., Alghamdi, R., Kwairanga, A., Qaisar, S.M., Al-Nory, M., Rambo, K.A.: Intrusion detection in smart grid using data mining techniques. In: 2018 21st Saudi Computer Society National Computer Conference (NCC), pp. 1–6. IEEE (2018)
26. Li, D., Deng, L., Lee, M., Wang, H.: IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. Int. J. Inf. Manag. **49**, 533 (2019)
27. Larijani, H., Ahmad, J., Mtetwa, N.: A heuristic intrusion detection system for Internet-of-Things (IoT). In: Intelligent Computing-Proceedings of the Computing Conference, pp. 86–98. Springer, Cham (2019)
28. Mansour, A., Azab, M., Rizk, M.R., Abdelazim, M.: Biologically-inspired SDN-based intrusion detection and prevention mechanism for heterogeneous IoT networks. In: 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1120–1125. IEEE (2018)

Kirti received her bachelor's degree in Computer Science and Engineering in 2016 from Beant College of Engineering and Technology, Gurdaspur. She is currently pursuing her master's degree in Digital Image Processing and working as Research Scholar at Chitkara University, Rajpura. Her main research interests include image processing, deep learning, and IoT

Gagandeep has completed his bachelor degree in Computer Science and Engineering in 2018 from CT Institute of Engineering and Technology. Currently he is pursuing his master's degree in IoT. His research interests include wireless sensor network and the Internet of Things

Anshu Singla received her PhD in Computer Science and Engineering. She is currently working as Associate Professor at Chitkara University, Rajpura. She has 12 years of teaching experience. Her areas of expertise are artificial intelligence, machine learning, pattern recognition, and image segmentation.

Integration of WSN with IoT Applications: A Vision, Architecture, and Future Challenges

Karan Bajaj, Bhisham Sharma, and Raman Singh

1 Introduction

The Internet of Things (IoT) is the connectivity of the physical devices and objects that are used in daily life, which are connected over the Internet network. It is connected to the different types of objects which communicate with each other through various sensors, actuators, and processors. The goal of IoT is to attain high degree of intelligence with least human intervention [1]. The IoT brings the automation and intelligence in all sectors of life, making it comfortable; here devices are made self capable to take smart decision by themselves. In the IoT, a large number of heterogeneous devices are connected over the network. Today the IoT covers a large domain and every aspect of the society from industry, healthcare, and transport to the agriculture and home environment provides the services.

A smart city covers all the domains of the society that use information and communications technologies (ICTs) [2]. It also covers all the different applications and makes the city services and monitoring more aware, interactive, and efficient [2]. wireless sensor network (WSN) is the backbone of IoT, without which the concept of a smart city cannot be realized. Sensors and actuators are the devices, which interact with the physical world and impose the changes. Under the heterogeneous environment, a large number of devices are connected together using sensors and

K. Bajaj · B. Sharma (✉)
Chitkara University School of Engineering and Technology,
Chitkara University, Himachal Pradesh, India
e-mail: karan.bajaj@chitkarauniversity.edu.in; bhisham.sharma@chitkarauniversity.edu.in

R. Singh
Department of Computer Science & Engineering, Thapar Institute of Engineering and Technology, Patiala, Punjab, India
e-mail: raman.singh@thapar.edu

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_5

generate large amount of data. This data is stored and analyzed to derive the information and support decision-making [1].

A smart city consists of a large number of heterogeneous devices, including smart as well as simple objects. A large amount of data is gathered due to a large number of sensors connected to the objects. IoT network in the case of a smart city must be scalable as there can be requirement of adding new devices and deleting old devices, anytime and anywhere. Due to wide application areas and difference of technology among the devices, incorporating WSN becomes challenging [3]. From the perspective of the smart city, the main facing challenges of IoT are interoperability, context awareness, scalability, and management of large volumes of data, security, privacy and integrity, dynamic adaptation, reliability, and latency.

The smart city covers all the aspects of society by having large number of applications. Figure 1 represents the key aspects of society that make the smart city. It shows healthcare, industries, transport, agriculture, and home automation; all are the essential part of the smart city. The smart city is equipped with several equipment and technologies which make the life of people smarter through several applications; there are several aspects of the smart city such as smart technology, infrastructure, and governance. IoT is bringing transformation in education sector and security requirements of smart cities [4].

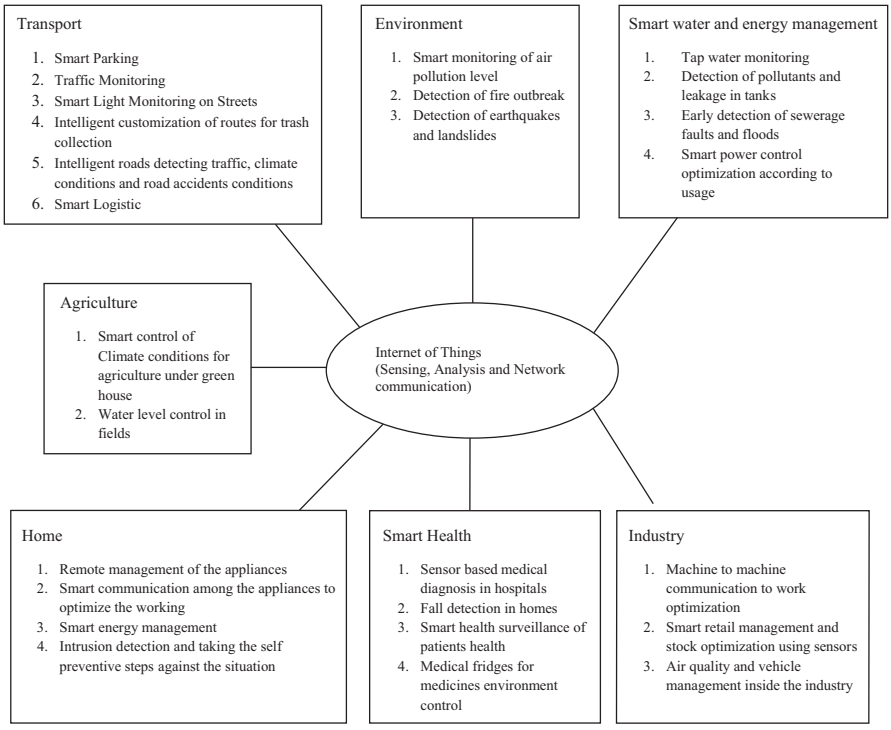


Fig. 1 Key aspects of smart city

2 Architectural Need of the Smart City

Architecture supports the services and their working and is required to solve the key issues that are faced by IoT applications. It provides the level of abstraction over physical devices and services and supports the heterogeneity and interoperability among devices, which is one of the key properties of IoT. A large number of devices and objects are connected under IoT having different functionalities, capabilities, characteristics, and Internet protocols which also raise the concern of security issues in IoT. In smart city IoT structure, a large number of independent systems or applications work together. These devices have different kinds of sensors, and both the hardware and software heterogeneity exist among the devices; therefore, we need the architecture which is flexible to support both hardware and software diversity among these objects.

In smart city IoT architecture, information is shared not only among the different applications of the society but also to the interested parties like government and management sectors, etc. The smart city should be capable to scale any number of devices with different technology anytime; therefore, cross-application services are the requirement of smart city. The author in [5] suggests that some domains in smart city need real-time immediate response for well-organized resource planning, to help in the effective use of resource utilization. There is the need of standardization among the architectures to solve the common issues that arise due to the management of a huge amount of data, communication issues related to a large number of protocols, real-time processing of data, data security, privacy and expansion in existing application due to changes in technology, and increasing usage also termed as scalability [6]. Security among the IoT applications, especially in the case of smart city where there is a large amount of intercommunication among the different applications, becomes one of the major challenges due to diversity among the devices and dynamic nature in terms of network and scalability. In IoT applications, the existing solutions do not fully satisfy the need of security. Some solutions demand high energy requirements and become costly solutions [7].

Figure 2 shows a generalized open architecture proposed to support the different applications. It also shows that different sectors will contain the sensors and will be connected to a common gateway as these sectors will share the information to support each other. The kind of processing requirement of the architecture to support the issues in IoT such as the processing of data will be done at edges; it means device level itself, to support critical applications like healthcare and also some data that cannot be handled at edge level, will be processed at middleware, also called as fog computing.

With the study of issues in architectures and understanding the need of the architecture in smart city, the conclusion is drawn that the smart city needs open flexible architecture which supports the scalability, which means a large number of devices can be added in the system anytime. Also, scalability and heterogeneity among the devices should be taken care of. A general architecture is proposed which is

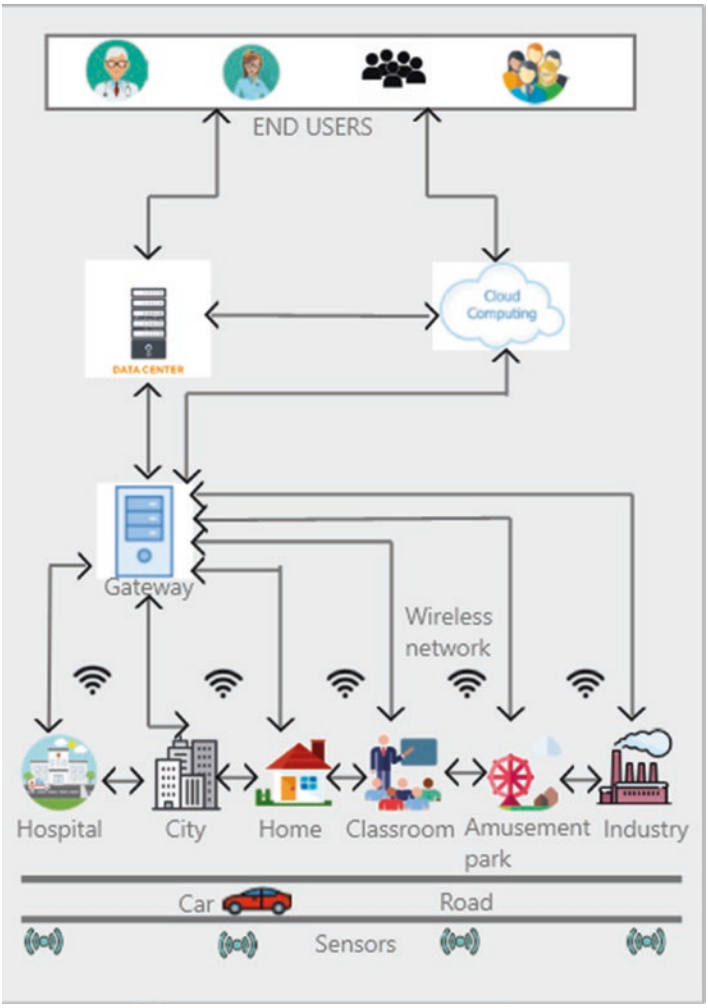


Fig. 2 IoT-based generalized architecture of smart city

edge-based open architecture so that real-time data processing can be done and latency issue can be handled.

Smart City Platform

The smart city uses the emerging technologies such as WSN and big data analytics as a large amount of data is produced by sensors to reduce the resource utilization and bring intelligence in applications. Effective data storage is also required because data grows at a very rapid rate and similarly high computational and processing requirement need is handled by edge devices [8].

For building the smart city, we need a network of smart things using sensors connectivity among them. They collect a huge amount of data using smart gateways where all devices send their data. Some initial amount of data can be processed by task off-loading to the nearby devices or using the concept of femto cloud or fog structure at the middleware level [9]. Whereas the tasks that need a high-computation cloud structure are used for processing and analytics and data lake for storing data, the value of which is yet to be defined and cleaned, and structured data is sent to the data warehouse. Data analytics and machine learning algorithms are implemented at the middleware level and cloud level for processing and analytics task, and finally commands are sent to the actuators to control the applications used by the end users [10].

IoT Application Requirements

To implement the IoT solutions, there is a need to create the applications, but application implementation requires some basic requirements that are:

1. Scalability is one of the main requirements of IoT. The platform should be capable of adding any number of devices anytime without having any effect on the application.
2. IoT applications should be secure and trustworthy. These are the essential components as information flows in wide forms over the sensor network.
3. IoT applications require self-adaptable, optimizable, and configurable system according to the changing need of the environment.
4. IoT applications should be able to understand the situation and emotion according to the context and personalize the services and are capable of decision-makings.
5. Critical applications in IoT are required to be dynamic and should respond in real time without any latency. For example: critical applications like healthcare and inter vehicle communications have dangerous impact in case of latency.
6. IoT applications collect a large amount of personal and private data which may contain the personal data and activity log of people. There is a requirement of privacy compliant law for data protection.

3 IoT-Integrated Applications and Role of WSN in Smart City

Smart cities are touching and transforming all the areas of modern society, like e-health, e-transport, energy, environment, and education. For example: data from weather department can be extremely helpful for environment, flood, and agriculture monitoring. Similarly monitoring the health of elder people and patients in the live environment can be highly useful. Some of the application fields where IoT is bringing a great advantage are:

3.1 IoT in Healthcare

IoT is transforming the healthcare and is one of the most important and critical applications among the society. Using wireless sensor networks to enhance the capability of healthcare structure and real-time monitoring and processing is one of the most challenging goals. Reducing the cost and improving the care of the patients and at the same time dealing with the shortage of staff are the primary concerns [11]. Problems related to complex data in terms of its variety, pace, and latency also need to be taken care of [12]. Healthcare needs multilayer architecture having edge-level computing at device level, fog computing, and cloud computing for computation-intensive tasks.

Mobile Computing in Healthcare Applications
Mobile can give the facility of edge computing to monitor the health of patients from the distant locations and can be done by using central cloud at local level. The authors in [13] proposed a window-based rate control algorithm (w-RCA) and medical quality of service (m-QoS) to provide better service and quality in the mobile edge computing based healthcare [13]. Patients will be wearing the sensor devices for continuous monitoring linked to the mobile applications for real-time processing.

The cloud platform implementation helps the patients' 24/7 monitoring by using smartphone app. Patients can track their health while traveling or relaxing at home anytime and anywhere. Farahani B. et al. [12] say P2P video/audio capabilities can be provided to patients for identification of diseases as well as their treatments and refills of medicine whenever required.

IoT in Medication
The IoT in medication of patients can be of great help especially in the case of elderly patients. In home caring service, a self-alarm system is proposed by the authors in [14] to take the medicine. Also the state of medicine bottle is tracked by the sensors using weight sensors to give warning in case of medicine overdose. In [15] authors purposed the use of RFID (radio frequency identification) technology labels and tags on patient's medicines connected over the Internet of Things with the patient's personal medical files. This will also help in better connectivity between the doctor and patient. Using this architecture, physician can remotely monitor the patient state, and warning can be generated to physician or nurse in case of some changes in patient state. Here the authors have used machine learning algorithms and probabilistic learning structure to enhance the accuracy using classification.

As studied in [16], the authors have proposed a smart necklace to determine the intake of medication by patients. It checks and observes the skin movement of the neck part during the intake of medicine. Bayesian network is used in the study to accurately identify the swallowing of medication capsules, normal speaking, and chewing of vitamins [16]. In combination, medicine bottles are also made smart with wearable audio sensors, and classifications are used to get the accuracy in assessment of medication adherence.

IoT in Ambient Assisted Living

The Ambient Assisted Living (AAL) [17] is particularly targeting the quality of life for older people who are dependent and are at home. It not only includes the medication and continuous health monitoring but also checks the indoor air quality (iAQ) and comfort. The devices and objects in the home will be connected to each other to help the elderly and disabled persons in their day-to-day routine activities [18]. It will also take care of the growth of diseases by live check on the vital signs of the persons.

Challenges in IoT Healthcare

IoT in healthcare brings lots of new hopes to patients and elderly people, but the seamless connection among locations, patients, and hospitals is not easy to achieve. The main challenges in the way of IoT integration in healthcare are:

1. Management of a large amount of data in the healthcare system. The large numbers of medical sensors are attached to the patients and around them. The dynamic nature of the body with continuous state changing becomes more challenging. So collecting and analyzing data with accuracy becomes challenging.
2. Different formats among the data is also an issue as some data is collected by the images using cameras, some data is captured in the form of variations and vibrations, some in the form of body temperature, etc. Accumulating all these different data and analyzing on common platform become an issue.
3. IoT applications particularly in the case of healthcare are time bounded, and emergency services cannot tolerate latency and require real-time monitoring and analysis. But the tasks that require high computations cannot be handled at the edge level, so an open research challenge is present in the domain.

IoT healthcare has lot of advantages and scope, but still there are lot of challenges which need to be addressed like device-network human interfaces, security, and privacy. A large variety and volume of data and lack of standard architecture are also an issue, including this network architecture, which should be scalable; latency rate should be lower with high bandwidth.

3.2 IoT in Industries

The IoT is bringing revolution in industries by improving the machine-to-machine and machine-to-human communication and bringing intelligence in value chain of system and making it a smart value chain. Industries are embedding intelligence and network communication among the process belts to improve their own systems and products. Checking the events, warning of failures, and suggestions to improve and upgrade the existing hardware, refineries, and offices according to IoT applications to enhance the efficiency of the existing system are the advantages of bringing the IoT. The main purposes of bringing the IoT in industries to offer their customers new sets of premium services are:

- Using machine learning (ML) and natural language processing (NLP) to bring smart handling of equipment and their pre-maintenance.
- Making pricing dynamic and analyzing the data based on the usage and providing it to the manufacturing value chain help companies increase efficiency and reduce the processing costs.
- In retail sector, giving retailers and customers personalized experience [19].

The IoT is among one of the future technologies gaining large popularity for all kinds of industrial domains. In this, there is a global network where machines and devices work in conjunction with each other. The author in [20] says that the full power of IoT in industries can be achieved by complete connectivity of devices in industries. For all kinds of processing, monitoring and management of data cloud-based business model can be used. IoT is not only touching but also becoming part of every aspect of industries from logistics, retail management, and customer support to supply chains.

IoT Value Chain

In a broader view, it is not restricted to one organization; rather it allows the data to be shared publicly in multiple organizations. This data is the information that can help the other actors to perform better in terms of design, decision-making, and controlling other devices to optimize the services. IoT value chain has different components like, for taking inputs, there are different sources of IoT value chain, devices/sensors, open data, and corporate databases. Then, initial development of information and components is done under production and manufacture, while processing of information is done using data analytics to create knowledge. Packaging is also a component of this chain, wherein a product is made ready for distribution; and finally distribution and marketing. In this information products are used for improving internal decision-making and for resale to other economic actors.

Today corporate sector wants to provide direct and customized service to the consumer, and this is becoming possible with the merging of machine-to-machine (M2M) value chain with IoT services. Data has not remained specific company based now; it is collected over various sensors and radio frequency identification (RFID). Today we need information-driven value chain in industries. Industries not only want to sell their products but also want to know the potential of the business. Before starting up, analysis reports are generated to know the current and future aspect of business, what can be its growth rate, how future demand will rise or decline, or what kind of scalability will be required in the business [21]. For example, today your GPS device can learn that, after a long journey, you prefer a cup of coffee, and after journey your smartphone shows you immediately the nearest best cafe areas, or coffee business makers can learn that in this region lot of customers after traveling from train prefer a coffee, so let's start cafeteria in a nearby location; earlier no smart learning or searching was there, and people use to walk and search by asking the people nearby.

Similarly, clothing retailers can learn your preference and choices from your buying and trial habits which he could use to give customized service to customer

as well as it can help him to stock only the preferred choices of customers in the store.

Challenges in IoT Industry

Here the IoT deals with some common challenges that the healthcare system deals with, like scalability is a big challenge in IoT implementation in industries, it means growth in terms of capability, system, and network. Infrastructure and processes in industries grow at a rapid rate; the IoT structure should be capable to accommodate that growth. As industries are of different domains, for example, manufacture sector is different from retail and logistic sector; similarly, information technology sector is different from the production. There is a gap of technological standardization as a lot of hardware is involved in the technology or platform. Due to the lack of standards, companies that make the IoT-based products use the random architectures that they feel comfortable and easy in implementation [21].

As different hardware and platforms are involved, interoperability becomes a challenge. This hardware makes use of different software to swap over and utilize information, and a broader software infrastructure will be needed on the network and on background servers in order to deal with the smart objects and offer services to support them.

Fault tolerance is a big issue in IoT devices, as they are dynamic and mobile in nature. They change their state and behavior rapidly. Structuring an Internet of Things and an ability to automatically adapt to changed conditions is required [21].

3.3 Internet of Things in Agriculture

Recently agriculture farming has gone through technological transformations. In the last decades, it has become more technology-driven and industrialized, bringing a large number of benefits to the farmers. The ever-increasing demand of food in terms of both quality and quantity has made agriculture more as industry where now farmers have gain complete control from production to selling of crops. Revolution of technology in agriculture is possible due to the Internet of Things (IoT); it is a highly promising family of technologies which offer solutions to the several existing problems in agriculture. Researchers and scientific groups are continuously working on IoT applications integrated with wireless sensor network (WSN) to help the agriculture sector to deliver better services and enhanced IoT products.

Using automated machinery to control and optimize water use, energy management and use of chemicals for pest control and use of fertilizers, precision agriculture [22] aims to boost and develop agricultural processes to make sure maximum output and require quick, dependable, scattered measurements in order to give growers a more detailed overview of the in progress state in their cultivation area. Agriculture applications will also keep track on weather and environment information, gather the data from various heterogeneous systems, evaluate the knowledge and organize them in the form of smart algorithms to provide a better insight into

the in progress processes, do the interpretation of the present conditions, and make predictions based on heterogeneous inputs, and based on the collected information, warning signal will be produced. The different fields of agriculture where the IoT is bringing changes are:

1. Greenhouses observe the climate conditions using sensors and control them to maximize the production and maintain the quality.
2. Control the various parameters of humidity and temperature levels to form the compost to prevent fungus and other microbial contaminants.
3. Tracking the animals and identifying their grazing locations using sensors and study of the air quality in farms and detection of harmful gases from excrements.
4. Continuous monitoring of crops for reducing spoilage and crop waste [23].

Implemented Solutions Available in IoT Agriculture

The Kaa IoT platform provides sensor-based remote monitoring of crops and equipment including livestock management with climate monitoring and forecasting. Provided services include livestock tracking, stats on livestock production, and smart logistics and warehousing [24].

Farm Logs is a sensor-based software application for technology-enabled farms. It helps to manage day-to-day operations on the field and create agronomic plans that calculate field-level profit/loss based on your input expenses and rates. It also helps in documentation for reporting and analysis and tracks your marketing position and makes more profitable crop sales [25].

The Phytech gives the ability to direct plant sensing, connects you directly to the plants, sensors are connected to the plants micro-variations of stem diameter that are scientifically proven stress indicators. The data is transmitted in real time to the Phytech cloud for further analytics, providing certainty in decision-making, optimizing production, and reducing risk. Patented algorithms are continuously performing data analysis and do predictive analysis to provide meaningful alerts and recommendations. Machine learning algorithms provide irrigation scheduling recommendations to maintain the plant status in the optimal zone with minimal resources [26].

The Semios platform with monitoring of conditions also checks the disease condition and plant health in real time. It's a powerful tool in yield improvement that helps growers assess and respond to insect, disease, and plant health conditions. It provides sensor-based integrated pest control, whether monitoring with forecasting, disease model conditions and risk evaluation, and monitoring moisture and soil conditions using big data analysis and data prediction [27].

Challenges of IoT in Agriculture

In agriculture, for the successful implementation of IoT, there is a deployment of the large number of IoT devices because of the large area; this can arise the interference problem with the local spectrum such as ZigBee, Wi-Fi, Sigfox, and LoRa [28]. There is one more challenge of exposition of devices to the harsh environmental conditions like physical damage and degradation.

The IoT in agriculture will need a large number of IoT devices, while the lack of standardization in existing gateways and protocols leads to heterogeneity and scalability issue [28].

3.4 IoT-Integrated Smart Home/Building

A smart home and building using devices and objects connected over the Internet for remote monitoring of daily used appliances of home such as lightning, water utilization, monitoring and optimizing electrical equipment. Using smart homes and buildings concept, not only day-to-day devices like smart doors, lights are controlled but also security of home and building are monitored. IP-based cameras, alarms, motion sensors, firefighting equipment, and connected door locks give more home security. To provide such kind of automations in home and buildings, IoT-connected wireless sensors are bringing the revolution.

The IoT in conjunction with sensors provides a large number of services and applications such as smart metering to optimize the energy usage and sending the consumption data to the energy provider to reduce the waste further; in a similar manner, smart metering for water consumption can be done, which can provide great aid to societies and cities by looking into the matter of depleting water resources. In the same way, all home resources work together by sharing the information among each other processing, optimizing the tasks, and taking decision accordingly form the smart environment. Sensors optimize the home utilities based on human activity, for example temperature sensor, humidity sensor to auto control the air conditioning. For elder people alone at home it can support their medication and raise alarm in case of emergency situations, giving support to the elder people and patients [29].

Smart home works by automation of home and its appliances and minimizes the user input for controlling home appliances. One of the most common hardware platforms that is used to create a smart home application is Arduino using sensor and actuators, and for networking, Zigbee technology is mostly used. Cloud structure is an important part for big data analytics and data prediction [30]. In literature, Son et al. [31] introduced a system based on resource awareness; they mentioned mobile device access remotely to home using Web Services Description Language (WSDL) and Simple Object Success Protocol (SOAP). Energy management is also an important application in smart home and buildings in this context; Han et al. [32] suggested a new smart home energy management system (SHEMS) based on IEEE802.15.4 and ZigBee, a multi-sensing application for reducing the total energy cost. Wu et al. [33] studied the home nature of a smart home in serving its users; they mentioned a framework of intercommunication among the services and users, using the framework, and they developed two pervasive applications of “Media Follow Me (MFM)” and “Ubiquitous Skype.” To predict the user activity, a sequence prediction algorithm is proposed by

Alam et al. [34] using enhanced episode discovery. It monitors the user behavior in sequence of activities. Based on human activity patterns, Chen et al. [35] used a multi-sensor approach which consists of activity recognition from context ontology modelling and situation formation process, for real-time continuous activity recognition.

Challenges of IoT in Home and Building Structure
Heterogeneity among the IoT objects becomes one of the challenges of smart home and building; the IoT should be capable of integrating these devices seamlessly. In the case of a smart city, proposing the general architecture of IoT is hard due to a large number and different types of devices, protocols, and services [36].

Seamless connection among the devices means easy to connect anytime and anywhere in the IoT system, termed as interoperability. It's a prime concern in smart home devices and network system comes from a different vendor, so joining them to achieve interoperability becomes a challenge.

In IoT smart homes and buildings to achieve self maintenance and management becomes one of the major concern, devices should be capable of self-monitoring to optimize their health and notify the user [37].

3.5 Intelligent Transport System

The IoT is playing a big role in smart transportation giving solutions to many existing problems and providing Intelligent Transportation System. There are large numbers of issues that exist among the transport application like traffic congestion, management, minimize the environment impact due to pollution to give the benefits of transportation to commercial users and the public in general. Intercommunication applications among vehicles can be provided to help citizens save time for smarter city. Intelligent Transport System (ITS) works to improve the traffic management by reducing traffic issue, giving the prior information about real-time traffic, local convenience, seat availability, etc., which helps commuters as well as enhances their safety and comfort.

Application Areas of Intelligent Transport System
In smart city, all domains of the society will be digital to make the life of the citizens easy. The transport system for children going to school and people to office and college should be safe. In case of elderly people, the need of smart transport even rises. Old-age drivers and pedestrians have more accidental rate; a large number of application areas exist in Intelligent Transportation Systems (ITS) to enhance the user, and citizen facility in smart city like blind people can be helped by self-guidance applications and can save a lot of time of the users.

For the implementation of IoT to make smart transport, a large number of sensors are embedded in vehicles by the automotive manufacturers to enhance the road safety and better management of traffic. Government departments for road and con-

struction can use the smart ITS to enhance the road infrastructure by implementing sensors, devices, and cameras that will monitor the environment and traffic in live conditions.

The authors in [38] mentioned that ITS is providing great help in improving the road safety, reducing the traffic congestion by using a number of sensors and actuators like tire-pressure monitoring and rear-view visibility; through this, many more sensors are now embedded in vehicles to enhance and monitor the performance. Number of sensors is continuously increasing in vehicles to make the vehicles as the smarter vehicles.

In [39] the authors have mentioned that the IoT and WSN are supporting a large number of applications like logistics support, emergency services, and several other applications. Not only are the vehicles with sensors but number of sensors are also used on the roads to enhance the road safety and conditions.

Challenges of IoT in Smart Transport System

In intelligent transport system, a large number of vehicles are connected using IoT in geographically dispersed area using cloud computing centers; a huge amount of data is generated and transferred. Big data processing and analytics are performed. Due to the large amount of data created and processed, the issue of latency arises which is risky in case of medical emergency.

Fog computing brings the solution to the above problem by real-time big data analysis which gives the feature of processing data at the middleware level and the edge of nodes, but the smart transport systems have a dynamic nature, so implementing such solution becomes challenging; also, the huge amount of big data collected over the transport system is heterogeneous in nature [40].

3.6 Efficient Energy Management Using IoT

Smart utilization and management of the energy are the biggest concern of the modern society. Using IoT to make the city smart require large number of IoT-enabled applications. IoT devices are increasing in number and features, the need of power to manage these devices also grow. It is the essential need of the smart city to efficiently utilize the energy. The energy utilization information of smart homes, buildings including school's offices, amusement parks and roads street lights etc. are collected and analyzed for the optimization as also send to the grid system for proper resource utilization.

The authors in [41] mentioned that consumption of energy can be minimized by effective management of home appliances, education, and healthcare system. To manage the energy consumption of home, commercial, and industries, big data is collected from them and utilized by using various processing algorithms and making analysis. Energy management system (EMS) and data acquisition system on chip (SoC) are presented in the paper to gather the consumption data of energy from the devices. Data is sent to the centralized server where it can be processed and

analyzed. In [42] the authors propose an on-demand supply model. Here consumer is also informed about their consumption nature so that user can make decision on their consumption to reduce the cost and consumption itself.

DC-powered home concept is given in [43] as a distributed system for residential area, but due to the lack of any standardization in protocols, intelligent DC-powered home currently cannot be considered to replace the traditional system of AC supply. In [44] multiple in-home display systems (IHDs) and automatic meter reading systems (AMR) are discussed to provide energy management information. Here, the smart home system, by analyzing the proper condition of the resources, chooses by itself the display interface such as television, smartphone, etc. A home energy management system (HEMS) architecture is proposed in [45]. Here, smart meter data is used for monitoring real-time information on home energy consumption and giving online remote control to devices status. This model is only proposed for small area using the HTTP protocol, but for large residential areas, Message Queuing Telemetry Transport (MQTT) protocol is required. In [46], a model is proposed where all the nodes and devices connected in smart home plan their operations based on the weather conditions. In this system, data is sent to the Web server using Extensible Markup Language (XML) and XML files, but bandwidth issues are faced due to large size of files.

Smart grid concept is discussed in [47] for effective monitoring, smart control, and reliable and efficient power delivery. Using IoT, a smart grid is formed by having wireless sensor networks as it is the main component. The smart grid provides the smart monitoring, which is the main goal of it. Smart plugs, gateways, and meters connected to the appliances using network create a communication channel between the provider and consumer to provide a better energy production and consumption. The smart grid keeps the track of both energy generation and consumption.

Challenges in Efficient Energy Management

Various kinds of attacks can be done on smart home and buildings like impersonation/identity spoofing that aims to consume someone's energy on its behalf. Eavesdropping is another attack on IoT-based smart grid as it uses the public communication infrastructure to gain the energy consumption information of the user and households. In data tampering, attackers gain the access of modifying the exchanged data, can change the rate pricing of energy. Attackers can gain the authorization and control access and can remotely monitor and configure energy utilization information by changing the readings of smart meters and sensors. Including this private information of the users can be monitored by analyzing the usage information [48].

In general, the energy resources are volatile in nature, and smart grid should be capable of managing the volatile behavior; also, energy systems have to follow governmental laws and regulations, and this includes energy delivery that needs to be optimized according to the business needs and potential legal constraints [49].

3.7 Smart Water Management

Smart water management means various processes to manage the water resources and its consumption, in optimized way, so that there will be least wastage. We know that water depletion is a big challenge among the society; in [50] the author looks into these issues including equipment maintenance. The water management system works in conjunction with the water resources, society, and environmental systems. The water management system is fragile and continuously changing and evolving due to the different sectors from industries to agriculture, and household has a different requirement.

The utilization of water is the biggest consumer in the field of agriculture [51], while the main causes of the water wastage are leakages in distribution and irrigation. Moreover, problems like under-irrigation and over-irrigation need to be managed. The IoT in agriculture needs the integration of large number devices, objects having heterogeneous, and advanced sensors. They will work in conjunction with the software application that will implement cloud computing and big data analytics.

In [52] distribution of large number of sensors and actuators near to the water grid, water distribution resources are proposed for real-time monitoring and controlling for efficient management. Water meter and pumps are monitored and controlled in real time. A smart water quality monitoring system was proposed in [53], and an interface was designed for data storage and data processing. The different sensors used for quality monitoring are temperature sensor, turbidity sensor, pH sensor, and water flow sensor. The system is connected with the Arduino hardware for measurement and analysis. This proposed system was designed for maintaining the quality of environmental water resources reservoirs.

Jing [53] designed a model based on software using language VC++6.0 to remotely manage the water supply based on wireless sensors based on GPRS and microcontroller. Purohit and Gokhale [54] used Intel microcontroller to design a real-time water quality measurement system based on water quality measuring sensors. Beri [55] designed a device that measures in real-time various parameters of water such as pH, temperature and turbidity. In [56] the author proposed an android-based mobile application where the user can check the water level in tank using sensors, and this information will be sent to the cloud. This model can help the residential societies to minimize the water wastage level.

Several major advancements have been attempted to automate meter reading such as smart motor controlling, and automated meter reading (AMR) systems are the features of the proposed system. This model will also do troubleshooting by:

Identifying the leaks and breaks and optimizing performance through optimizing pressure, flow, and usage.

Challenges of IoT in Water Management

In water management scenarios, one of the biggest concerns is the risk of physical attacks over the devices; most of the devices are accessible, making capturing easy. Cloning of the devices can be done, by installing any malware or firmware.

Water is a vital resource for life, and management of water is facing big challenges like interoperability and lack of standardization in monitoring protocols and equipment.

Cyber security of the implemented devices in the IoT is also a big concern as devices and objects are vulnerable during networking and intercommunication [51, 57].

3.8 Environment Monitoring Using IoT

The optimization of home resources according to the usage is termed as home automation, similarly if the environment can be made to self-optimizing according to the needs of the human termed as smart environment [58]. A smart environment means making things around us easy, for example, moving heavy objects for the elderly. IoT-based smart environment focuses to facilitate our lives and to investigate its effect on human life; it gains the knowledge from inhabitants and adapts according to its inhabitants. The integration of IoT with the environment will consist of several applications to monitor and analyze the environment. These applications will enable to monitor the environment and its various parameters from the remote sites, smart home, building, transport, health, etc.; all in composition become the part of smart environment [59].

In [60] the author proposed microcontroller-based garbage bins or dustbins having IR wireless system; this system will show the current status of garbage on mobile Web browser and when the dustbins are overloaded. Air pollution is one of the biggest threats to the environment, and the main causes of the air pollution are industrialization and emission of harmful gases through vehicles; thus, a real-time monitoring is required to detect the pollutants [61]. This paper presents IoT-based solution to the air pollution problem called Polluino. This is an Arduino-based system that monitors the air pollution, and a cloud-based platform is also developed to maintain the data coming from several external sensors. The following parameters are measured to determine the quality of air carbon monoxide, carbon dioxide, nitrogen dioxide, methane, hydrogen sulfide, ozone, ammonia, particulate matter, benzene, ethanol, toluene, and propane.

In [62] this paper presents the air quality monitoring system with context awareness, which means personalizing the services based on situation and context of person or place. In a context-aware system, monitoring alone is not enough; there should be a notification system regarding citizens; there is a need to give alerts in real time; and the information provided to users should be adapted accordingly to the activity in which the user is going to be involved, and notifications should be sent accordingly. In this paper, a smart context-aware system has been proposed and implemented. This system can obtain relevant context from the user, provide real-time air quality information, and notify citizens accordingly. With such a system, we can prevent unexpected health issues related to poor air quality conditions, as

well as be able to suggest more suitable places or activities to users according to their context and current air quality. Therefore, the system provides one step forward in the scope of smart cities, improving life quality for citizens, in general, and for risk groups, in particular.

In [63] an early warning firefighting system is proposed based on the Internet of Things; it detects the early sign of fire by using the various sensors like temperature, humidity, flame, and gas. While warning message is generated based on the threshold value set in the sensors accordingly, the system generates the notification email and text message to the user's phone and switches off the main power system.

Wireless sensor networks (WSN) are providing an aid in measuring the environmental parameters in real time including environmental disaster, and live monitoring. In [64] a Raspberry Pi-based IoT system enabled with video cameras is proposed for landslide detection. The data collected by the video streaming are sent to the computer vision algorithm and generate notifications through android application.

Topographical images are used to perform the surface modelling and detect the recent activity of landslides known as Light Detection and Ranging (LIDAR) [65]. In [66] satellite images make use of image thresholding by genetic programming to detect landslide activity in a region. Bag-of-Visual-Word (BoVW) and Probabilistic Latent Semantic Analysis (pLSA) [67] methods are used for landslide detection using the image sensing classification method based on k-NN classifier to detect landslide and non-landslide region.

The authors in [68] proposed a complete solution to monitor the landslides; this architecture is composed of micrometeorological node to collect temperature, relative humidity, wind vane, wind speed, and rainfall and a ground node which measures the soil moisture at different depth.

Animals are under observation for the early detection of natural calamities [69]. This article presents that various animal can detect early the approaching disaster; therefore, the applications that use sensors and computer vision to collect data on animal behavior need to be developed. The behavior of animals is studied as an indicator of natural disasters using data processing and analysis.

In [70] the authors proposed an earthquake early warning using IoT integrated with WSN. The sensors are placed in the surface of the earth. The system is based on compression P wave and transverse S wave which radiates during the earthquake; P wave travels faster and trips the sensors, and early alert signals are generated giving humans and automated electronic system a warning to take precautionary actions with S waves. The Zigbee transmitters are used to send the alert signals, while warnings are sent to the smart phones.

Challenges of IoT in Environmental Study

Deployment of IoT to create the smart environment needs a successful meeting of certain parameters like compatibility of different products being connected. A large amount of data is generated, and attention should be given to storage, access, and processing of such big data generated by devices forming an IoT environment.

It is difficult to monitor every landslide-prone area because of the costly instrumentation and maintenance; also, the delay in sensitive information is critical to the environment [65].

Recognition of animal activities is not accurate all the time, since there can be several other parameters that can change the behavior of animals like climatic conditions, magnetic storms, seasonal factors, noise, etc. [69].

4 Comparative Analysis and Discussions

After the study of various issues and challenges in IoT, a conclusion is drawn, and it has been found that, irrespective of application areas, there are some common key issues that exist, including incorporation of WSN in the IoT, which are summed up in Table 1.

After the detailed study of the various applications and understanding the challenges in them, a detailed discussion about the IoT in healthcare and agriculture is made in Table 2, as both the applications are essential in the realization of the smart city concept. In Table 2, implementation aspects of the applications along with the main sensors used by them with their feature and contribution details are discussed.

Table 3 discusses the smart home/building; its requirement for sensing has been divided into three categories of units. With this, the features of home and building that it support are discussed.

Table 1 Challenges of IoT in WSN

Challenges	Descriptions
Inherently distributed	As IoT applications deals with video of different kind and type of systems design, a common approach for development and designing is challenging
Data management	In IoT applications, the large number of heterogeneous devices with a huge number of sensors is connected; they generate a large volume of data having different formats and are generated at different speeds. There is a need of regular application maintenance system due to risk failure of sensors or introduction of an invalid data by a malicious user
Human-centric applications	Psychological and behavioral data of humans are required to be studied, which vary from human to human; therefore, it becomes more complex to design human-centric application
Interdependent applications	Several problems in IoT applications arise due to interdependency among one or more applications; in real life, there is sharing of the resources among the applications. Services of different applications can also conflict with each other. Detecting and resolving such issues are critical and challenges in the IoT system

Table 2 Feature details of the sensors in applications

Applications	Sensor	Features	Contribution
IoT in healthcare	Accelerometer [71]	The ADXL362 from Analog Devices, 3-axis MEMS accelerometer with ultralow power utilization, which consumes less than 2 μA when the output datarate is 100 Hz and only 270 nA	The ADXL362 is an accelerometer which is used for recognizing the fall; it wakes the MCU controller up and an emergency notification generated to smartphone
	Temperature sensor [71]	It has a high accuracy range of 0.1 °C from 37 °C to 39 °C, high-resolution (16-bit) and low-power utilization (600 μA at 2.7 V to 3.3 V)	It can provide an over temperature alarm and communicate with the MCU
	Pulse sensor [71]	The pulse sensor works on low power and contains low-power light photo sensor (APDS-9008) and amplifier (MCP6001) with the typical supply current of 42 μA and 100 μA, respectively	Pulse sensor can measure the heartbeat of the radial artery at the wrist
	Chest-worn ECG monitor [72]	Three electrodes, two of them elliptical (6.5 cm and 3.5 cm), for ECG were stitched on the two sides of the torso on the belt and a circular electrode for the ground (Ø2.5 cm) next to the navel	Long-term ECG recording, distant expertto identify cardiovascular problems earlier
IoT in agriculture	Temperature sensor [73]	The LM 35 sensor is vastly used because its output voltage is linear with the Celsius scaling of temperature. The range isfrom −55 degrees to +150 degrees	Used as an indicator of water level inside a tank and water resources
	Moisture sensor [73]	There is the principle of open and short circuit. The output is high or low reflected by the LED	Sensor used to sense the moisture level of soil
	PIR sensor [73]	PIR sensors detect the infrared radiation generated or reflected from an object	This sensor detects the progress of people, animals, and other things
	Humidity sensor [74]	The HDC1010 digital humidity sensor is used to measure the moisture and humidity level in the environment	The HDC1010 is stronger against dirt, dust, and other ecological impurities

Table 3 Sensor unit type of smart home and building

	Sensing unit type	Power supply	Features
IoT-integrated smart home/building [58]	Hot water system monitoring	Electrical outlets	Real-time monitoring of warm water and solar heating system
	Household electrical appliance monitoring and controlling	Electrical outlets	Monitoring and controlling of normal domestic appliances such as battery charging units, room heaters, washing machines, refrigerators
	Measuring environment temperature	Battery	Sensors are capable of measuring the room temperature accordingly and enable to regulate the usage of the appliances

5 Conclusions

In this paper, a detailed study of IoT applications is done with the major issues and challenges in their implementation. After the study, a conclusion has been drawn that there are some common issues among all the applications related with the integration of WSN with the Internet of Things (IoT). Later in the chapter, implementation details of the key sensors used in the applications with its features are discussed. A requirement of edge-based open and flexible architecture that can support the heterogeneity and scalability issue is also proposed. This paper will aid the researchers to understand the representation of the physical world of devices and objects connected over the network using wireless sensors.

References

1. Seth, P., Sarangi, S.R.: Internet of things: architectures, protocols, and applications. J. Electr. Comput. Eng. **2017**, (2017)
2. Jin, J., Gubbi, J., Marusic, S., Palaniswami, M.: An information framework for creating a smart city through internet of things. IEEE Internet Things J. **1**(2), 112–121 (2014)
3. Giri, A., Dutta, S., Neogy, S., Dahal, K., Pervez, Z.: Internet of things (IoT): a survey on architecture, enabling technologies, applications and challenges. In: Proceedings of the 1st International Conference on Internet of Things and Machine Learning, p. 7. ACM (2017)
4. Talari, S., Shafie-Khah, M., Siano, P., Loia, V., Tommasetti, A., Catalão, J.: A review of smart cities based on the internet of things concept. Energies. **10**(4), 421 (2017)
5. Bawany, N.Z., Shamsi, J.A.: Smart city architecture: vision and challenges. Int. J. Adv. Comput. Sci. Appl. **6**(11), 246–255 (2015)
6. Al-Qaseemi, S.A., Almulhim, H.A., Almulhim, M.F., Chaudhry, S.R.: IoT architecture challenges and issues: lack of standardization. In: Future Technologies Conference (FTC), pp. 731–738. IEEE (2016)
7. Li, Y., Björck, F., Xue, H.: Iot architecture enabling dynamic security policies. In: Proceedings of the 4th International Conference on Information and Network Security, pp. 50–54. ACM (2016)

8. Hashem, I.A.T., Chang, V., Anuar, N.B., Adewole, K., Yaqoob, I., Gani, A., et al.: The role of big data in smart city. Int. J. Inf. Manag. **36**(5), 748–758 (2016)
9. Aazam, M., Zeadally, S., Harras, K.A.: Offloading in fog computing for IoT: review, enabling technologies, and research opportunities. Futur. Gener. Comput. Syst. **87**, 278–289 (2018)
10. How To Build a Holistic Smart City Architecture.: Retrieved from https://www.iotforall.com/holistic-smart-city-architecture/ (2019)
11. Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M.L., Tarricone, L.: An IoT-aware architecture for smart healthcare systems. IEEE Internet Things J. **2**(6), 515–526 (2015)
12. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., Mankodiya, K.: Towards fog-driven IoT eHealth: promises and challenges of IoT in medicine and healthcare. Futur. Gener. Comput. Syst. **78**, 659–676 (2018)
13. Sodhro, A.H., Luo, Z., Sangaiah, A.K., Baik, S.W.: Mobile edge computing based QoS optimization in medical healthcare applications. Int. J. Inf. Manag. **45**, 308–318 (2019)
14. Sohn, S.Y., Bae, M., Lee, D.K.R., Kim, H.: Alarm system for elder patients medication with IoT-enabled pill bottle. In: 2015 International Conference on Information and Communication Technology Convergence (ICTC), pp. 59–61. IEEE (2015)
15. Laranjo, I., Macedo, J., Santos, A.: Internet of things for medication control: service implementation and testing. Procedia Technol. **5**, 777–786 (2012)
16. Kalantarian, H., Motamed, B., Alshurafa, N., Sarrafzadeh, M.: A wearable sensor system for medication adherence prediction. Artif. Intell. Med. **69**, 43–52 (2016)
17. Marques, G., Pitarma, R.: An indoor monitoring system for ambient assisted living based on internet of things architecture. Int. J. Environ. Res. Public Health. **13**(11), 1152 (2016)
18. Rghioui, A., Sendra, S., Lloret, J., Oumnad, A.: Internet of things for measuring human activities in ambient assisted living and e-health. Netw. Protoc. Algorithms. **8**(3), 15–28 (2016)
19. P. Raj and A. C. Raman, The Internet of Things: Enabling Technologies, Platforms, and Use Cases. Boca Raton, FL, USA: CRC Press (2017)
20. Lee, I., Lee, K.: The Internet of Things (IoT): applications, investments, and challenges for enterprises. Bus. Horiz. **58**(4), 431–440 (2015)
21. J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, and D. Boyle, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Amsterdam, The Netherlands: Elsevier (2014)
22. Tzounis, A., Katsoulas, N., Bartzanas, T., Kittas, C.: Internet of Things in agriculture, recent advances and future challenges. Biosyst. Eng. **164**, 31–48 (2017)
23. Patel, K.K., Patel, S.M.: Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. International journal of engineering science and. Computing. **6**(5), (2016)
24. Solutions for Smart Farming (Agriculture IoT).: Retrieved from https://www.kaaproject.org/smart-farming (2019)
25. Powerful software for running a modern farm.: Retrieved from https://farmlogs.com (2019)
26. The Phytech Platform.: Retrieved from https://www.phytech.com/ (2019)
27. Semios We Help Growers Worry Less.: Retrieved from https://semios.com/ (2019)
28. Elijah, O., Rahman, T.A., Orikumhi, I., Leow, C.Y., Hindia, M.N.: An overview of Internet of things (IoT) and data analytics in agriculture: benefits and challenges. IEEE Internet Things J. **5**(5), 3758–3773 (2018)
29. Sundmaeker, H., Guillemin, P., Friess, P., Woelfflé, S.: Vision and challenges for realising the Internet of things. Clust. Eur. Res. Proj. Internet Things Eur. Commiss. **3**(3), 34–36 (2010)
30. Soliman, M., Abiodun, T., Hamouda, T., Zhou, J., Lung, C.H.: Smart home: integrating internet of things with web services and cloud computing. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, vol. 2, pp. 317–320. IEEE (2013, December)
31. Son, J.-Y., et al.: Resource-aware smart home management system by constructing resource relation graph. IEEE Trans. Consum. Electron. **57**, 1112–1119 (2011)
32. Han, D.-M., Lim, J.-H.: Design and implementation of smart home energy management systems based on zigbee. IEEE Tran. Consum. Electron. **56**, 1417–1425 (2010)

33. Wu, C.-L., Fu, L.-C.: Design and realization of a framework for human–system interaction in smart homes. IEEE Trans. Syst. Man Cybern. **42**, 15–31 (2012)
34. Alam, M.R., et al.: SPEED: an inhabitant activity prediction algorithm for smart homes. IEEE Trans. on Systems, Man and Cybernetics. **42**, 985–990 (2012)
35. Chen, L., Nugent, C.D., Wang, H.: A knowledge-driven approach to activity recognition in smart homes. IEEE Trans. Knowl. Data Eng. 961–974 (2012)
36. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of things for smart cities. IEEE Internet Things J. **1**(1), 22–32 (2014)
37. Pradeep, S., Kousalya, T., Suresh, K.A., Edwin, J.: Iot and its connectivity challenges in smart home. Int. Res. J. Eng. Technol. **3**, 1040–1043 (2016)
38. Guerrero-Ibáñez, J., Zeadally, S., Contreras-Castillo, J.: Sensor technologies for intelligent transportation systems. Sensors. **18**(4), 1212 (2018)
39. Abdelhamid, S., Hassanein, H.S., Takahara, G.: Vehicle as a mobile sensor. Procedia Comput. Sci. **34**, 286–295 (2014)
40. Darwish, T.S., Bakar, K.A.: Fog based intelligent transportation big data analytics in the internet of vehicles environment: motivations, architecture, challenges, and critical issues. IEEE Access. **6**, 15679–15701 (2018)
41. Ejaz, W., Naeem, M., Shahid, A., Anpalagan, A., Jo, M.: Efficient energy management for the internet of things in smart cities. IEEE Commun. Mag. **55**(1), 84–91 (2017)
42. Al-Ali, A.R., Zualkernan, I.A., Rashid, M., Gupta, R., Alikarar, M.: A smart home energy management system using IoT and big data analytics approach. IEEE Trans. Consum. Electron. **63**(4), 426–434 (2017)
43. Rodriguez-Diaz, E., Vasquez, J.C., Guerrero, J.M.: Intelligent DC homes in future sustainable energy systems: when efficiency and intelligence work together. IEEE Consum. Electron. Magaz. **5**(1), 74–80 (2016)
44. Kim, D.S., Son, S.Y., Lee, J.: Developments of the in-home display systems for residential energy monitoring. IEEE Trans. Consum. Electron. **59**(3), 492–498 (2013)
45. Son, Y.S., Pulkkinen, T., Moon, K.D., Kim, C.: Home energy management system based on power line communication. IEEE Trans. Consum. Electron. **56**(3), 1380–1386 (2010)
46. Kushiro, N., Suzuki, S., Nakata, M., Takahara, H., Inoue, M.: Integrated residential gateway controller for home energy management system. in IEEE Trans. Consum. Electron. **49**(3), 629–636 (2003)
47. Ozger, M., Cetinkaya, O., Akan, O.B.: Energy harvesting cognitive radio networking for iot-enabled smart grid. Mob. Netw. Appl. **23**(4), 956–966 (2018)
48. Bekara, C.: Security issues and challenges for the IoT-based smart grid. Procedia Comput. Sci. **34**, 532–537 (2014)
49. Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I.A.T., Siddiqa, A., Yaqoob, I.: Big IoT data analytics: architecture, opportunities, and open research challenges. IEEE Access. **5**, 5247–5261 (2017)
50. Robles, T., Alcarria, R., de Andrés, D.M., de la Cruz, M.N., Calero, R., Iglesias, S., López, M.: An IoT based reference architecture for smart water management processes. JoWUA. **6**(1), 4–23 (2015)
51. Kamienski, C., Soininen, J.P., Taumberger, M., Fernandes, S., Toscano, A., Cinotti, T.S., et al.: SWAMP: an IoT-based smart water management platform for precision irrigation in agriculture. In: 2018 Global Internet of Things Summit (GIoTS), pp. 1–6. IEEE (2018)
52. Ntuli, N., Abu-Mahfouz, A.: A simple security architecture for smart water management system. Procedia Comput. Sci. **83**, 1164–1169 (2016)
53. Nikhil, R., Rajender, R., Dushyantha, G.R., Jagadevi, N.: Smart water quality monitoring system using IoT environment. Int. J. Innov. Eng. Technol. **10**(4), (2018). Jing, M.: The design of wireless remote monitoring system of water supply based on GPRS. In: Computer Science and Society (ISCCS), 2011 International Symposium on, Kota Kinabalu, pp. 29–31 (2011)
54. Purohit, A., Gokhale, U.: Real time water quality measurement system based on GSM. IOSR J. Electron. Commun. Eng. **9**(3), 63–67 (2014)
55. Beri, N.N.: Wireless sensor network based system design for chemical parameter monitoring in water. Int. J Electron. Commun. Soft Comput. Sci. Eng. **3**(6),

56. Wadekar, S., Vakare, V., Prajapati, R., Yadav, S., Yadav, V.: Smart water management using IOT. In: 2016 5th International Conference on Wireless Networks and Embedded Systems (WECON), pp. 1–4. IEEE (2016)
57. Koo, D., Piratla, K., Matthews, C.J.: Towards sustainable water supply: schematic development of big data collection using internet of things (IoT). Procedia Eng. **118**, 489–497 (2015)
58. Kelly, S.D.T., Suryadevara, N.K., Mukhopadhyay, S.C.: Towards the implementation of IoT for environmental condition monitoring in homes. IEEE Sensors J. **13**(10), 3846–3853 (2013)
59. Ahmed, E., Yaqoob, I., Gani, A., Imran, M., Guizani, M.: Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wirel. Commun. **23**(5), 10–16 (2016)
60. Navghane, S.S., Killedar, M.S., Rohokale, V.M.: IoT based smart garbage and waste collection bin. Int. J. Adv. Res. Electron. Commun. Eng. **5**(5), 1576–1578 (2016)
61. Fioccola, G.B., Sommese, R., Tufano, I., Canonico, R., Ventre, G.: Polluino: an efficient cloud-based management of IoT devices for air quality monitoring. In: 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow (RTSI), pp. 1–6. IEEE (2016)
62. Garcia-de-Prado, A., Ortiz, G., Boubeta-Puig, J., Corral-Plaza, D.: Air4People: a smart air quality monitoring and context-aware notification system. J. Univ. Comput. Sci. **24**(7), 846–863 (2018)
63. Eltom, R.H., Hamood, E.A., Mohammed, A.A., Osman, A.A.: Early warning firefighting system using internet of things. In: 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), pp. 1–7. IEEE (2018)
64. Aggarwal, S., Mishra, P.K., Sumakar, K.V.S., Chaturvedi, P.: Landslide monitoring system implementing IOT using video camera. In: 2018 3rd International Conference for Convergence in Technology (I2CT), pp. 1–4. IEEE (2018)
65. McKean, J., Roering, J.: Objective landslide detection and surface morphology mapping using high-resolution airborne laser altimetry. Geomorphology. **57**(3–4), 331–351 (2004)
66. Rosin P.L., Hervas J.: Image Thresholding for Landslide Detection by Genetic Programming (unpublished)
67. Gong, C., Lei, G., Tianyun, Z., Junwei, H.: Automatic landslide detection from remote-sensing imagery using a scene classification method based on BoVW and pLSA. Int. J. Remote Sens. **34**(1), 45–59 (2013)
68. El Moulat, M., Debauche, O., Mahmoudi, S., Brahim, L.A., Manneback, P., Lebeau, F.: Monitoring system using internet of things for potential landslides. Procedia Comput. Sci. **134**, 26–34 (2018)
69. Pirmagomedov, R., Blinnikov, M., Amelyanovich, A., Glushakov, R., Loskutov, S., Koucheryavy, A., et al.: IoT based earthquake prediction technology. In: Internet of Things, Smart Spaces, and Next Generation Networks and Systems, pp. 535–546. Springer, Cham (2018)
70. Alphonsa, A., Ravi, G.: Earthquake early warning system by IOT using Wireless sensor networks. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1201–1205. IEEE (2016)
71. Wu, T., Wu, F., Redouté, J.M., Yuce, M.R.: An autonomous wireless body area network implementation towards IoT connected healthcare applications. IEEE Access. **5**, 11413–11422 (2017)
72. Mankodiya, K., Hassan, Y.A., Vogt, S., Gehring, H., Hofmann, U.G.: Wearable ECG module for long-term recordings using a smartphone processor. In: Proceedings of the 5th International Workshop on Ubiquitous Health and Wellness, vol. 2629. Copenhagen, Denmark (2010)
73. Suma, N., Samson, S.R., Saranya, S., Shanmugapriya, G., Subhashri, R.: IOT based smart agriculture monitoring system. Int. J. Recent Innov. Trends Comput. Commun. **5**(2), 177–181 (2017)
74. Prathibha, S.R., Hongal, A., Jyothi, M.P.: IOT based monitoring system in smart agriculture. In: 2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT), pp. 81–84. IEEE (2017)

Karan Bajaj received his Bachelor of Engineering in Computer Science in 2009 and Master of Engineering in Computer Science in 2013 and is currently pursuing PhD. He is currently Assistant Professor in the Department of Computer Science and Engineering in Chitkara University His main research interests include machine learning, wireless network, and IoT.

Bhisham Sharma received a PhD in Computer Science and Engineering from the PEC University of Technology (formerly Punjab Engineering College), Chandigarh, India. He is currently Associate Professor in the Department of Computer Science and Engineering, Chitkara University, India. His research interests include mobile computing, wireless communication, wireless sensor networks, wireless mesh networks, network security, and Internet of Things. He has published more than 30 papers in international and national journal/conferences.

Raman Singh is working as Assistant Professor with the Computer Science and Engineering Department, Thapar Institute of Engineering and Technology Patiala (India). He has completed PhD (CSE) from the University Institute of Engineering and Technology, Panjab University, Chandigarh, on February 2016. He has completed Master of Engineering (IT) from UIET, Panjab University, Chandigarh, in May 2010. He has published 14 research papers in international journals and conferences. He has won Best Publication of the year 2016 award from UIET Panjab University. He is currently executing three funded research projects. He has served the Information Technology industry for 2 years as a technology solution consultant. He is a Microsoft Certified Technology Specialist (MCTS) and Microsoft Technet Certified Technology Expert. His area of interest includes intrusion detection, network security, and machine learning.

Impact of IoT-Based Smart Cities on Human Daily Life

Ghazanfar Latif, Jaafar M. Alghazo, R. Maheswar, P. Jayarajan, and A. Sampathkumar

1 Introduction

Since the dawn of man, human beings have shown huge interest in living in groups. This group evolved from couples to tribes, from tribes to villages, from villages to cities; but why? Studies have shown that people feel safe when they are in groups. Nowadays, people prefer living in the cities. According to a UN study in 2016, the statistics show that 54.5% of the total populace currently live in urban areas. In addition, the UN anticipates that by 2030, 60% of the total populace will live in modern cities [1]. Thus, what we can conclude from that is individuals will live in urban areas; now, the question is, are these cities ready for that? Some cities barely handle the number of people they already have as illustrated by traffic problems, health problems, security problems, and housing problems. Therefore, cities must solve these problems before more people inhabit them! One of the presented solutions is called a Smart City. Therefore, this chapter will analyze the problems and advantages in modern cities and the reasons why we need Smart Cities. In addition, the chapter will define and analyze the concept of Smart Cities, showing how the IoT is an important factor, critique the existing model—IBM's—highlight the

G. Latif (✉) · J. M. Alghazo
Department of Computer Science, Prince Mohammad Bin Fahd University, Al-Khobar, Saudi Arabia
e-mail: glatif@pmu.edu.sa; jghazo@pmu.edu.sa

R. Maheswar
School of Electrical & Electronics Engineering (SEEE), VIT Bhopal University, Bhopal, Madhya Pradesh, India

P. Jayarajan
Department of ECE, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

A. Sampathkumar
School of Computing Science and Engineering, VIT Bhopal University, Bhopal, India

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_6

advantage of Smart Cities, and try to present new solutions for the disadvantages. Moreover, since the Internet of Things (IoT) is presently getting to be a one-on-one promising technology in this world, big data analysis is becoming a powerful tool to be used to build a Smart City.

2 The Modern City

Today, the cities of the world face variuos challenges, including job opportunity, economic growth development, ecological supportability, and social versatility. Emanations and pollutants from car engines have turned into a noteworthy well-structured contamination in huge and medium-sized world urban areas. Numerous substantial urban communities experience authentic air pollution and ozone damaging substance radiation, which is aggravated by growing development. Considering these challenges, the European Association and various countries are placing assets into ICT research and progression toward making methodologies to upgrade the individual fulfilment of locals and the practicality of urban networks. Of the human population, 54.5% of us live in Modern cities. However, it varies from one region to another. The following basic factors lead a city to be called Modern:

Health Centers Specifically, easy access to hospitals and clinics for everyone in the city.

Transportation It is the vein that runs any city, without it, the city will be paralyzed and messy, and people will depend more on cars since there is no public transportation.

Investment Job opportunities; we can say it is the most important factor in this list, because we can say that health centers are investments, and we can say the same thing for transportation too. Also, it is the reason why people move from villages to cities and from one country to another. More investment equals more jobs; also note that investment is nothing without security, which is our next point.

Security The factor that holds everything together. The first thing anyone who wants to move to a new place thinks about is safety and security. Without it investments will decline as no one wants to invest in a troubled place.

2.1 Problems in Modern Cities

Human factor This is the most significant problem in Modern Cities. While not all humans have a bad influence on cities, here, the meaning refers to how dependent on humans cities are, in every detail. People need to be trained, and most importantly, they need professional ethics in order to eliminate behaviors such as long lunch breaks, piling paperwork, and missing deadlines. All these reasons make some cities

slower and slower, thus becoming inefficient. Moreover, humans can only work for a limited time such that if there is a problem at night, hopefully, it will be fixed the following morning. Therefore, automating some tasks such as driving will save a lot of our resources.

Human–Machine interaction People in Modern Cities are not used to having a lot of interaction with machines, except for simple machines such as parking lot meters and ATMs. Everything else is human–human interaction, and that wastes a lot of time. Humans should automate routine tasks. That is a very huge disadvantage to this model.

Thus, to solve these problems, people came up with a model called the Smart City. Next, we will define it, introduce a famous model, then critique it, but first we will explain the backbone of the Smart City [2].

3 IoT – The Backbone

The IoT can be characterized as the tremendous interconnection of smart gadgets. This concept is applied from small sensors to large vehicles. Some people consider the IoT as the fourth generation of computers, and that is how important IoT systems are. Many people use them every day, without even knowing. If you want to know whether you use the IoT or not, let us break down its name and definition, "The expanding interconnection of smart devices". Thus, it is the connection or a communication among smart devices. Or rather, from its name Internet of Things, as internet—communication or interconnection—of things such as smart devices [3]. The IoT has helped society and businesses around the globe uniquely unlock new and immense chances to access volumes of information and present new and distinctive applications and administrations to make a superior future for the urban community, diminishing force utilization, and enhancing productivity of the general public.

3.1 Role of the IoT in Smart Cities

The IoT is all related in one way or another to communication among different devices in different places [4]. The IoT is going to play an important defined role in every field of industry and daily life activities. Let us take Smart Housing and Smart Vehicles as an example to explain the role of the IoT in development of Smart Cities.

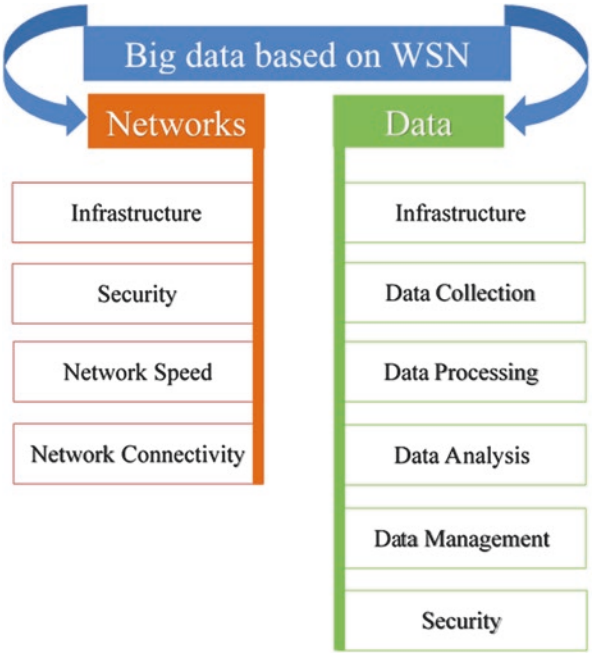
In a Smart House, there are infinite applications for the Internet of things. We can apply it on doors, so that if a friend or family member is waiting for you outside the house, you can easily unlock the door, because the key is connected to the internet. Also, you can apply it in the kitchen. There is a refrigerator that tells you

when a product is going to expire. Furthermore, it also has an internal camera that shows you the missing products so that you can get them while you are at the supermarket. One of our colleague once said: Maybe one day the refrigerator will come to me instead of me going to it. While that was said as a joke, who knows, maybe it will come true one day. Also, you can integrate the IoT in the bedrooms and so on [5].

A second example is Smart Vehicles. What we mean here is not vehicles that help you park or have a camera with some ultrasound sensors; rather, we are talking about driverless cars such as Teslas, Waymos, and future options. These cars are very useful for all people. The vehicles enable people to sleep, study, prepare for a meeting while traveling, or they can be used to transport children, elderly, or people who have difficulty driving such as blind people. It is also applicable to fix any issue related to it with just a software update. The new smart car now is called Tesla Model 3 that offers a double engine all-wheel drive, 20″ Execution Haggles, and lowered suspension for aggregate control, in every single climate condition. What is more, a carbon fiber spoiler enhances security at high speeds, enabling the Model 3 to accelerate from 0 to 60 mph within 3.3 seconds [6].

3.2 Role of 5G Technology in the IoT and Big Data Analysis

The brisk development and improvement of 5G technology in the Internet of things, Cloud computing, software-defined networks, and big data analytics, has made dependable headway and formed a solid relationship between them. For instance, the IoT applications that generate information with enormous volume and smart speed require 5G, with attributes of high information rate and low laziness, to transmit such information quicker and more reasonably. Obviously, that information likewise needs the Cloud for processing and storage, and moreover, a software defined network to give a flexible structure framework to move this giant volume of information in an ideal manner. This topic investigates the associations among the improvement of the Internet of things, the Cloud, big data, and the software-defined networks in the coming 5G period, and we can perceive them as the five most valuable ICTs (information and trades progress) to watch for in 2020 in terms of their potential, blend, and applications. 5G improvement creative work has presently begun, and some 5G highlights or subsystems are already accessible. By embedding 5G compact broadband in the center, 5G will fill in as a predominant passage and transport sort out for IoT applications so that IoT data can be passed on even more profitably and monetarily [7]. Plus, IoT will end up one of the genuine wellsprings of big data by conveying a gigantic volume, at quick speed, and different assortments of information. The mass proportion of information being made by the IoT can change everything from collecting to therapeutic administrations to the plans and workings of sagacious urban regions—empowering them to work more gainfully and valuably than ever before.



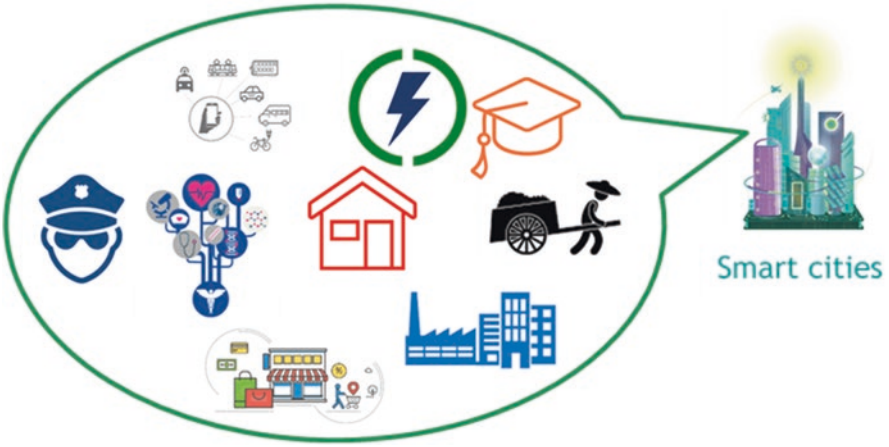
3.3 The Smart City

A Smart City explores, experiments with, and uses technologies—such as the IoT—to improve its community [8]. The goal of Smart Cities is to build a sustainable and modern environment by applying IoT technologies to help the nation serve its population [9]. A Smart City has the same properties as the Modern City with some major adjustments as follows:

Smart Housing From its name, you may think we mean Smart homes, but that is not the case. Although it is a part of The Smart City, what concern us here in this chapter is how neighborhoods are designed, what services they have in case of emergency, and so on, which we will explain more in the IBM definition section [10].

Smart Security It has the same basics we explained before in The Modern City section; here, we are going to focus more on cyber security, as we are going to see in the IBM model, sensors and cameras are all over the place. There must be a strong system that safely stores all the private information. Also, the City runs on communication systems; therefore, the government must keep the online communication ready at all times. Additionally, security in general will be improved, because there will be cameras; we can not only film the criminal but also identify them. This is because of computer vision algorithms and methods and movement analysis technologies such as face detections.

Smart healthcare Healthcare is an integral part of any community, but in the Smart City, it is a bit different. A large number of sensors are connected in one web frame that can be accessed by the hospital facility and family members [11]. The hospital facility can use the data stored in the web to see the patient history, diseases, medication that the patient uses, and emergency contact. Also, family members can get notifications when the patient is in the hospital.



4 Impact of Smart Cities on Human Life

The United Nation organization has a great example of Smart Cities that they want to be different from all the cities around the world. As a result, they asked the UNECE and some of their partners to join them for this huge project. They will be focusing on mobility and sustainable houses, having clean energy, and achieving cities using the IoT [12].

The United Nation program of world Smart Cities created Sustainable Development Goals (SDGs) to know the exact level of performance compared to any city in any place. These SDGs are a piece of the programs. The main goals of it are wide, yet every one has a different rundown of focuses to accomplish.

4.1 Eliminate Poverty

Obliterating dejection in all world structures remains presumably the best feat defying humankind. Extensively, more than 800 million people are currently living on under $1.25 every day; numerous requirements include adequate sustenance, clean drinking water, and sanitation. SDGs are resolved to end dejection in all circum-

stances and structures by concentrating on those living in defenseless conditions, extending access to basic resources and organizations, and reinforcing systems affected by hardship and climate related fiascos.

4.2 Eliminate Hunger

Hunger has been around forever, and we must fight it through the Smart Cities program that the United Nation created. To be able to eliminate this problem before it kills more people, we need to collaborate and to eliminate it from all the cities on the Earth. These are generally titanic achievements as lack of strong sustenance remains a huge issue in various nations. In 2014, 795 million individuals were surveyed to be interminably undernourished as a fast-delayed consequence of typical debasement, dry spells, and loss of biodiversity. More than 90 million children younger than five are hazardously underweight. Furthermore, one in four people in Africa are still hungry.

4.3 Responsible Consumption

Accomplishing money related progression and rational improvement necessitates that we drastically alter our impression of nature by changing the way we make and fund things and assets. Farming eats up a lot of water the world over. Regardless, the current water structure guarantees around 70% of all freshwater for human use. The valuable association of our ordinary trademark assets and the way wherein we discard poisonous waste and toxins are central focuses to accomplish this objective. Empowering attempts, affiliations, and buyers to reuse and decrease waste is similarly essential, as is supporting nations to move toward sensibly practical occurrences of utilization by 2030.

4.4 Gender Equality

Gender equality is not only a basic human right but also an essential foundation for a quiet, prosperous, and sensible world. Outfitting women and young women with proportionate access to preparation, restorative administrations, decent work, and depiction in political and money related essential initiative techniques will fuel doable economies and favorable social request positions, and humankind will be free to move around at will. We have seen astounding improvement starting now, and they should continue into the foreseeable future. Increasingly, young women are by and by in school in contrast from 15 years earlier, and most areas have accomplished gender equality with fundamental guidance.

4.5 Clean Drinking Water

Water deficiency impacts in excess of 40% of individuals in the world, an angering wonder that is predicted to increase with the ascending of temperatures, even though 2.1 billion individuals have gotten improved water sanitation since 1990. Decreasing supplies of safe drinking water are an important issue influencing each mainland.

4.6 Affordable Energy

Somewhere between 1990 and 2010, the number of individuals with access to power reached 1.7 billion, and as the population keeps rising, so will the excitement for a weather-beaten vitality. A general economy subject to oil subordinates, and the advancement of ozone-depleting substance discharges, is negating genuine upgrades to our air structure. This is affecting each territory. Starting in 2011, endeavors to significantly empower clean energy accomplished in excess of 20% of power being made by unlimited sources. Still, one out of seven individuals needs access to power, and as the interest keeps ascending, there should be a general increase in the amount of reasonable power sources throughout the world.

4.7 Building New Industries

Enthusiasm for structure and headway are basic drivers of money related advancement and improvement. Creative headway is the way to discover suffering responses for both financial and natural challenges. For instance, giving new occupations and propelling imperativeness capability. Advancing reasonable endeavors, and putting resources into clever research and progress, are unfathomably basic approaches to invigorate fiscal improvement.

4.8 Acts against Climate Change

There is no nation on the planet that is truly not encountering the remarkable impacts of change. Ozone-depleting substance floods continue to rise and are now 50% higher than their 1990 estimation. Also, a general temperature adjustment is rolling out alterations in our atmosphere structure, which relates to irreversible results if we do not make a move now. The yearly customary mishaps from waves, tropical storms, and flooding mean a couple of billions of dollars, requiring an undertaking

of US$6 billion reliably in a calamity threat alone. The objective intends to gather $100 billion reliably by 2020 to address the necessities of making nations prepared and help moderate condition related calamities.

4.9 Greater Life on Earth

Human life relies on the earth as much as the sea for our sustenance and occupations. Vegetation makes up 80% of our food source, and we depend upon horticulture as an essential cash related asset and methods for progress. Forests make up 30% of the world's surface, providing habitat for myriad animal varieties and pivotal hotspots for clean air and water; and they are basic for engaging normal change. Today, we are seeing unimaginable land debasement and the loss of 30% of arable land to different events at a veritable rate. The dry season and desertification are also on the rise every year, connoting the loss of 12 million hectares and affecting poor frameworks all around. Out of the 8300 creature breeds known, 8% are dying out and 22% are in danger of extinction.

4.10 Peace and Justice Around the World

Without concordance, soundness, human rights, and convincing organization, in perspective on the standard of law—we cannot look for viable progression. We are confronting a day by day reality with the end goal that is dynamically parceled. A couple of territories have acknowledged and proceeded with measurements of agreement and accomplishment, while others fall into plainly vast cycles of contention and savagery. This is in no way, shape or form, unavoidable and must be tended to. Anomalous measures of prepared violence and slightness ruinously influence a country's improvement, affecting money related advancement and normally achieving long-standing grumblings that can crop up for a very long time. Sexual severity, bad behavior, misuse, and torment are in like manner pervasive where there is a war or no standard of law, and nations must take measures to ensure the well-being of the general population who are most in peril.

5 The Critique on Smart Cities

Every scientific advancement has its drawbacks. Therefore, in our critique we hope to highlight the disadvantages to help guide future researchers and designers who are interested in the Smart City in their own research and models. First, the high level of complexity in the city, due to all the connected components of all embedded

systems and sensors, complicates the network and may cause a lot of damage to the city. How many workers are required to maintain the embedded systems and sensors? Also, there is the question of, what is the raw data going to be used for? Are we even able to process all this data in real time? Thus, alongside this complexity of network, we need a strong processing unit working all day and night to analyze the data collected from the embedded systems and sensors. The second thing is the storage units. All the unprocessed data and the processed ones need a place to be stored and also secure backups. Additionally, some of the collected data are private, such as your car movement and water usage. Some of this data may be used to benefit the city's database, someone can argue, but some of them, such as car movements are a huge breach of privacy [13].

Another problem in the IBM model for a Smart City is that in case of an extreme emergency, they base their solutions for saving the city on the existence of a nearby Smart City, which is difficult and expensive. Also, what guarantees that what affected the first Smart City would not affect the second Smart City? The problems highlighted above are very critical, in our opinion. We hope future researchers and designer solve them; in the next section we will present some solutions.

5.1 Solutions

The most critiqued point in the present model is the distribution of embedded systems and sensors; if we could find a method for an efficient distribution, we would save a lot of money from lower system maintenance and its original cost. Also, fewer embedded systems and sensors means less data to process and store, which also would save a lot of money [14]. Additionally, if we could develop some deep learning and machine learning algorithms, these algorithms would decrease the number of relevant data that the city uses, so we would have a small number of storage units compared to what is represented in the model above. Another problem is that the Smart City should be fully prepared in case of emergency. The Smart City must be able to stand on its own. We could achieve that by using high end robots; these robots can help the Smart City officials to decrease the human factor such as fighting natural disasters [15].

6 Conclusion

To conclude with, we trust that we gave you a decent look at the idea of the Smart City and how the fourth era of PC—The Internet of Things—is going to assume an enormous role in its advancement. We likewise accept that Smart Cities are the eventual fate of any up and coming human progress, and we trust this chapter helped or if nothing else enlivened somebody to illuminate and build up this idea.

References

1. Wahome, M., Mbatia, P.: Causes of under-nutrition in Mukuru and Viwandani urban informal settlements. Am. J. Food Sci. Nutr. **1**(1), 25–34 (2017)
2. Song, H., et al.: Smart Cities: Foundations, Principles, and Applications. John Wiley & Sons, Hoboken, NJ (2017)
3. Tyagi, A.K.: Building a smart and sustainable environment using Internet of Things. Available at SSRN 3356500 (2019)
4. László, G.E.R.E.: An introduction and critical assessment of smart city developments. Deturope. **10**(3), 33–52 (2018)
5. Kar, A.K., et al. (eds.): Advances in Smart Cities: Smarter People, Governance, and Solutions. CRC Press, Boca Raton (2017)
6. Huh, S., Cho, S., Kim, S.: Managing IoT devices using blockchain platform. In: 2017 19th International Conference on Advanced Communication Technology (ICACT). IEEE (2017)
7. Lin, B.S.P., Lin, F.J., Tung, L.P.: The roles of 5G mobile broadband in the development of IoT, big data, cloud and SDN. Commun. Netw. **8**(01), 9 (2016)
8. Batty, M.: Big data, smart cities and city planning. Dialogues Hum. Geogr. **3**(3), 274–279 (2013)
9. Assembly, General: Sustainable Development goals. (SDGs), Transforming our world: the 2030 (2015)
10. Gaur, A., et al.: Smart city architecture and its applications based on IoT. Procedia Comput. Sci. **52**, 1089–1094 (2015)
11. Kulkarni, A., Sathe, S.: Healthcare applications of the Internet of Things: a review. Int. J. Comp. Sci. Inf. Technol. **5**(5), 6229–6232 (2014)
12. Wenge, R., et al.: Smart city architecture: a technology guide for implementation and design challenges. China Commun. **11**(3), 56–69 (2014)
13. Hepbasli, A., Alsuhaibani, Z.: A key review on present status and future directions of solar energy studies and applications in Saudi Arabia. Renew. Sust. Energ. Rev. **15**(9), 5021–5050 (2011)
14. Stallings, W.: Computer Organization and Architecture: Designing for Performance. Pearson Education India, Upper Saddle River, NJ (2003)
15. Komarevtseva, O.O.: Smart city technologies: new barriers to investment or a method for solving the economic problems of municipalities? R-Economy. **3**(1), 32–39 (2017)

Ghazanfar Latif is a research coordinator (Deanship of Graduate Studies and Research) and PhD scholar at the University of Malaysia Sarawak, Malaysia. He earned his MS degree in Computer Science from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2014 and his BS degree in Computer Science from FAST National University of Computer and Emerging Sciences, Pakistan, in 2010 while remaining on the Dean's honor list. Throughout his educational carrier, he has received a number of achievements such as a full scholarship for FSc, BS-CS, and MS-CS. He worked as an Instructor at Prince Mohammad bin Fahd University, Saudi Arabia for 3 years in the CS Department and has 2 years industry work experience. His research interests include Image Processing, Artificial Intelligence, Neural Networks, and Medical Image Processing.

Jaafar M. Alghazo obtained his PhD and MSc in Computer Engineering from Southern Illinois University Carbondale, in 2004 and 2000, respectively. He joined Prince Mohammad Bin Fahd University (PMU) as founding Dean of the College of Computer Engineering and Science and held various positions, including Dean of Graduate Studies and Research, Dean of Institutional Relations, and Dean of Continuing Education and Community Service. Currently, he is an Assistant Professor at PMU. His research interests include Modeling and Realization of Biological Mechanism using CAD and FPGAs, Modeling and Realization of Arithmetic Operations using CAD and FPGAs, Low Power Cache Design, and Assistive Technology for students with disabilities.

R. Maheswar completed his B.E. (ECE) at Madras University in 1999, M.E. (Applied Electronics) at Bharathiyar University in 2002, and Ph.D. in the field of Wireless Sensor Network at Anna University in 2012. He has about 17 years of teaching experience at various levels and presently works as an Associate Professor in the School of EEE at VIT Bhopal University, Bhopal. He has published 40 papers in International Journals and Conferences. His research interests include Wireless Sensor Network, IoT, Queueing Theory, and Performance Evaluation.

P. Jayarajan completed his B.E. (EEE) at Madurai Kamaraj University in 2004, M.E. (Applied Electronics) at Anna University in 2008, and Ph.D. in the field of Wireless Sensor Network at Anna University in 2018. He has about 11 years of teaching experience and presently works as an Associate Professor in the Electronics and Communication Engineering Department, Sri Krishna College of Technology, Coimbatore. He has published 15 papers in International Journals and Conferences. His research interests include Wireless Sensor Network, Modeling and Simulation, and the IoT.

A. Sampathkumar received his Bachelor in Information Technology in 2009, Master in Mainframe Technology in 2012, and Ph.D. in 2019 at Anna University Chennai. He has 8 years of academic experience and currently works as an Assistant Professor in the school of CSE at VIT Bhopal University, Bhopal. He has published several articles in peer-reviewed journals and is a member of CSI societies. His research interests include Artificial Intelligence, Data Mining, Machine Learning, IoT, Data Analytics, and Optimization Techniques.

Internet of Things: Reformation of Garment Stores and Retail Shop Business Process

Ghazanfar Latif, Jaafar M. Alghazo, R. Maheswar, P. Jayarajan, and A. Sampathkumar

1 Introduction

In order to define the concept of the IoT, it's important to understand the meaning of the Internet. The internet can be defined as a worldwide system that connects computers via the concept of computer networks, specifically using the Internet protocol suite (TCP/IP). Furthermore, the IoT surpasses the concept of Internet by proposing a system to connect not only smart devices such as computers and smartphones, but also it enables normal devices that are not technologically advanced such as kitchen devices, medical devices or light bulbs to interact and make decisions spontaneously with each other without the interference of humans. Therefore, IoT embedded sensors and other devices can be considered as physical devices to make the communication possible with the Internet through physical or wireless networks [1].

Related concepts of IoT existed since the 1970s. However, in 1999, Kevin Ashton, a British technology expert, first created the term IoT, and it was intended to describe a new technology connecting the technology of radio frequency identification (RFID) and the technology of Internet. Nevertheless, the term IoT received

G. Latif (✉) · J. M. Alghazo
Department of Computer Science, Prince Mohammad Bin Fahd University, Al-Khobar, Saudi Arabia
e-mail: glatif@pmu.edu.sa; jghazo@pmu.edu.sa

R. Maheswar
School of Electrical & Electronics Engineering (SEEE), VIT Bhopal University, Bhopal, Madhya Pradesh, India

P. Jayarajan
Department of ECE, Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

A. Sampathkumar
School of Computing Science and Engineering, Bhopal, India

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_7

no attention until 10 years after. Huge international companies started using the term to establish new strategies for their technologies.

Moreover, IoT was invented to guarantee efficiency, speed and accuracy for users through their lives, instead of relying on people to manually input commands to machines, requiring more time, extraordinary effort and attention to details, which is difficult for human beings to have all at one time and for long periods of time. Therefore, IoT has become of great importance since it supports the concept of self-automation by performing at a high level around the clock. Specifically speaking, IoT has recorded some significant life-changing experiences in the retail stores through some of its applications including smart shelves, robot employees, beacons and much more [2].

2 Current Issues in Garment and Retail Store Methodology

In physical garment and retail stores, stores sell clothes of different companies from different countries. Some stores are branches of the official companies while others are not. Many stores get clothes from wholesale with customers being completely unaware. Upon looking at these clothes, it is quite evident that some are indeed fake brands. The meaning of fake brands is having stores sell clothes with the trademarks of different companies, when, in reality, the clothes have no affiliation with their official companies whatsoever. The fake brands also use materials that are not durable and are not good to use for long time periods. Despite that, these fake brands share the same prices of the original pieces made from the official companies while costing much less to produce. The main issue is that some customers buy clothes without checking the authenticity. For example, customers fail to ask themselves what type of clothes they are looking at. Which company made them? How much should it cost? Customers should be able to fully recognize these fake shops and avoid them. Another main issue is that numerous garment and retail stores do not provide information about their clothes, including the type of clothes, the company that originally made them, details about sizes and average height and weight that fits to the person. This type of information should be presented to the customer. The quality of colour of clothes is also important to look at. Most fake brands are made of low-quality materials and colours. Once washed, the clothes begin to change in colour. If original brand clothes were to be put in washing machines alongside fake brands, all clothes will be affected by the colours of the fake brand. The third issue of garment stores is that some stores do not provide payment by card while simultaneously not having any change. Numerous customers face issues attempting to pay the stores for the goods they attempt to purchase. For example, the ATM is far away from the store; the consumer will waste their time going to ATM machines and coming back to the store to pay, thus reducing number of customers. Some people simply do not like carrying cash. The fourth issue is that some garment stores do not provide services to the customers, including lists, regulation and sticker with the price of the items. Also, some sellers are unhelpful to customers; in those cases, the customer feels uncomfortable buying. Finally, business people should choose the best location for the garment stores.

Stores located in main cities and malls, where many people come, are far more likely to generate traffic. Stores also need great logos potentially using laser lights to attract customers. Advertising is the best way to attract customers, some locations of garment stores are not in main places where people go to every day, and owners do not have enough budget to make advertisements of their garment stores. In this case, they are unable to achieve any profits and eventually go out of business. Figure 1 shows the current methods of garment and retail store shipment.

The sales of online purchases are increasing and all the industries are focusing on new technologies and integration of IoT to their garment and retail shops. Figure 2 shows the statistics of retail electronic sales in the United States from the period

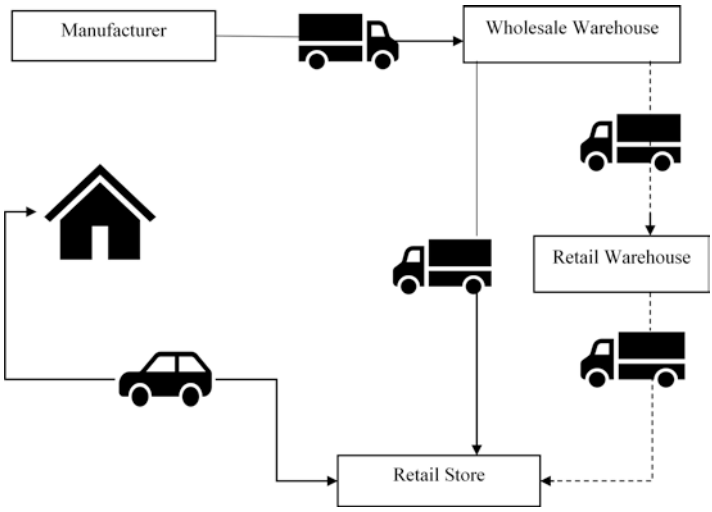


Fig. 1 Traditional retail product

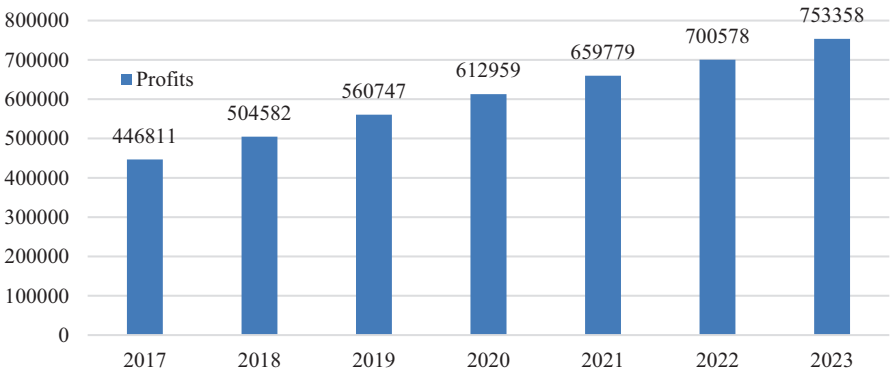


Fig. 2 Retail sales in the United States in years 2017–2023

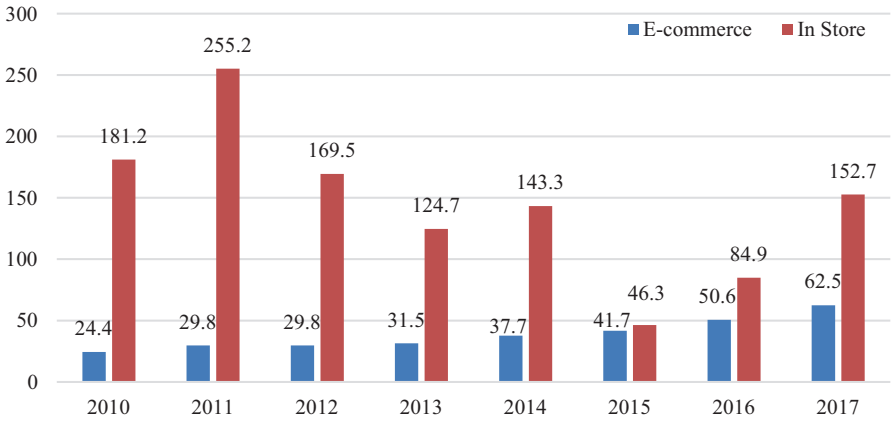


Fig. 3 Comparison between E-commerce and in-store sales (in US dollars)

2017–2023 [3]. Figure 3 shows the online versus in-store shopping up to 2017 [4]. Clearly in-store purchases are still dominant which has more justification to incorporate IOT in stores for a smart shopping experience.

3 Challenges for Using IoT in Garment and Retail Shops

Privacy and security are the primary challenges linked with the IoT solutions. The access to the consumer database offers retailers many opportunities to defraud the customers and increases the chances of cyberattacks [5]. Further, many retailers do not have the basic setup and network to handle large chunks of data generated by IoT. Consequently, the retail stores require significant infrastructure changes to accommodate Internet-based retail. Considerable investment is required by the retailer when it comes to IoT implementation. This is the primary reason that retailers still weigh the advantages of IoT systems against the cost of implementation [6].

Park and other authors published a study concerned with the interactive digital signage application [7]. This classic IoT application functions by receiving direct command from both machines and humans. Additionally, it creates a wireless environment to integrate all commands the system receives. Different issues can arise from this approach such as data collision, scalability issues and high cost and complexity of deployment. Therefore, another technology is introduced to resolve these issues; the technology utilizes the concept of container-based distributed virtual client architecture that avoids all previously mentioned issues by controlling the flow of data on different domains and processing them effectively. Finally, the results of this study have shown that the cloud-based server architecture takes the request from each user, which is then sent to the digital signage server resulting in less dependency on the distance with an average of 50% for all customers.

Moreover, another research by Grewal et al. focuses on analysing the different methods that enable the IoT in the retail industry [8]. The business model is one of the fundamental factors in the online retail industry. It proposes identification and organizing the data received from customers according to different business models, resulting in efficient performance when data is needed for analysis. Another method is the virtual mall technique, meaning the creation of large platforms by websites to host brands and merchants online such as Amazon. Also, the aggregator method is the use of data collected from retailers and collaborating with them in creating trading environments between sellers and customers. Lastly, the search agent method provides an extremely fast and optimized service to provide a software to search for your item accordingly.

The study done by Balaji et al. proposes that IoT will grow the co-creation value in the retail industry [9]. Data was collected from 289 customers that experienced the technology of IoT in the retail industry. Using data analysis techniques and the result of measuring the partial least squares (PLS) equation, it was possible to find that some essential elements had the largest impact on the customer feedback and the increasing value of the co-creation which are the ease of use, the superior functionality, the aesthetic appeal and the presence. Figure 4 shows the IoT value of co-creation concept with the business platforms, platform interoperability and educational platforms.

Qing et al. discuss the RFID technology and its implementation in the retail industry. Specifically, the RFID is used to create technology to support the idea of smart shelves that can be used in the retail industry to make a significant contribution to increasing sales, enabling auto-generated reports about products for managers

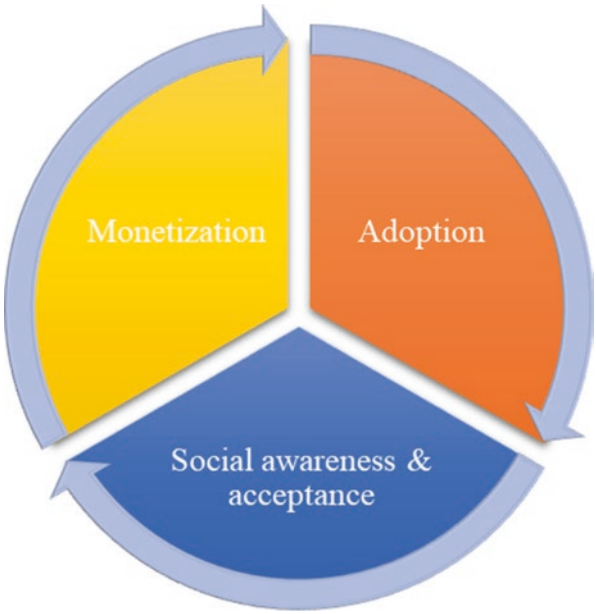


Fig. 4 IoT value of co-creation concept

as well as consumers. In addition, it is extremely comfortable for both the sellers and the consumers. The RFID consists of three fundamental pieces including an antenna system, a multiplexer and a reader or writer; thus, these important elements enable a direct connection with the system, providing data and information about the availability of products, their location, expiry date, etc. [10].

Elliot and Fowell investigate the experiences of customers who shop through the Internet to determine the possible factors that may promote or inhibit the habit. The authors collected data using open questionnaires that focused on several parameters [11]. This included ease of use, convenience and the ability of the model to meet their demands. The findings revealed that customers were satisfied with 70% of the services provided, particularly regarding the extensive amount of available goods, convenience and customized service. However, issues concerning security and the ease of use of the platform emerged. Nevertheless, many people were willing to complete their shopping online. Therefore, the article is crucial in demonstrating how the Internet has improved the ability of retailers to meet the needs of their customers with convenience.

Burnes and Towers examined the development of Omnichannel retailing within the fashion industry and how its knowledge could influence smart cities. Customers are given the ability to select different convenient ways of purchasing a product, such as identifying a product and ordering it online or visiting a showroom to confirm its specifications. By establishing a physical presence, the authors contend that retailers have the option of selling more products to a consumer than in a virtual world. The researchers used deductive reasoning to arrive at this conclusion. Hence, the paper addresses the importance of physical infrastructure even in the age of the IoT [12].

Bilinska-Reformat and Stefanska identify the target market when integrating the IoT with the retail market and garment stores. The researchers used critical analysis of existing literature and observation of young customers in retail chains in Poland to collect the necessary information. According to the findings, young customers have embraced the use of technology in their shopping. As a result, several retail chains began integrating their services with the IoT when targeting this market. The article is crucial in examining the target market for retail firms that have integrated their services with IoT [13].

Many people are discouraged from using the Internet for shopping due to problems with privacy and security. Brill investigates ways in which a person could build trust and maximize benefits despite the challenges associated with the IoT. The author uses an exploratory research style to make assumptions and arrive at conclusions. The author states that increased stringent policies could increase accountability and transparency amongst firms that deal with big data, which would reduce the challenges affecting the IoT. Therefore, retail companies can establish stronger legislation to protect a client's privacy and security, resulting in the enhancement of the integration of the IoT in this sector [14].

Shankara, Mahanta, Arora and Srinivasamurthy study the influence of the IoT in the retail industry. Notably, the authors critique available literature to investigate how the IoT has revolutionized garment stores and retail sectors, thus enhancing

profitability. According to Shankara et al., technology will result in a paradigm shift and the data collected will facilitate the creation of knowledge that can contribute to value added. As such, the article highlights the benefits of integrating the IoT in garment stores and amongst retailers [15].

Dlamini and Johnston explore the usefulness of the utilization of IoT in the retail industry and stores [16]. The authors explore existing research to gather appropriate data and draw conclusions. The authors find out that the intensive use of the IoT in garment stores and the retail industry is attributable to its unique ability in identifying products, ease of communication and the ability to provide real-time information [17]. For instance, the use of sensors could be used to track the shelves with the highest traffic; this knowledge can be of advantage in increasing sales. The information gathered by IoT devices can be analysed to understand consumer behaviour and shape marketing strategies. Additionally, customers could use the technology to track the location of specific products, while retailers could use it to replenish shelves. Therefore, the article provides vital insight into the applicability of IoT in the retail industry.

Today's marketplace is described as a competitive market. Every consumer is looking for the easiest way to purchase products. IoT is the highest-trending technique that retailers are using to set their businesses on the right track. However, they are faced with many challenges in the industry. Retailers need to be informed about the input data from the server including coming and going customers, the purpose of coming into the store and how that translates to the revenue of the store. The procedure of buying by using the IoT procedure is based on sensors. Whenever the sensor has caught the items, it will import the product to the application as a message including name, unit and colour set. After that, the seller will be informed about ongoing and outgoing customer transactions even if the buyer were to refund the items.

Certainly, whenever technology techniques are published, retailers are expected to think about new capabilities including organization and technology areas. This technology should be in well-chosen areas with the appropriate cultures, knowledge and structure to secure and assure the rights of the business. Moreover, the IT department is not enough to save the market; the business department is another aspect of this field required to make the organization strong and survive by having new ideas and solutions for marketing the products [18].

4 Proposed Methodology

There are many new looks of clothes provided by a handful of companies such as American Eagle and sport clothes like Nike and Adidas. In the business activities, nowadays social media is one of the marketing tools used to increase business sales, clothing companies making accounts on Facebook, Instagram and Twitter to introduce their products. This activity makes it easier for customers to search for new clothes based on their interests through online shopping instead of physically going

to shops. Some shops post their social media handles on the door or on the desk. One of the reasons that makes online shopping less efficient than traditional shopping is the customers need to customize materials of garments they purchase meaning they need the "feel and touch experience". Price is one of the attributes that attracts customers to online stores. Customers' brains rely on visual attention to process information that promotional websites present for the setting and product. Some clothing retailers use Facebook as their primary shopping website allowing consumers to order via email or phone. Additionally, some clothing stores with Instagram accounts post links of their websites or Facebook accounts. This is how the marketing works and achieves sales through social media. As physical shopping moved to online shopping, it has become easier in modern days. There are many mobile applications that are designed for shopping for clothes, electrical devices, food, etc. On mobile applications, *JOLLYCHIC*, *SHEIN* and *NAMSHI FASHION*, all popular in Arabian gulf countries, are known as the top applications of shopping. The customers can choose their size, colour and colours and feel like they are designing their own clothes.

Another technology is the beacon devices, which are devices installed with low-energy Bluetooth that gets activated within limited range of the network. Therefore, beacons become handy when customers enter the area supported with this technology. Upon entering places such as malls and markets they will be notified of discounts of sales and special offers to make them more likely to enjoy real-time experiences in shopping. Also, beacons provide retail companies with customers' updates and data to provide customized services and grab customer's attention [19].

Figure 5 shows the proposed model to use of IOT in the garment industry. As shown in Fig. 5, a customer can use his/her access to the Internet to make online

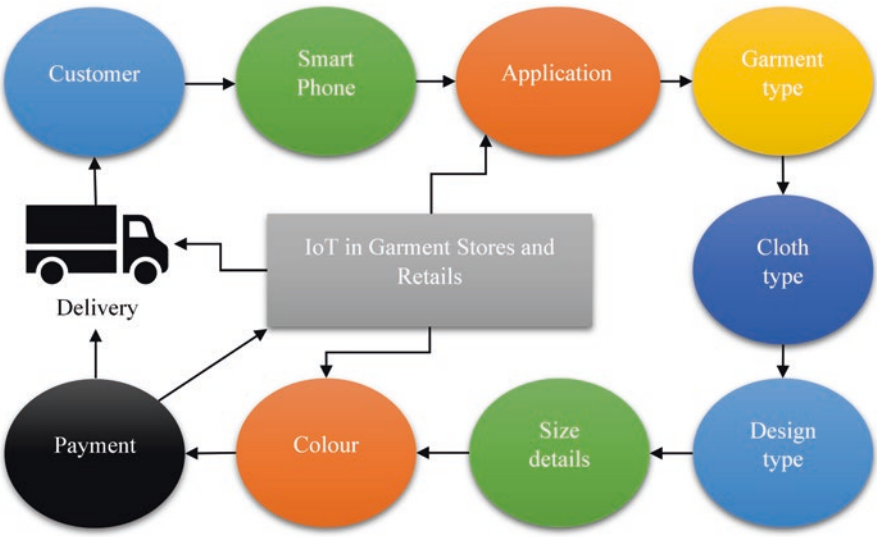


Fig. 5 Proposed model for usage of IoT technologies for online garment stores

purchases detailing garment type, design, size, etc., and make the payment. This shopping experience is coordinated through the use of IOT including shipping and tracking of the item until it is delivered. User interface (UI) is one of the most important strategies in developing store applications and making them successful. The user should fully understand the information provided to browse for their needs, for example, organizing and accessing the database using tabs and lists, search button and account creation. This study has been done by Andrea Savage who created the *iOS Application for Inventory in Small Retail Stores* [20]. As technology has improved and many applications have been designed to serve users, most people have become dependent on their smartphones as part of their daily lives. They can understand types of products without asking the seller. However, there are many people that do not use smartphone technology, who are mostly old people; they prefer to go to stores and "shop traditionally" instead of shopping online. They like to see everything directly rather than seeing it on a monitor. Some garment and retail stores provide sewing services for customers, with measuring giving body sizes.

Smart shelf technology is a convenient inventory management system and one of the most outstanding applications of IoT. Smart shelf wireless system generates real-time updates to its system that can be accessed by employees. It notifies employees about information such as products' availability and expiration dates. In addition, the technologies used to keep track of the products include built-in weight sensors within the shelves. Also, it requires RFID readers and tags placed on each product to help optimize the system and send notifications to the system when products are not organized to their assigned shelves accordingly. Therefore, this system performs and deals effectively with the huge amount of data it collects and analyses it automatically [21]. Figure 6 shows the integration of RFID as middleware of IoT-based garments and retail shops.

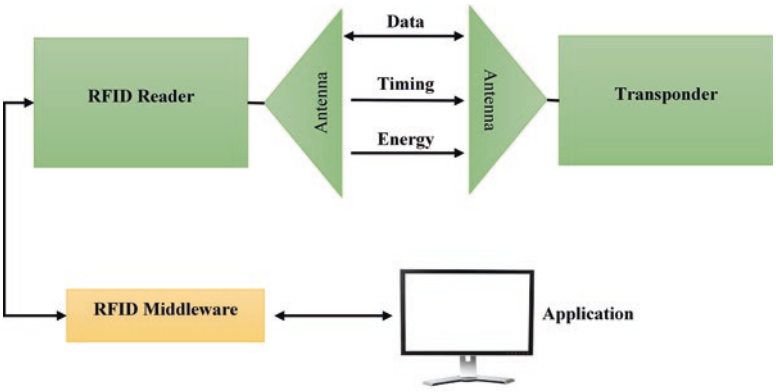


Fig. 6 The integration of RFID in retail shops

5 Benefits

With the advancement in technology, the IoT implements hi-tech sensors to collect and analyse data for retail and garment stores and further facilitates necessary actions [22]. The contemporary customer wants to understand how the product was made and how can it be maintained. The IoT can permit retailers to communicate about a specific product and can also enable them to meet the customized need for the product: for example, what types of cloth are used in the T-shirt? Where is it made and by which company? How long can it be used? What is the average of appropriate height and weight for the person who will wear it? These are the most important information for the customer.

IoT offers the garment stores and retailers the chance to refine the purchasing process of the customers in a store. The IoT could allow incorporation of elements such as customized pricing based on the acquisition history and brand loyalty. The retailers can efficiently collect their orders and track individual items through the supply chain, which will give details of each product and arrival time easily [23]. IoT also safeguards the retailers with fraud identification and loss prevention. Counterfeit products make up approximately 5–7% of the total world trade. Moreover, brands expend considerable resources to curb such fraudulent occurrences. So, the IoT is used to track brands and identify the counterfeit goods while averting the fraudulent sales that use their brand name.

Further, IoT technology can offer a clear overview of the stocks and thereby facilitate the optimization of the brand's storage and automatic replenishment of their stocks. What makes it more efficient is that these actions are aligned to the needs of the customers. It also enables retailers to target high-end clients. Before entering a store, customers often perform comprehensive research about the products they wish to purchase. The stores can keep a record of the browsing history of their customers, their visits, purchasing patterns, the amount they spend, to develop a productive relationship. Moreover, for a personalized experience, the store staff can recommend options based on the browsing record and previous purchases made by the customer at the store. The garment and retail stores can use IoT to understand the needs of their customers better and improve customer services [24].

IoT has become a relationship of the digital world with the real world. Key determinants for IoT is value of co-creation, coinciding with rapid improvement in information technology (IT) the last few years. IoT has become more active in our daily lives. While IoT is still under development and upgrading, it is generally known that the IoT is a pattern where technology equips networking, identifying and processing in order to gain communication with other devices through the Internet to perform desired tasks. IoT is recognised amongst the top techniques of technology that are expected to create business breakthroughs in the beginning of the 2020s. McKinsey expects of the 2020s the existence of over 30 million IoT objects, which will have an effectiveness that guarantees the US $11 trillion per year by 2025. While the area of applications for IoT technology is vast, it is also one of the most prominent areas of business sales including retail industries. For the concept of IoT in smart

networking objects, it is tagged with unique identifiers as a quick response code or RFIDs. A German grocery retailer (Dohle) uses smart carts to provide information of products at the store, which enables checkout without wasting the time of waiting for retrieval information in exact time. Therefore, retailers can develop and improve retail systems using IoT technology, creating real-time experiences and interaction with customers. IoT technology can help buyers make their decisions and positively contribute to their overall shopping experience [9].

IoT has existed for several years now. It was introduced by the MIT audio-ID centre. In the future internet, there are many terms to characterise the future development of the network. There are services of IoT like 3D Internet. Moreover, the collaboration will continue, and more efforts of countries will increase the development of IoT like Japan and the United States. From the economic perspective, the future Internet will depend on websites to optimize economic services, allowing garment and retail stores to save parts of their budgets. There will be multiple services through the Internet; these services will make the difference between high-level business service and low-level sensor services in the IoT. The purpose of IoT is to make contact between the physical world and representation of the information system; this is how IoT is described [25]. Campolargo et al. speak about converging technologies for smart environments and integrated ecosystems; the book predicts the future of IoT services, such as garment stores, workplaces, restaurants and hospitals. All machines can communicate with each other using sensors including computers, embedded system machines, smart discs, etc. These sensors allow all devices to retrieve information and databases from other devices and access them; auto-accessing information can save money while completing the process faster than humans [26].

6 Conclusion

In conclusion, this chapter discussed the concept of IoT in the retail industry by analysing the most common and efficient methods and technologies. Technologies include RFID smart shelf, interactive image technology (IIT) and low-energy Bluetooth beacons. Therefore, IoT enables the direct connection between objects or even humans and objects. It creates a great opportunity to manage and deal with numerous data that is increasing over time, which normal humans cannot deal with due to their limited capabilities and limited time. However, machines do not have time limits if designed efficiently and kept on routine maintenance. Machines do not get tired either which makes a major difference between humans and machines with respect to their performance, quality and speed. Moreover, each technology was discussed while exploring their advantages, disadvantages, results and other supporting techniques used to implement and utilize them accordingly in effective ways. In addition, many of the studies discussed in this paper have implemented different experiments and studied cases where they took into consideration the feedback from customers who experienced the impact of IoT in the retail industry.

The results indicated that many customers are satisfied with the services provided by these technologies, whereas some customers had concerns regarding their private information and how retail companies make use of their personal information.

References

1. Shang, W., et al.: Challenges in IoT networking via TCP/IP architecture. Technical Report NDN-0038. NDN Project (2016)
2. Rezaei, S., Emmi, M.: Apps-commerce in emerging markets: insights and future business models. In: Apps Management and E-Commerce Transactions in Real-Time, pp. 51–69. IGI Global, Hershey (2017)
3. Clement, J.: Retail e-commerce sales in the United States from 2017 to 2023 (in Million U.S. dollars) (2019). Retrieved from https://www.statista.com/statistics/272391/us-retail-e-commerce-sales-forecast/
4. Cordero, M., Levy, S.: E-commerce retail sales hit $453.5 billion in 2017, as brands invest in omnichannel. Retrieved from http://www.cbre.us/real-estate-services/real-estate-industries/retail-services/research-and-insights/us-marketflash-e-commerce-2017/
5. Pacheco, J., Hariri, S.: IoT security framework for smart cyber infrastructures. In: 2016 IEEE 1st International Workshops on Foundations and Applications of Self∗ Systems (FAS∗ W). IEEE (2016)
6. Vikram, N., et al.: A low cost home automation system using Wi-Fi based wireless sensor network incorporating Internet of Things (IoT). In: 2017 IEEE 7th International Advance Computing Conference (IACC). IEEE (2017)
7. Park, Y., et al.: Design and implementation of a container-based virtual client architecture for interactive digital signage systems. Int. J. Distrib. Sens. Netw. **13**(7), 1–14 (2017)
8. Grewal, D., Iyer, G.R., Levy, M.: Internet retailing: enablers, limiters and market consequences. J. Bus. Res. **57**(7), 703–713 (2004)
9. Balaji, M.S., Roy, S.K.: Value co-creation with Internet of things technology in the retail industry. J. Mark. Manag. **33**(1–2), 7–31 (2017)
10. Qing, X., Chen, Z.N., Cai, A.: Multi-loop antenna for high frequency RFID smart shelf application. In: 2007 IEEE Antennas and Propagation Society International Symposium. IEEE (2007)
11. Elliot, S., Fowell, S.: Expectations versus reality: a snapshot of consumer experiences with Internet retailing. Int. J. Inf. Manag. **20**(5), 323–336 (2000)
12. Burnes, B., Towers, N.: Consumers, clothing retailers and production planning and control in the smart city. Prod. Plan. Control. **27**(6), 490–499 (2016)
13. Bilinska-Reformat, K., Stefanska, M.: Young consumers' behaviours in retail market and their impact on activities of retail chains. Bus. Excell. **10**(2), 123 (2016)
14. Brill, J.: The internet of things: building trust and maximizing benefits through consumer control. Fordham Law Rev. **83**, 205–217 (2014)
15. Ciuciu, I., et al.: On the move to meaningful internet systems: OTM 2015 workshops. In: On the Move to Meaningful Internet Systems: OTM 2015 Federated Conferences and Workshops. Springer, Cham (2015)
16. Dlamini, N.N., Johnston, K.: The use, benefits and challenges of using the Internet of Things (IoT) in retail businesses: a literature review. In: 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE). IEEE (2016)
17. Zhang, Y., Wen, J.: An IoT electric business model based on the protocol of bitcoin. In: 2015 18th International Conference on Intelligence in Next Generation Networks. IEEE (2015)
18. Gehrt, K.C., Yan, R.-N.: Situational, consumer, and retailer factors affecting Internet, catalog, and store shopping. Int. J. Retail Distrib. Manag. **32**(1), 5–18 (2004)

19. Sornalatha, K., Kavitha, V.R.: IoT based smart museum using Bluetooth low energy. In: 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-informatics (AEEICB). IEEE (2017)
20. Savage, A.: iOS Application for Inventory in Small Retail Stores, Software Engineering Project Report. California Polytechnic State University (2016)
21. Parada, R., et al.: Using RFID to detect interactions in ambient assisted living environments. IEEE Intell. Syst. **30**(4), 16–22 (2015)
22. Fernández-Caramés, T., Fraga-Lamas, P.: Towards the internet-of-smart-clothing: a review on IOT wearables and garments for creating intelligent connected E-Textiles. Electronics. **7**(12), 405 (2018)
23. Kumar, A., Ting, P.: RFID & Analytics Driving Agility in Apparel Supply Chain, Master Thesis. MIT - Massachusetts Institute of Technology. (2019)
24. Gaur, L., Singh, G., Ramakrishnan, R.: Understanding consumer preferences using IoT SmartMirrors. Pertanika J. Sci. Technol. **25**(3), 939–948 (2017)
25. Haller, S., Karnouskos, S., Schroth, C.: The internet of things in an enterprise context. In: Future Internet Symposium. Springer, Berlin, Heidelberg (2008)
26. Fantana, N.L., et al.: IoT applications—value creation for industry. In: Vermesan, O., Friess, P. (eds.) Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, pp. 153–204. River Publishers, Aalborg (2013)

Ghazanfar Latif is a research coordinator (Deanship of Graduate Studies and Research) and PhD scholar at University of Malaysia, Sarawak, Malaysia. He earned his MS degree in Computer Science from King Fahd University of Petroleum and Minerals, Saudi Arabia, in 2014 and BS degree in Computer Science from FAST National University of Computer and Emerging Sciences, Pakistan, in 2010 by remaining in Dean's honor list. Throughout his educational carrier, he got a number of achievements like full scholarship for FSc, BS-CS and MS-CS. He worked as an Instructor at Prince Mohammad bin Fahd University, Saudi Arabia, for 3 years in CS Department and has a 2-year industry work experience. His research interests include image processing, artificial intelligence, neural networks and medical image processing.

Jaafar M. Alghazo obtained his PhD and MSc in Computer Engineering from Southern Illinois University, Carbondale, in 2004 and 2000, respectively. He joined Prince Mohammad Bin Fahd University (PMU) as founding Dean of the College of Computer Engineering and Science and held various positions including Dean of Graduate Studies and Research, Dean of Institutional Relations and Dean of Continuing Education and Community Service. Currently he is Assistant Professor at PMU. His research interests include modelling and realization of biological mechanism using CAD and FPGAs, modelling and realization of arithmetic operations using CAD and FPGAs, low-power cache design and assistive technology for students with disabilities.

R. Maheswar has completed his BE (ECE) from Madras University in the year 1999, ME (Applied Electronics) from Bharathiar University in the year 2002 and PhD in the field of Wireless Sensor Network from Anna University in the year 2012. He has about 17 years of teaching experience at various levels and presently working as an Associate Professor in the School of EEE, VIT Bhopal University, Bhopal. He has published 40 papers at International Journals and International Conferences. His research interest includes wireless sensor network, IoT, queueing theory and performance evaluation.

P. Jayarajan has completed his BE (EEE) from Madurai Kamaraj University in the year 2004, ME (Applied Electronics) from Anna University in the year 2008 and PhD in the field of Wireless Sensor Network under Anna University in the year 2018. He has about 11 years of teaching experience and presently working as an Associate Professor in the Electronics and Communication Engineering Department, Sri Krishna College of Technology, Coimbatore. He has published 15 papers at International Journals and International Conferences. His research interest includes wireless sensor network, modelling and simulation and IoT.

A. Sampathkumar received his Bachelor in Information Technology in 2009, Master's in Mainframe Technology in 2012 and PhD degree in 2019 under Anna University Chennai. He has 8 years of academic experience and currently working as Assistant Professor in the school of CSE, VIT Bhopal University, Bhopal. He had published several articles in peer-reviewed journals and a member of CSI societies. His research interest includes artificial intelligence, data mining, machine learning, IoT, data analytics and optimization techniques.

Toward Smart Urban Development Through Intelligent Edge Analytics

Mahmoud Abu Zaid, Mohamed Faizal, R. Maheswar, and Osamah Ibrahiem Abdullaziz

1 Introduction

Urban population of the world has seen a rapid growth, from 751 million in 1950 to 4.2 billion in 2018 [1]. According to UN 55% of all world's population lives in urban areas and this figure is predicted to go up, by as much as 68% by 2050. The net effect of urbanization according to projections in the growth of global population is another 2.5 billion people will be added to urban areas by 2050, with close to 90% of this demographic expected to be in Asia and Africa [1]. All of this means the world has been becoming urban and the trend is poised to continue in the future.

An increase in urban population comes with its own set of associated challenges in several areas, some of which include: an increase in environmental pollution, managing increasingly complex transportation system, making healthcare accessible for growing population, making government services accessible to all citizens, and providing safety and security to all population. All of these has led to the increase in intelligence in cities and a trend toward smart urban development by taking advantage of existing IoT technologies to mitigate most of the abovementioned issues; we will explore a few solutions in this chapter.

M. A. Zaid · O. I. Abdullaziz
Department of Electrical Engineering & Computer Science, National Chiao Tung University, Hsinchu City, Taiwan
e-mail: abozedmn.03g@g2.nctu.edu.tw; yabolahan.04g@g2.nctu.edu.tw

M. Faizal (✉)
Department of Electronics Engineering, National Chiao Tung University, Hsinchu City, Taiwan
e-mail: mohamedfaizal.ee05g@nctu.edu.tw

R. Maheswar
School of Electrical & Electronics Engineering (SEEE), VIT Bhopal University, Bhopal, Madhya Pradesh, India

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_8

The current technological framework is primarily based upon cloud and local computing with increasing reliance on edge and fog in the recent years. With the expected growth in gathering large amounts of data ("big data") in highly populated urban areas, cloud-based technologies suffer from major shortcomings, which we will highlight in this chapter; we will also present the technological trends to mitigate the same.

In moving toward the next generation of innovative and more capable applications, IoT big data analytics comes as an important cornerstone. With the current wave of the rapidly increasing data volumes, which are generated by many sensors, actuators, and devices, the need for decision-making and extracting knowledge out of this data is a necessity. IoT big data analytics plays an important role in achieving the same. The real-time response requirement stated by emerging applications, such as connected vehicles, arises a new challenge. Therefore, edge computing came into the picture to overcome the delay of processing the data entirely on the cloud. In this chapter, we show the current design approaches, protocols, and technologies that are being proposed for IoT big data analytics on both the cloud and the edge in the context of smart urban development. Also, we present some of the use cases that fit the context of smart cities and urban development.

With the recent boom in IoT and related technologies the trend in urban development has been toward increasing intelligence, i.e., it's common to see "smart cities" where sensors are deployed in key areas and the data collected is processed using intelligence analytics. Efficient machine learning algorithms are used to enable previously unavailable services and making available services more accessible; this is the whole paradigm of smart city development [2].

More recently with the explosion in the fields of IoT, big data analytics, and artificial intelligence, there is a convergence among all these fields in the context of urban development; this paradigm shift has led to what we call "cognitive smart cities" [3]. All of this will be further elaborated in this chapter.

2 Edge Networking for Internet of Things

Wireless networks will eventually become key enablers of ultra-reliable and low-latency applications. The driving force for wireless systems is the demand for high-quality applications which they provide to users. While industry pilots such as automotive, intelligent automation, telemedicine, and entertainment applications offer new opportunities for operators, they present new challenges in terms of reliability, latency, and cost requirements. For example, augmented reality applications will change the entertainment industry as they improve the user experience through realism. Providing a realistic and user-friendly experience requires minimal round-trip time to act and react [4].

To meet these challenging needs, edge computing and network function virtualization (NFV) has become a solution for bringing cloud services to the proximity of the user. On the one hand, multiple access edge computing (MEC) and fog

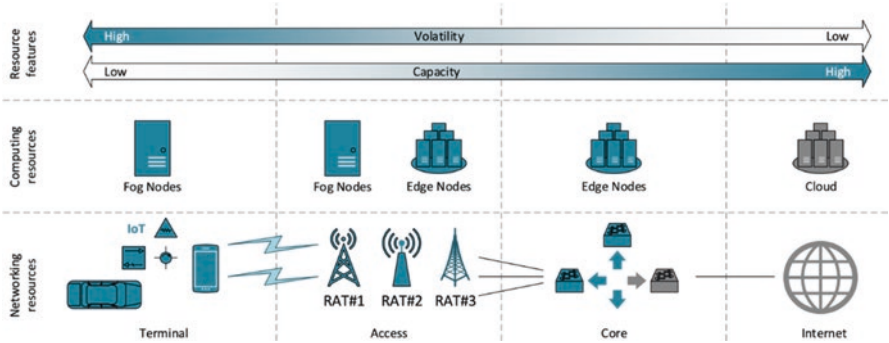


Fig. 1 Cloud, edge, and fog resources and characteristics [6]

virtualize network edge applications, reducing end-to-end latency. On the other hand, NFV separates network functions and applications from the underlying hardware and allows them to be implemented as software. Mobile services can now be deployed in a distributed manner independent of hardware, and software-defined networking (SDN) can provide a dynamic responsive network for new services. SDN decouples the control and data planes, and thus it benefits MEC and NFV by simplifying management, enabling programmability, and enhancing performance.

These technologies work together to provide operators with effective means to coordinate and scale their infrastructures. An innovative joint of these technologies is presented by 5G-CORAL [5] which exploits edge solutions to provide low-latency and enhanced QoS across multiple-RAT environment (see Fig. 1). It adopts ETSI NFV and MEC standards as well as considers mobile and volatile resources.

2.1 Edge and Fog Computing System

The EFS is a logical system comprised of fog and edge resources belonging to an administrative domain. An administrative domain is a collection of isolated resources managed by a single organization. The EFS virtualizes functions and applications and can interact with EFS in other domains. The software part of EFS consists of the following:

- *Function* is a virtualized instance deployed within the EFS for networking purposes.
- *Application* is a virtualized instance deployed within the EFS for serving end users and third parties.
- *Service platform* is a data storage for telemetric data collected from the EFS environment.
- *Entity manager* is responsible for applying configuration and management policies on the EFS elements as specified by the OCS. Compared to NFV and MEC

standards, the entity manager of the EFS service platform plays the role of the MEC platform manager. For more details, please refer to 5G-CORAL deliverable D2.1 [6].

5G-CORAL considers three types of the computing layers in the continuum between user devices and core network: fog, edge, and cloud. The most commonly known computing layer today is the cloud. Cloud is a remote high-powered data center which offers virtualized computing, storage, and networking services to businesses and end users. Lately, edge (i.e., MEC) and fog emerged aiming at moving the virtualized resource closer to IoT and end users to reduce the latency. While edge architecture mainly focuses on the deployment of virtualized resources at the edge of operators' infrastructure (e.g., base station), fog architecture extends the reach of resources even closer to the user (e.g., home gateway).

2.2 Enabling Virtualization Technologies for IoT in the Edge

Hypervisor-Based Virtualization it runs at the hardware level and provides independent and host-isolated virtual machines (VM). Each VM runs its own kernel and operating system (OS). Therefore, the hypervisor can create Windows guests on Linux host. However, isolation and host abstraction features come with a cost. Memory, disk, and CPU resources must be specified at runtime to execute VM kernel and OS. Also, hardware emulation is required for I/O operations. In the case of high-density virtualization, VM deployment becomes resource inefficient, especially for small edge and fog applications. One good example of hypervisor-based virtualization is kernel-based virtual machine (KVM).

System-Based Containerization it isolates processes at the OS level and runs on top of the host kernel. There are two types of containers, namely, system container and application container. System containers (also known as machine containers) behave like a standalone Linux system. That is, the system container has its own root access, file system, memory, processes, and networking and can be rebooted independently from the host. While system containers are lightweight due to the absence of guest kernel and hardware emulation, they can only run on Linux host and are bonded to the host's kernel. Linux container (LXC/LXD) is an example of system-based containers.

Application-Based Containerization it isolates an application from other applications running on top of shared kernel and shared OS. Because of sharing the same kernel and OS, application containers are lighter than system containers. The application container only encapsulates the necessary libraries, configurations, and dependencies needed to run the application. Therefore, its resource footprint is significantly lower than VM and system containers. This makes the instantiation of virtualized applications appropriate for IoT services [7]. A well-known example of an application container is Docker.

A. *State-of-the-Art Edge Network Solutions for IoT Applications*
B. *Access Migration*

In the standard IEEE 802.11, clients actively scan for available APs for association in a discovery phase. During the scanning process, the AP responding to the probe message becomes a candidate for the client. When the client selects an AP, the association occurs between the AP basic service set identifier (BSSID) and the client MAC address. During this process, the infrastructure cannot control client association decisions. In order to change the AP, the client initiates a handoff process, which takes approximately 2 seconds [8].

In order to minimize the reassociation time, many fast handoff schemes have been proposed in [9–13]. These techniques can be divided into a) scanning time minimization and b) authentication time minimization. In the process of minimizing the scanning time, the goal is to identify a target AP as soon as possible. For example, synchronization scan [9], intelligent channel scanning [10], neighboring graph [11], selective neighbor caching [12], AP prediction [13], and IEEE 802.11k are scanning time minimization techniques. In authentication time minimization, preauthentication [13] was presented and detailed in IEEE 802.11r. While the proposed technique can minimize the reassociation latency, they involve modification to client devices and require additional signaling. The fact that these techniques require changes to the client side challenges the idea of bring your own device, which states that the infrastructure must accommodate variety of user devices.

In order to move client-AP association decisions from the client to the infrastructure, a virtual access point (vAP) was introduced in [14]. A vAP is an abstraction of the network functions created to connect clients. Each client associates to a dedicated vAP with unique parameters. Based on [14], the client associates with the vAP and periodically receives beacons to know that it is still within the coverage of its AP. The received signal strength perceived by the client is encapsulated in the beacon so that neighboring APs can also learn clients signal strength. Each AP maintains two databases, namely, managed and monitored lists, which keep clients' signal strength. The managed database stores the signal levels of clients currently associated with the AP, while the monitored database stores the signal levels of clients that the AP can hear. Access migration occurs when a neighboring AP receives a beacon from the client with signal strength higher than the signal strength advertised by the serving AP. This way, the association decision is moved to the infrastructure. However, there are drawbacks. It is assumed that all APs operate on the same channel so they are able to hear the advertised signal level. This makes the solution impractical for large-scale deployment and frequency planning. In addition, since the management of the vAPs is in a distributed fashion, a global view is absent.

To advance the work presented in [14], a multichannel extension of vAP paradigm is proposed in [15]. In multichannel vAP deployment, the APs operate in different channels and communicate with each other to support client mobility. After a client connects to a vAP managed by physical AP, the AP monitors the client signal strength level. If the signal level reaches below a predefined threshold, the AP sends a scan request to the neighboring APs. As soon as a neighboring AP responds

to the request, the client is instructed to switch channels and continue communicating with the new AP. This solution defeats the interference problem caused by operating on the same channel, but still remains a distributed solution without a global view.

On the other hand, an SDN-based WiFi framework dubbed Odin is introduced in [16]. Odin incorporates SDN solutions into vAP paradigm. In other words, the programmability and global view features of SDN are used to manage clients' mobility. The Odin framework is used to migrate vAPs from an AP to another while generating game traffic on the client side in [17]. While [16, 17] enable flexible and scalable management, they still consider that all APs are running in the same channel. Lately, an approach incorporating the advantages of SDN while also operating in a multichannel is considered [18, 19].

Containerized Application Migration

Service migration can be divided into stateful and stateless. In a stateless migration, the state of the application is not preserved when the service is relocated to the target host. In the case of stateful migration, the state of the application is maintained when the execution of the application is continued on the target host. There are three types of stateful migration techniques, stop and copy [19], pre-copy [20], and post-copy [21]. Stop and copy freezes the application, checkpoints its state, copies the application and its state to the target, and then resumes the application. Pre-copy executes iterative state checkpoint while the application continues to run and then terminates with a shorter stop and copy. Finally, post-copy performs a short stop and copy to relocate the important execution state, then resumes the application at the target, and retrieves the rest of the data as required.

VM live migration is well investigated [22] and many effective solutions are commercially available. For instance, a pre-copy-based VM live migration scheme is presented in [21]. An active VM continues to run in the course of in-memory data iterative pre-copying. During a consecutive iteration, only changes in memory (dirty pages) are transferred. At last, a final state copy is performed while the VM instance is frozen and then transferred to the destination host. This way, the amount of downtime is greatly reduced when compared to a pure stop-and-copy scheme. Although the work in VM migration is mature, most of the existing solutions are tailored for data center environment where network-attached storage (NAS) and specific virtualization technology are utilized. NAS enables all the host machines in a data center to access a network-shared storage which removes the need for migrating disk storage. However, in a scenario where migration takes place between MECs, state and local disk storage has to also migrate over wide area network (WAN).

Lately, container migration has caught much attention from the research community [23, 24], especially since containerization offers many advantages, in terms of resource efficiency and performance, over traditional hypervisor-based

virtualization. This fact enables the instantiation of lightweight containerized applications suitable for IoT services [25]. In [23], container migration mechanism is developed for power efficiency optimization in heterogeneous data center. This work assumes that the source and destination hosts have access to a NAS and thus container data is not copied over WAN.

Furthermore, a framework for migrating containerized applications is presented in [24]. The proposed framework is the first to consider MEC environment for container migration. Fundamentally, the framework is a layered model which aims to reduce the downtime incurred by the migration process. While the presented results show reduction in downtime as a result of layering, the framework relies on stop-and-copy migration which is not an efficient method for containers with large in-memory state. In our proposed solution, we develop a pre-copy procedure to migrate containerized applications between edge clouds.

Mobility Support in Edge User Application

C. *ARNAB Double-Tier Migration*

ARNAB [26] is a novel architecture which provides transparent service continuity through access and application migrations. The term ARNAB is an Arabic word which means rabbit. ARNAB is given for the architecture since the user service exhibits the rabbit behavior hopping through the WiFi infrastructure to support user mobility. Furthermore, ARNAB is said to be transparent since there is no modification to the user device required for its operation. The main objective of proposed architecture is to deliver seamless user experience. ARNAB utilizes double-tier migration, namely, user connectivity migration and application migration. The first migration scheme uses vAP to eliminate WiFi handoff delay and relocate the association decision-making to the infrastructure. The second tier uses iterative copying scheme to minimize the downtime during application migration.

D. *Follow Me Cloud*

Follow me cloud (FMC) [27] is a novel architecture that enables cloud services (i.e., running in distributed data centers) to follow the users as they roam through the network. The FMC controller manages computing and storage resources of the data centers and decides which data center the user should be associated with. Based on FMC, a migration mechanism is developed to ensure service low latency [28]. However, the minimum reported migration downtime remains high for seamless service experience.

E. *Follow Me Fog and sFog*

Follow me fog (FMF) and seamless fog (sFog) are proposed to pre-migrate computation jobs before radio handover occurs during user mobility. This is

accomplished by constantly monitoring the received signal strength indicator (RSSI) from different fog nodes. Once the RSSI of the current node (i.e., serving the user) keeps decreasing and the RSSI of another node keeps increasing, the computing jobs are pre-migrated to the new node before the reassociation takes place. This way, FMF and sFog support user mobility by predicting the target fog node beforehand and thus reducing the waiting time for computing jobs to be available.

F. *SharedMEC*

SharedMEC [29] is an architecture which combines the standard cellular handover process with service handover. In SharedMEC, an edge platform is shared by multiple femto base stations to support user mobility. The architecture employs an algorithm to decide when to migrate user services. In addition, an analytical model is proposed to analyze the total cost of migrating user service.

3 Big Data Enabling Technologies

Velocity (real-time collection), volumes (large amount), and variety (different kinds) are the three data characteristics that are usually associated with the definition of big data. Traditional SQL-based database management systems fail to store and manipulate such data. Therefore, NoSQL (not relational) databases came into the picture as a solution. In this section, we present some technologies that deal with the storage and the analysis of big data.

3.1 Storage

MongoDB

MongoDB is a general-purpose, document-based, distributed database that is suitable for IoT application [30]. It provides an Intelligent Data Platform that supports IoT Apps from Edge to the core or the cloud. Figure 2 [31] shows the architecture of MongoDB. It also provides real-time and event processing.

CassandraDB

Apache Cassandra is an open-source NoSQL wide-column database. It adopts a data replication mechanism on a cluster of machines. Therefore, if one or more machines fail, based on the configuration of the replication factor, it still can provide the data with no data loss. Moreover, Cassandra allows adding/removing machines to existing clusters which permits scale up or scale down capability [32].

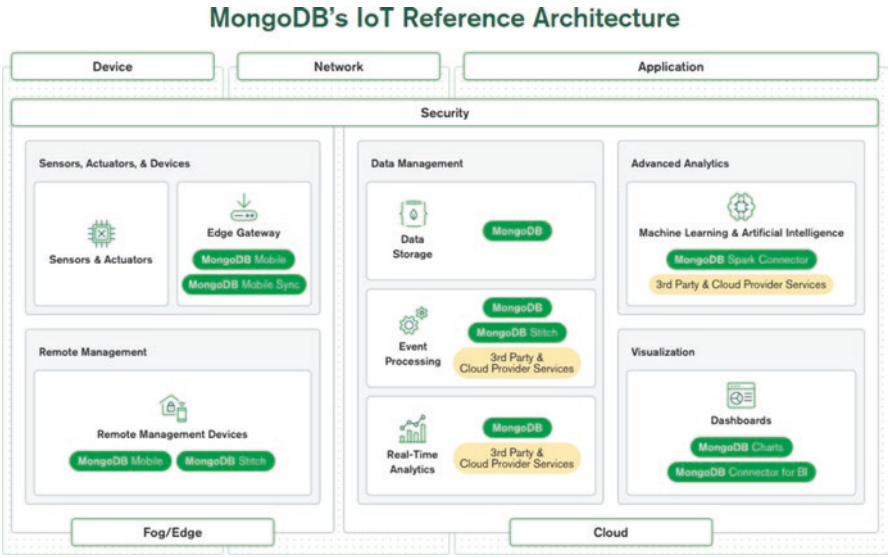


Fig. 2 Fog/edge placement in IoT architecture

HBase

Apache HBase is an open-source and distributed database that is created after Google's Bigtable. It presents Bigtable-like capabilities on top of Apache Hadoop and HDFS. Also, it provides a real-time read/write access and designed to host very large tables – billions of rows X millions of columns [33].

OpenTSDB

It's very common in IoT solutions that several sensors generate data that monitor physical/cyber metrics over time (time series). One suitable way to store such data is the time series database OpenTSDB. Time Series Daemen (TSD) provides APIs which allows client applications to write and read data. TSD stores the time series data on HBase [34].

3.2 Analytics

Hadoop MapReduce

One of the most widely used analytic frameworks is Hadoop MapReduce. It is designed to execute batch processing analytics tasks on a large amount of data in a parallel manner. A typical Hadoop cluster could have thousands of machines that are running both the storage node (HDFS) and the analytical node (MapReduce) [35].

Spark

Unlike Hadoop, Apache Spark is designed to support real-time and stream processing. Also, it stores the data on Hadoop; therefore Spark has the ability to run batch processing as well. Spark provides rich features with different APIs that make it very suitable for running machine learning applications. For example, Spark supports applications written in Java, Python, and Scala [36].

3.3 IoT Protocols

In this part, we demonstrate some of the used protocols, interfaces, and APIs in the realm of IoT, cloud, and big data analytics. Since the protocol stack from sensors to business in IoT is very wide, we selected the commonly used ones and applicable in the context of smart cities and urban development.

REST

One of the most commonly used web services is the representational state transfer (REST). As Wikipedia's definition, it is a software architectural technique that defines a set of constraints to be used for creating web services. Web services that are compliant to the REST architectural style provide interoperability between software component systems on the Internet using the http protocol. The exchanged messages could be in JSON or XML format [37].

AMQP

With heterogeneous platforms and systems in the IoT ecosystem. Connecting different systems with each other will become a challenge during the integration phase. Middleware technologies such as the Advanced Message Queuing Protocol (AMQP) could provide a standard way of getting the system connected. AMQP is an open standard for exchanging messages between different applications. Also, in a loosely coupled fashion, it connects systems, feeds business processes with the required information, and provides reliable transmission of the messages [38].

MQTT

In IoT architecture, one of the commonly used solutions to connect limited resources devices (sensors) to other elements, such as the gateway or the network server, is the MQ Telemetry Transport (MQTT). It plays the role of communication infrastructure where one device would publish the data to MQTT and another receiver would

subscribe to get it. MQTT is fitting for machine-to-machine (M2M) communication. Several products implement MQTT, for example, RabbitMQ, Mosquitos, and Erlang MQTT [39].

D2D

When we are considering edge computing in the fog devices, device-to-device (D2D) communication could play an important role as devices might hand off some tasks to a more capable device, to an idle device, or to a less loaded one. From another point of view, EC also could help in the utilization of the devices. Therefore, we present the D2D which is defined as direct communication between two mobile devices with no need for going through the base station (BS) or the core network [40].

The aforementioned technologies for both analyzing and storing big data are available as Docker containers. For example, Docker Hub [41] has images for MongoDB, Cassandra, HBase, OpenTSDB, and Spark. Also, a Docker image is available for [35]. Therefore, edge computing is achievable with the existence of these technologies.

3.4 Edge-Based and Cloud-Based Use Cases

GeeLytics

Large-scale implementation of IoT solutions in different areas will lead to the need for real-time processing of stream data. Sensors like surveillance cameras, smartphones' cameras, and audio recording will generate a massive amount of streaming data. The proposed system in GeeLytics [42] attempts to provide a solution by exploiting the edge computing for processing the stream data. GeeLytics uses the cloud for offloading. Moreover, it takes into consideration the geographic location of the data stream sources and dynamically steers the processing of the tasks to the edge. These tasks could be depicted as isolated Docker containers. In summary, GeeLytics [42] could be used in different use cases, such as smart traffic, crowd prediction, and globalized smart city, which promises to provide the application with real-time processing of stream data.

Vehicular Fog Computing

Traffic management systems (TMS) play an important role in smart cities and urban development. However, it demands an ultralow latency for managing and monitoring the traffic. Edge computing can enable TMS to provide services that meet the aforementioned demands. The authors in [43] have proposed the vehicular

fog computing (VFC), which is a combination of exploiting fog computing (cloudlet layer) and vehicular networks. Cloudlet represents the grouping of some elements in the layer between the cloud and the vehicles. For example, routers, access points, and base stations are cloudlet layer's components. An important design principle of VFC is using both parked and moving vehicles as computing resources for data processing. Cloud computing is not totally abandoned, but it's being used for offloading. In order to minimize the response time, the authors in [43] proposed a VFC-enabled offloading algorithm for load-balancing optimization between the cloudlet fog layer and the vehicular network. The use case for the system was the real-world city map and routes of taxis in Shanghai, China. Compared to a random approach algorithm for offloading, the results show that the response time of the proposed solution was 0.6 second while the randomized approach was 4.2 seconds. In conclusion, with the use of edge computing and a novel load balancer algorithm, the system in [43] GeeLytics can provide a minimum response time for TMS.

Recommender System

IoT and big data analytics enable the development of smart and connected communities (SCC), where systems can make decisions such as reduce traffic congestion, fight crime, foster economic development, and manage the effects of a changing climate. The proposed architecture in [44] is composed of four layers. First is the sensing layer where data is being generated. Data sources are not only traditional sensors and open data but also personal smartphones' sensors as means of mobile crowdsensing (MCS). Second is the interconnecting layer which represents the communication infrastructure among all the layers. Third is the data layer which serves as the big data layer where data storage and analysis takes place. Finally, the fourth one is the service layer which has the APIs and the applications offered to the end users. In Trentino, Italy, the context-aware recommender system TreSight was implemented.

The user (tourist) will wear a bracelet IoT device and install the recommendation system on his/her smartphone. Points of interest locations in the city will have a HotSpot device that interacts with the bracelet, senses physical quantities from the environment, and provides the data to the cloud. From the connected bracelets to the HotSpot, the system can calculate the number of tourists in a particular location. The HotSpot sensors feed information about the temperature, humidity, and other physical quantities to the system. From OPenData Trentino, the system can gather weather information.

The system stores the data in MongoDB and uses Wi-Fare Cosmos for Big Data Analysis integrate with Hadoop. Based on the input data, the system makes decisions. Therefore, it can send certain knowledge to tourist-related service providers (restaurants, hotels, etc.) and recommend the user of his/her next place to visit [44].

Digital Smart City

The community expects smart cities to facilitate the citizens, enhance people's everyday activities, and help the authorities for better planning of the city and the provided services. To achieve that there is a need for a general system, which plays the role of an integration medium to link all existing IoT smart city systems. Things from smart homes, smart parking, vehicular networking, weather stations, and surveillance systems generate a massive amount of heterogeneous data. The goal is to connect all these systems; therefore, the proposed system in [36] suggests a central data hub for data collection from all sources. Then, it will send it to the cloud for processing.

On the cloud, Spark provides real-time processing, Hadoop for batch data processing, and Giraph over Hadoop for big city graph processing. The system will provide a set of APIs which allow the applications to consume the processed version of the data for further application-specific knowledge extraction.

4 Machine Learning for Smart Urban Development

The explosion in data gathering ability of cities itself is not useful, unless effective analytics are employed to extract meaningful information. Intelligent machine learning (ML) algorithms are applied on the collected data for intelligent insights. This is where the big data analytics techniques, introduced in previous section, come into play. The focus of this section is on new and efficient machine learning algorithms that have been designed to exploit the big data analytics to further enhance urban development.

When it comes to Internet of Things, we collectively refer to different sensors, actuators, and other smart objects that are essentially the "things" [2] used for data collection in smart cities. The data generated in smart cities come with a host of challenges, in terms of volume, velocity, and variety. The ML algorithms in the context of smart cities need to accommodate all the abovementioned factors to process the generated data and extract information to make intelligent decisions. The following section – a primer on machine learning – will lay a groundwork for ML algorithms in the context of smart decision-making for urban development.

4.1 A Primer on Machine Learning

This section will serve as brief introduction to machine learning and various approaches in the context of smart urban development. Relevant examples are also included in this section. This is to show how the confluence of big data and machine learning advances propel smart urban development.

A pioneer in the area of machine learning is Arthur Samuel who has formulated the definition of machine learning as: "Field of study that gives computers the ability to learn without being explicitly programmed" [45]. A more workable definition was given by an expert, Tom Mitchell, whom defines a well-posed learning problem as: "A computer program is said to learn from experience E with respect to some task T and some performance measure P, if its performance on T, as measured by P, improves with experience E" [46]. To illustrate this definition in the context of smart urban development, we base our discussion on smart home systems, such as Google Home, Amazon's Alexa, and Apple Home, which cater to user's requests primarily through voice commands. In accordance to the definition, the following are defined:

- *Task T* – The task expected to be performed by the end user, like carrying out the desired voice command.
- *Performance measure P* – The accuracy of the voice command.
- *Experience E* – The actual execution of the voice command, both when it's interpreted correctly or otherwise. This includes vast amounts of historical data, which may also include human feedback.

In general, machine learning algorithms can be broadly classified into: supervised learning, unsupervised learning, and reinforcement learning. There are other types of algorithms like recommender systems, etc., but the aforementioned are the most relevant to the current context.

Supervised Learning

Algorithms of this category typically solve problems with the following characteristics:

- A dataset to train the system.
- There's a notion of expected output.
- Usually the problems solved using this algorithm have some sort of relationship between input and output.

These are typically the defining features of a supervised learning problem. And supervised learning problem can be further classified into two categories:

1. *Regression Problem*: The basic framework of supervised learning remains the same, the characteristics of regression problem is the output is a continuous data stream, i.e. input variables are mapped to a continuous function.
   Example: Given the sizes of different houses and the respective prices in the current real estate market, predicting the price of a house based on size is a regression problem since price is a continuous function of size here.
2. *Classification Problem*: The difference here is the output in supervised learning is a discrete quantity and depends on the input.

Example: Reformulating the previous example in regression problem, if the objective is to check if the selling price of house is above or below a certain value, then in this case there are just two possible outputs; this is a classification problem [47].

Unsupervised Learning

Algorithms in this category typically solve the problems with the following features:

- There is a dataset to train the system.
- The defining feature is the output; there is very little to no information of what the expected output would be.
- Usually the result of applying this algorithm is, a structure is derived in seemingly unrelated data.

The algorithms in this category can be classified as:

1. *Clustering Problem*: The objective here is to group the raw data based upon the similarities.
   Example: A supermarket chain grouping its customers based on the brands they prefer, to estimate the future demand of a brand.
2. *Non-clustering Problem*: The objective in this case is to filter data from what could be considered as irrelevant noise.
   Example: A voice recognition intelligent home system trying to separate voice commands in a noise-filled environment (more formally known as "the cocktail problem" in literature) [48].

Reinforcement Learning

Reinforced learning algorithms are defined by the following features:

- The software agents involved take actions with the sole purpose to maximize some notion of cumulative reward, which depends on the context of the problem solved.
- Unlike supervised learning it is not necessary to label the inputs and outputs, and there is no need to rectify suboptimal actions.
- The algorithms in RL tend to find a balance between exploring the unknown and exploiting the known [49, 50].

Many of the smart city applications involve RL, since there is absence of output in many cases and choosing the correct action is cumulatively rewarded, so that the desired outcome can be extracted. However, there is a drawback when it comes to smart city context. This is due to the enormous volumes of data; it's practically

impossible for humans to provide a reward feedback. A work around for this problem is to apply semi-supervised learning where data is partially labelled [3].

Most of the ML algorithms in the literature fall into one of the aforementioned categories. However, the future trend seems to shift toward deep learning (DL) and deep neural network (DNN). Briefly speaking deep learning is a subset of machine learning where multiple layers of ML algorithms are applied, such that the output of one stage is fed to the input of the next. This is implemented using specialized algorithms known as neural networks, aptly named, since they resemble the network of neurons in the human body [51].

4.2 Characteristics and Challenges for ML Algorithms in Smart City Ecosystem

Smart cities as mentioned in the previous section must face three Vs – variety, volume, and velocity – to handle data and to effectively use it in ML algorithms. Another challenge comes when choosing the layer to run the ML algorithm, i.e., edge, fog, or cloud. This depends on the type of smart city application. As an example, let's take the case of autonomous vehicles – here the application demands stringent latency requirements for safety purposes. Hence, the processing is usually done in the vehicle itself, i.e., the edge node, instead of sending it to the cloud. It's imperative that all these factors are taken into consideration when implementing ML algorithms.

M. Mohammadi et al. in [3] also observe the following challenges for ML in smart city context:

- Implementing constant human feedback to enable learning would be difficult due to enormous volume of data involved.
- The rate of data generation, i.e., the velocity, also further makes it difficult for human review; hence learning should be automated.
- Since applications in smart cities tend to evolve overtime, a continuous and dynamic learning mechanism becomes a need.
- Because of the huge scale and volume, uncertainty and noise exist in thus generated data. Challenges are summarized in Fig. 3.

4.3 ML Smart Urban Development: A Few Use Cases from Literature

Accurate object detection is needed for traffic control and autopilot in self-driving cars. NVIDIA has developed a state-of-the-art tool called NVIDIA Deep Learning GPU Training System (DIGITS) [52]. The link to the complete article can be found

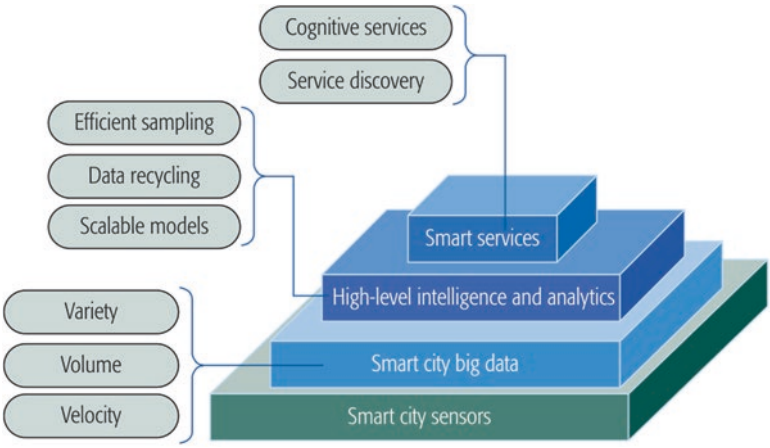


Fig. 3 Challenges in smart cities for ML implementation [3]

in the bibliography. YOLO (current version YOLOv3) [53] is another object detection algorithm commonly used for object detection. Nagaraj et al. [54] implemented a traffic object detection using the abovementioned tools on the edge node. Edge node was chosen to keep the latency low, a common requirement for such applications. Their system could distinguish and detect objects from 14 different categories. In another case, Pacheco et al. [55] have implemented object detection in all the three different nodes, i.e., edge, fog, and cloud, for their smart classroom, thus demonstrating the versatility of these algorithms.

Nikouei et al. further have implemented surveillance as a service on the edge [56]. They have used lightweight detection tracking algorithms. The focus of their work is human object detection, further demonstrating that edge node can be used for effective implementation of ML algorithms.

In the field of crime and security for cities, Lourenco et al. [57] developed a framework called CRiMINaL (Crime patteRn MachINe Learning). The system uses historical data of various crimes like theft to assist the authorities in crime prevention. A relational machine learning approach was used in this framework. This system has been implemented by the authors.

Traffic flow prediction is another area of concern for any city. This can also be tackled by ML algorithms. Mohammed and Kianfar [58] designed and implemented ML algorithms to predict the traffic flow in Interstate 64, Missouri, USA. With such systems, proactive traffic management can be implemented for smart cities.

There are many use cases where ML techniques are increasingly being used to undertake smart urban development. In Fig. 4, the gist of data flow and levels in ML algorithms for smart city applications are summarized.

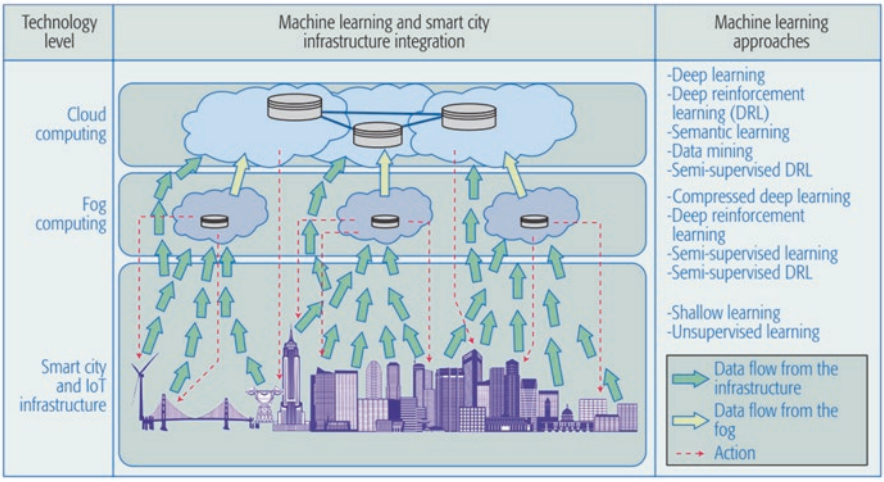


Fig. 4 Machine learning approaches for smart city applications [3]

5 Conclusion

This chapter discusses the role of emerging technologies in smart urban development, specifically how edge computing empowers big data and machine learning with computational power to enable disruptive IoT applications. Also, it presents the current trending technologies in the storage and the analytics of big data. For example, NoSQL databases enable the storage of massive amounts of data. Moreover, analytics frameworks provide the necessary data analysis, processing, and visualization. Machine learning algorithms allow knowledge extraction, classification, clustering, as well as other functions to make sense of the data, thereby enabling a more intelligent decision-making system. On the other hand, from the use cases presented in this chapter, we infer that edge computing holds great potential in improving the way computational tasks are currently being processed. In applications such as waste management systems, smart traffic, and recommender systems, the use of edge computing can dramatically reduce the latency. Such improvements will expedite the development process toward smart cities.

References

1. 2018 Revision of World Urbanization Prospects | Multimedia Library – United Nations Department of Economic and Social Affairs [Online]. Available: https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html. Accessed 8 Sept 2019
2. SAS Institute: A Non-Geek's A-to-Z Guide Internet of Things. https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper1/non-geek-a-to-z-guide-to-internet-of-things-108846.pdf
3. Mohammadi, M., Al-Fuqaha, A.: Enabling cognitive smart cities using big data and machine learning: approaches and challenges. IEEE Commun. Mag. **56**(2), 94–101 (2018)

4. Lema, M.A., et al.: Business case and technology analysis for {5G} low latency applications. IEEE Access. **5**, 5917–5935 (2017)
5. {5G-CORAL H2020} project. http://5g-coral.eu/
6. 5G-CORAL D2.1: Initial design of {5G-CORAL} edge and fog computing system. https://cordis.europa.eu/project/id/761586
7. Schulz-Zander, J., et al.: Evaluating performance of containerized {IoT} services for clustered devices at the network edge. IFIP Int. Conf. Pers. Wirel. Commun. **25**(3), 194–203 (2017)
8. Mishra, A., Shin, M., Arbaugh, W.: An empirical analysis of the {IEEE} 802.11 {MAC} layer handoff process. ACM SIGCOMM Comput. Commun. Rev. **33**(2), 93–102 (2003)
9. Ramani, I., Savage, S.: {SyncScan}: practical fast handoff for 802.11 infrastructure networks. In: 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 1, pp. 675–684 (2005)
10. Kwon, K., Lee, C.: A fast handoff algorithm using intelligent channel scan for {IEEE 802.11 WLANs}. In: 6th IEEE International Conference on advanced Communication Technology, vol. 1, pp. 46–50 (2004)
11. Park, S.-H., Kim, H.-S., Park, C.-S., Kim, J.-W., Ko, S.-J.: Selective channel scanning for fast handoff in wireless {LAN} using neighbor graph. In: IFIP International Conference on Personal Wireless Communications, pp. 194–203 (2004)
12. Pack, S., Jung, H., Kwon, T., Choi, Y.: SNC: a selective neighbor caching scheme for fast handoff in {IEEE} 802.11 wireless networks. ACM SIGMOBILE Mob. Comput. Commun. Rev. **9**(4), 39–49 (2005)
13. Tseng, C.-C., Chi, K.-H., Hsieh, M.-D., Chang, H.-H.: Location-based fast handoff for 802.11 networks. IEEE Commun. Lett. **9**(4), 304–306 (2005)
14. Grunenberger, Y., Rousseau, F.: Virtual access points for transparent mobility in wireless {LANs}. In: IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6 (2010)
15. Berezin, M.E., Rousseau, F., Duda, A.: Multichannel virtual access points for seamless handoffs in {IEEE} 802.11 wireless networks. In: IEEE 73rd Vehicular Technology Conference (VTC Spring), pp. 1–5 (2011)
16. Schulz-Zander, J., Suresh, P.L., Sarrar, N., Feldmann, A., Hühn, T., Merz, R.: Programmatic orchestration of WiFi networks. In: USENIX Annual Technical Conference, pp. 347–358 (2014)
17. Saldana, J., de la Cruz, J.L., Sequeira, L., Fernández-Navajas, J., Ruiz-Mas, J.: Can a {Wi-Fi WLAN} support a first person shooter? In: Proceedings of the 2015 International Workshop on Network and Systems Support for Games, p. 15 (2015)
18. Sequeira, L., de la Cruz, J.L., Ruiz-Mas, J., Saldana, J., Fernandez-Navajas, J., Almodovar, J.: Building an {SDN} enterprise {WLAN} based on virtual {APs}. IEEE Commun. Lett. **21**(2), 374–377 (2017)
19. Sapuntzakis, C.P., Chandra, R., Pfaff, B., Chow, J., Lam, M.S., Rosenblum, M.: Optimizing the migration of virtual computers. ACM SIGOPS Oper. Syst. Rev. **36**(SI), 377–390 (2002)
20. Clark, C., et al.: Live migration of virtual machines. In: Proceedings of the 2nd Conference on Symposium on Networked Systems Design & Implementation, vol. 2, pp. 273–286 (2005)
21. Hines, M.R., Deshpande, U., Gopalan, K.: Post-copy live migration of virtual machines. ACM SIGOPS Oper. Syst. Rev. **43**(3), 14–26 (2009)
22. Medina, V., Garcia, J.M.: A survey of migration mechanisms of virtual machines. ACM Comput. Surv. **46**(3), 30 (2014)
23. Nider, J., Rapoport, M.: Cross-{ISA} container migration. In: Proceedings of the 9th ACM International on Systems and Storage Conference, p. 24 (2016)
24. Machen, A., Wang, S., Leung, K.K., Ko, B.J., Salonidis, T.: Live service migration in mobile edge clouds. IEEE Wirel. Commun. **25**(1), 140–147 (2018)
25. Morabito, R., Farris, I., Iera, A., Taleb, T.: Evaluating performance of containerized {IoT} services for clustered devices at the network edge. IEEE Internet Things J. **4**(4), 1019–1030 (2017)
26. Abdullaziz, O.I., Wang, L.-C., Chundrigar, S.B., Huang, K.-L.: {ARNAB}: transparent service continuity across orchestrated edge networks. In: 2018 IEEE Globecom Workshops (GC Wkshps), pp. 1–6 (2018)

27. Taleb, T., Ksentini, A., Frangoudis, P.: Follow-me cloud: when cloud services follow mobile users. IEEE Trans. Cloud Comput. **7**(2), 369–382 (2019)
28. AkremAddad, R., Dutra, D.L., Bagaa, M., Taleb, T., Flinck, H.: Towards a fast service migration in {5G}. In: IEEE Conference on Standards for Communications and Networking (CSCN), pp. 1–6 (2018)
29. Nasrin, W., Xie, J.: {SharedMEC}: sharing clouds to support user mobility in mobile edge computing. In: IEEE International Conference on Communications (ICC), pp. 1–6 (2018)
30. mangodb [Online]. Available: https://www.mongodb.com/. Accessed 1 Sept 2019
31. Internet of Things | MongoDB [Online]. Available: https://www.mongodb.com/use-cases/internet-of-things. Accessed 1 Sept 2019
32. Apache Cassandra [Online]. Available: http://cassandra.apache.org/. Accessed 1 Sept 2019
33. Apache HBase – Apache HBase™ Home [Online]. Available: https://hbase.apache.org/. Accessed 1 Sept 2019
34. OpenTSDB – A Distributed, Scalable Monitoring System [Online]. Available: http://opentsdb.net/overview.html. Accessed 1 Sept 2019
35. GitHub – sequenceiq/hadoop-docker: Hadoop docker image [Online]. Available: https://github.com/sequenceiq/hadoop-docker. Accessed 1 Sept 2019
36. Rathore, M.M., Paul, A., Hong, W.H., Seo, H.C., Awan, I., Saeed, S.: Exploiting IoT and big data analytics: Defining Smart Digital City using real-time urban data. Sustain. Cities Soc. **40**, 600–610 (2018)
37. REST API [Online]. Available: https://en.wikipedia.org/wiki/Representational_state_transfer
38. Ebert, J., Kazimierczuk, M., Kazimierczuk, M.: Class E high efficiency tuned power oscillator. IEEE J. Solid State Circuits. **16**(2), 62–66 (1981)
39. MQTT [Online]. Available: http://mqtt.org/. Accessed 1 Sept 2019
40. Asadi, A., Wang, Q., Mancuso, V.: A survey on device-to-device communication in cellular networks. IEEE Commun. Surv. Tutorials. **16**(4), 1801–1819 (2014)
41. Docker Hub [Online]. Available: https://hub.docker.com/. Accessed 1 Sept 2019
42. Cheng, B., Papageorgiou, A., Cirillo, F., Kovacs, E.: GeeLytics: Geo-distributed edge analytics for large scale IoT systems based on dynamic topology. In: 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 565–570 (2015)
43. Ning, Z., Huang, J., Wang, X.: Vehicular fog computing: enabling real-time traffic management for smart cities. IEEE Wirel. Commun. **26**(1), 87–93 (2019)
44. Sun, Y., Song, H., Jara, A.J., Bie, R.: Internet of things and big data analytics for smart and connected communities. IEEE Access. **4**, 766–773 (2016)
45. Samuel, A.L.: Some studies in machine learning using the game of checkers. II-Recent progress. Annu. Rev. Autom. Program. **6**(PART 1), 1–36 (1969)
46. Mitchell, T.M.: Machine learning. McGraw-Hill international edit, McGraw Hill Higher Education. McGraw-Hill, New York (1997)
47. Ng, A.: Lecture note on SL (regression, optimi) STANFORD, pp. 1–30 (2000)
48. Ng, A.: Machine Learning & Machine Learning Extended (Apr 2013). http://cnx.org/content/col11500/1.4/
49. Kaelbling, L., Littman, M., Moore, A.: Reinforcement learning? A survey. J. Artif. Intell. Res. **4**(1), 237–285 (1996)
50. Kazimierczuk, M.K., Bui, X.T.: Class-E amplifier with an inductive impedance inverter. IEEE Trans. Ind. Electron. **37**(2), 160–166 (1990)
51. Dormehl, L.: What is an artificial neural network? Here's everything you need to know | Digital Trends (2018) [Online]. Available: https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/
52. Tao, A., Barker, J., Sarathy, S.: DetectNet: Deep Neural Network for Object Detection in DIGITS (2016). https://devblogs.nvidia.com/detectnet-deep-neural-network-object-detection-digits/
53. Redmon, J., Farhadi, A.: YOLOv3: An Incremental Improvement (2018). https://pjreddie.com/media/files/papers/YOLOv3.pdf
54. Nagaraj, S., Muthiyan, B., Ravi, S., Menezes, V., Kapoor, K., Jeon, H.: Edge-based street object detection. In: 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced &

Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, pp. 1–4 (2017)
55. Pacheco, A., Cano, P., Flores, E., Trujillo, E., Marquez, P.: A smart classroom based on deep learning and osmotic IoT computing. In: 2018 Congreso Internacional de Innovación y Tendencias en Ingeniería. CONIITI 2018, pp. 1–5 (2018)
56. Nikouei, S.Y., Chen, Y., Song, S., Choi, B.Y., Faughnan, T.R.: Toward Intelligent Surveillance as an Edge Network Service (iSENSE) using lightweight detection and tracking algorithms. IEEE Trans. Serv. Comput. **PP**(c), 1 (2019)
57. Lourenco, V., Mann, P., Guimaraes, A., Paes, A., De Oliveira, D.: Towards safer (smart) cities: discovering urban crime patterns using logic-based relational machine learning. Proc. Int. Jt. Conf. Neural Netw. **2018**, 1–8 (2018)
58. Mohammed, O., Kianfar, J.: Flow prediction: a case study of interstate 64 in Missouri. In: 2018 IEEE International Smart Cities Conference, pp. 1–7 (2018)

Mahmoud Abu Zaid received his B.S. in Computer Science from Assiut University, Egypt, in 2011 and his master's degree from Electrical and Computer Engineering, National Chiao Tung University, Taiwan. His current research interests include software-defined networks (SDN), Internet of Things (IoT), and big data. He's also currently a research and development engineer at AnaSystem Inc., Taiwan.

Mohamed Faizal received his B.E. in Electronics and Communication Engineering from Anna University (Sri Krishna College of Technology), in 2011. He also has worked as a Junior Research Fellow (JRF) in Indian Institute of Technology from January 2014 to April 2016. He earned his M.S. in Electronics Engineering from National Chiao Tung University, Taiwan. His Research interests include semiconductor devices, radio-frequency circuits, EDA, and machine learning. He is currently a RF Engineer at Wealth Tech System Co., Ltd.

R. Maheswar has completed his B.E. (ECE) from Madras University in the year 1999, M.E. (Applied Electronics) from Bharathiar University in the year 2002 and Ph.D. in the field of Wireless Sensor Network from Anna University in the year 2012. He has about 17 years of teaching experience at various levels and presently working as an Associate Professor in the School of EEE, VIT Bhopal University, Bhopal. He has published 40 papers at International Journals and International Conferences. His research interest includes wireless sensor network, IoT, queueing theory, and performance evaluation.

Osamah Ibrahiem Abdullaziz received the B.S. and M.Eng.Sc. degrees from Multimedia University, Malaysia, in 2011 and 2015, respectively. He is currently a Ph.D. candidate at the department of Electrical and Computer Engineering, National Chiao Tung University, Taiwan. His current research interests include software-defined networks, multi-access edge computing, network security, and network information hiding. He's also currently a researcher at Industrial Technology Research Institute (ITRI) of Taiwan. He's an excellent researcher with several publications in reputed journals under his belt.

The Perspective of Smart Dust Mesh Based on IoEE for Safety and Security in the Smart Cities

Raluca Maria Aileni, George Suciu, Martin Serrano, R. Maheswar, Carlos Alberto Valderrama Sakuyama, and Sever Pasca

1 Introduction

This chapter describes smart dust structures and its application in today's intensive Internet of Everything, Everywhere (IoEE) environment. It also presents the functionality of the smart dust microdevices in a meshed network and its application in a smart city environment, targeting security aspects.

The study based on microdevices started in 1961 when the first silicon pressure sensor was introduced. Micro-electromechanical systems (MEMS) represent a technology in which tiny integrated devices or systems are built.

MEMS are defined as an integrated microscale system that performs the following functions:

R. M. Aileni (✉) · S. Pasca
Politehnica University of Bucharest, Faculty of Electronics, Telecommunication and Information Technology, Bucharest, Romania

G. Suciu
Politehnica University of Bucharest, Faculty of Electronics, Telecommunication and Information Technology, Bucharest, Romania

Beia Consult International, Bucharest, Romania

M. Serrano
National University of Ireland Galway, Insight Center for Data , Galway, Ireland

R. Maheswar
School of Electrical & Electronics Engineering (SEEE), VIT Bhopal University, Bhopal, Madhya Pradesh, India

C. A. Valderrama Sakuyama
University of Mons, Faculty of Engineering, Department of Electronics and Microelectronics, Mons, Belgium

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_9

1. Conversion of physical stimuli, events, and parameters to electrical, mechanical, and optical signals and vice versa
2. Control, diagnostics, signal processing, and data acquisition features, along with microscale features of electromechanical, electronic, optical, and biological components (structures, devices, and subsystems) [1]
3. Actuation, sensing, transducer roles

MEMS handle motion, electromagnetic, radiating energy, and optical microdevices/microstructures—driving/sensing circuitry—controlling/processing integrated circuits.

In 2000, MEMS optical-networking components were fabricated, becoming a significant invention [2]. Smart dust is intended to create a millimeter-scale sensing and communication platform for a massively distributed sensor network. It is expected to be a micro-sized device with sensors, computation, bidirectional wireless communications, and a power supply. These devices must be based on inexpensive technologies for becoming widespread globally [3].

Internet of Everything Everywhere aims to connect various devices over larger areas; thus, it can be applied for building smart cities. Having that in mind, smart dust systems meet this requirement, that is, they are easy to fabricate and maintain, for example, mesh networks comprised of sensor nodes or motes are considered appropriate for the IoEE environment. In a smart city, smart dust networks can be used for monitoring parameters such as air quality, magnetic and electrical fields, water pollution, seismic activities, closed-circuit television (CCTV), traffic control, etc.

The following paragraph presents an example of a mesh network suited for applications in smart city monitoring.

The topological structure of wireless networks is shown in Fig. 1 [3]. The mesh topology is used in the development of this network. In the mesh topology, each mote is independent.

This network is formed of a mesh topology of MEMS motes that communicate through a gateway to the Internet, sending Ambiental data, for example. Furthermore, the data are collected in the form of processed data to a database. This database can send queries to the gateway and the mesh network. The terminal user can access this

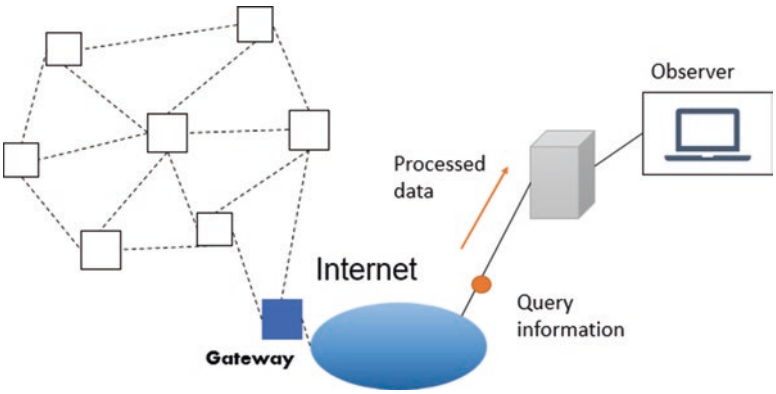


Fig. 1 The topology of mesh wireless sensor networks [3]

database to see environmental values. In this topology, the structure of the mote contains a processor, battery, interfaces to other sensors, and a radio transmitter [3].

Figure 2 shows a wireless sensor network (WSN) system diagram for real-time monitoring with a ZigBee connection. It consists of several motes for sensing temperature, humidity, dust particles concentration in the air, and acoustic level [4].

Each mote has a Global Positioning System (GPS) sensor for precise localization. The gateway module is a device with a ZigBee radio interface and a USB port that enables wireless medium transmissions to be sent over to the wired medium and to the server. The client can access information sent by the motes and their location on a map using Google Maps API, through the web application [4].

These smart city microdevices are used in the topology presented in Fig. 3.

- *Dust particles sensor (GPY21010AU0F)*: It is an optical sensor whose principle of operation is based on the detection of the infrared light emitted by an infrared

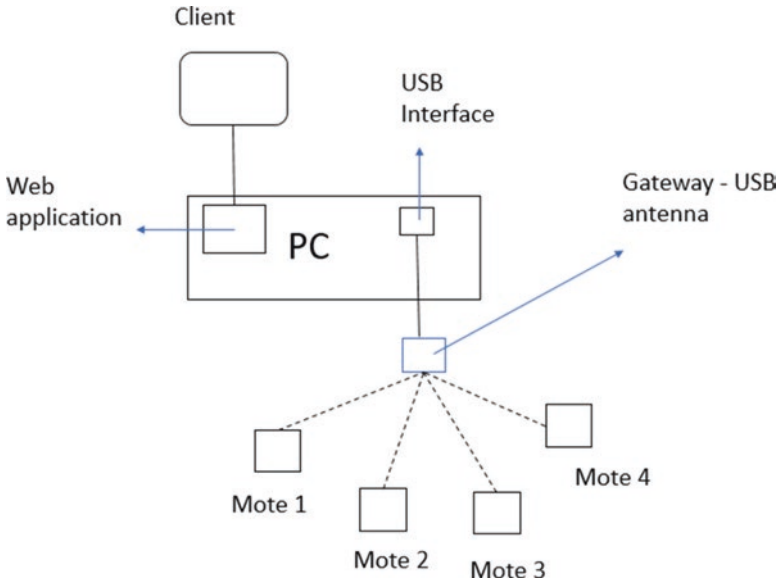


Fig. 2 A real-time monitoring system [4]

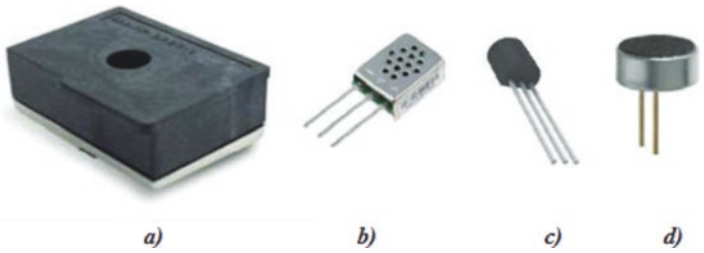


Fig. 3 Sensors used in smart city for analysis of (**a**) dust particles, (**b**) humidity, (**c**) ambient temperature, (**d**) audio

light emitting diode, reflected by the dust particles and captured through a phototransistor. The range of output values is between 0 and 0.8 mg/m^3.

- *Humidity Sensor (808H5V5)*: It is an analog sensor which provides a voltage output proportional to the relative humidity in the atmosphere. The range of output voltages is between 0.8 V (0.1% relative humidity) and 3.9 V (99% relative humidity) at 25 °C.
- *Temperature Sensor (MCP9700A)*: It is an analog sensor which proportionally changes the temperature value to an analog voltage. The output voltages range is between 100 mV −40 °C and 1,75 V 125 °C, generating a variation of 10 mV/°C, with 500 mV of output for 0 °C.
- *Audio Sensor (POM-2735P-R)*: It is an omnidirectional condenser microphone with an almost flat response in the whole frequency range of human hearing, between 20 Hz and 20 KHz. Because the output of the analog-digital converter is not correlated with the received sound pressure level, it has to be calibrated so that the return output is in the range between 50 dBA and 100 dBA.

Section 2 presents an overview of the needs, technologies, and future architectures in the context of IoT and smart cities, followed by Sect. 3 which mentions the impact of smart dust concept in healthcare surveillance for smart cities. Furthermore, Sect. 4 presents the concepts of environmental surveillance in smart cities based on IoT smart dust. Section 5 describes the main ideas about security applications based on IoT smart dust for smart cities, while Sect. 6 focuses on the privacy aspects in the context of IoEE in smart cities. Moreover, Sect. 7 introduces the concept of applications in communication, signal processing, and low power consumption by energy harvesting, which are essential in building smart dust devices. Section 8 presents the system miniaturization and architecture challenges of smart dust devices, and last but not least, Sect. 9 is the concluding section of this chapter.

2 Overview of Needs, Technologies, and Future Architectures in the Context of IoT and Smart Cities

Latest advancements of the Internet of Things (IoT) technology is to empower smart city projects and smart strategies throughout the world [1]. This section describes the actual need, future trends, technologies, and architectures of a smart city and IoT. According to a report from Gartner [1], the interest in IoT will be vital to develop and maintain smart cities and services, generating majority of the income for the economy.

A proficient smart city development should create and fuse IoT platforms that meet the requirements of the current IoT, permit the administration of a large number of associated devices, frameworks, and individuals. The main features that should be met by an IoT platform are as follows:

- Diminish expenses and create and develop IoT services
- Provide possibility to connect multiple, different systems in a city

- Reduce the implementation time and develop IoT services that are part of the smart city innovative actions
- Provide reliable and expandable service access and come up with novel opportunities for the city
- Conceive value from devices and intelligent associated data, such as top intelligent services

To create the smart city concept, numerous governments plan to adopt in the future the Information Communication Technology (ICT) concept in the administration or the public services [3].

Papers [4, 5] present the main features that an IoT platform must achieve, namely:

- Analytics
- Security
- Device management and integration
- Networking
- Protocols for data collection
- Support for visualizations

For the continuous development of the smart city market, numerous ICTs are empowering key segments, such as power, transportation, and urban planning. Latest technologies are utilized to provide intelligent and efficient innovative solutions to cities and civilians [1]. In the following, some of the trends mentioned above are highlighted, and their impact on smart cities is specified.

- *Networking and communications: LoRAWAN, 3G/4G, 5G*
- The communication technologies are fundamental for today's trends. It empowers smart cities to interface infrastructure with devices and civilians to collect information and to supply services to a multitudinous terminus. LoRaWAN technologies, 3/4G evolution, and 5G networking will play a key role in the future developments of smart cities: LoRaWAN technology uses unlicensed specter and focuses on low power and low-cost developments. Mobile technology evolutions are the focus of the 3GPP consortium which is working on CAT-1, CAT-M1, and the NB-LTE (Narrow-Band Long-Term Evolution). 5G offers a superior bandwidth and guarantees performances in energy consumption and flexibility.
- *Cloud and edge computing*
- Cloud computing has impacted the improvement of smart cities, influencing how urban communities oversee and convey services, empowering a vast number of stakeholders to enter the smart city market. Cloud computing offers different methods to reduce costs and improve efficiency. On the other hand, edge computing describes the deployment and utilization of handling inside as well as at the edge of the network.
- *Big data and data analytics*
- Big data, if organized and operated correctly, can provide insights and financial values that can be used by the stakeholders and civilians to increase effectiveness, and it can generate innovative services to enhance the quality of life.

- *Open data*
- With regard to smart cities, open data addresses the public policy that demands or gives support to public agencies to release information packages and provide accessibility to the public at large.

IoT and the other associated information technology deal with the Internet for reinforcing different devices to each other; all devices should be connected to the Internet. The most relevant applications of the IoT technology for smart city are as follows [7]:

1. *Environmental Pollution, Water, Weather, Health, and Surveillance Systems*
   Environmental pollution should be observed in a city and the gathered information transmitted to its citizens thus conveying to them the level of the pollution in their city. Sensors, such as temperature, humidity, rain, wind, etc., can be used in water and weather systems thus enhancing the effectiveness of smart cities. Also, surveillance systems can be useful to monitor the city so as to improve the degree of security continuously.
2. *Smart Grid and Energy-Efficient Operation*
   The smart grid is referring to all the newest technologies (autonomous and intelligent controllers, etc.) [5], which can create an automated and dispersed energy delivery network. The IoT technology, when applied to the power network, will contribute to a profitable power generation, consumption, transmission, and distribution.
3. *Smart Homes, Offices, Buildings*
   Sensors can maintain and control the power consumption of smart homes. The main ambition is to reduce the consumption and the resources (electricity, water, etc.) correlated with the buildings.
4. *Smart Traffic Management and Parking Lots, Urban Transportation (Public and Individual), Logistics*

Traffic management information is the most critical data source in a smart city and, by managing them properly, civilians and government could substantially profit [8]. Also, smart parking areas can be monitored; arrival and departure of various vehicles can be tracked for different parking lots in the city. Moreover, new parking lots will be built in the future when the number of vehicles exceeds the parking space.

In smart cities, sensors are essential in monitoring external parameters such as gas, smoke, air, electricity, and others. New technology must be implemented for the sensors to become robust, cheap, easy to use, and maintenance must be easy for technicians. Other ideas to monitor are to implement a series of sensors: accelerometers which can monitor acceleration and vibration, acoustic sensors used to detect sound waves. All these sensors will be minimized in size to be easily mounted and implemented with nanotechnology. Nanotechnology is especially applicable in bio-sensing applications [9].

Wireless networks are used to capture the information from the sensors, and then transmit it to a database. These networks consist of a processor, sensors, power supply,

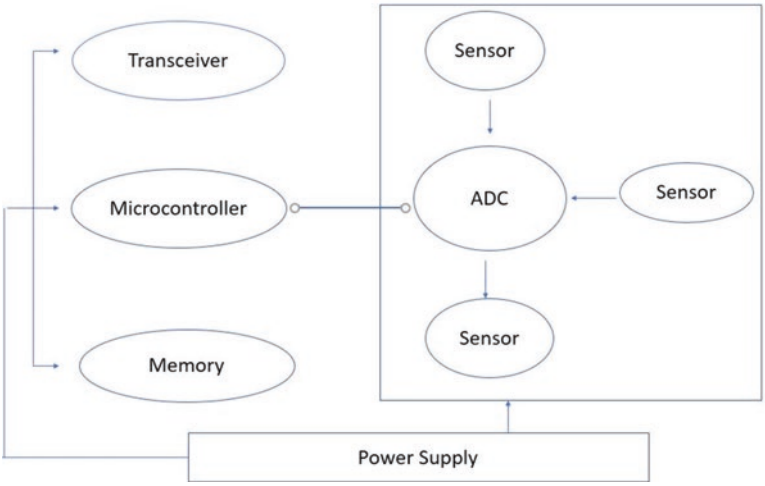


Fig. 4 Wireless sensor network

a radio interface, and a processor. Figure 4 is a diagrammatic representation of a wireless sensor network [14].

The wireless sensor network presented in Fig. 4 can be installed in a house as an indoor system based on diode (LED) lamps for capturing light and setting the intensity depending on natural light. The indoor monitoring system can be instaled on windows for capturing the factors from the room or outside to set the environmental light. These types of windows are designed to absorb or reflect light depending on the external electrical stimulus [10].

An interesting concept which arises in Big Data analytics is new in our days. This concept is used in domains like energy, transport, and smart cities. In smart cities that contain a multitude of sensors and store data on servers, these data can be analyzed.

Characteristics for big data:

- Volume: data comes from servers, social networks occupy much space, and the transmission is fast.
- Velocity: is another factor because it is based on processing speed and time to process the data.
- Variety: there are three types of data, but only two are basic: structure and unstructured and also semi-structured data. In this case, the database works for structured data [11].

Technologies and techniques for processing data:

- Store data using database and servers
- Interpret data using software programs, database, and clouds
- Collect data from sensors and process them [5]

- Enhance feasibility of algorithms using machine learning, statistics programs
- Utilize Wi-Fi networks, GPS, GPRS, LPWAN
- Visualize and interpret data for the general public

3 Healthcare Surveillance in Smart Cities Based on Smart Dust Concept

A smart city [6] has various entities, such as smart economy, smart environmental control, smart traffic system, smart governance, smart home, smart energy, and also smart healthcare. Smart healthcare doesn't necessarily mean only supervising the patient when they are in the hospital but also after the patient is discharged from the hospital. Some examples of continuous monitoring are sensing blood glucose, blood pressure, and heart rate sensors, along with the location of the patient.

Interestingly, the smart dust concept is not new; it was [7] first presented to the public in 2001 by Kristofer from the University of California. It was initially envisioned as a miniature wireless semiconductor device manufactured by using techniques from the microelectronics industry. With sizes comparable to those of grains of sand, these devices would combine sensing, computing, and communications in a single package. A smart dust network is comprised of numerous smart dust devices, enabling not only mutual communication but also data collection. Smart dust belongs to the Internet of Things environment, and at the intersection with the Web of Things, WSNs are resulted, as shown in Fig. 5.

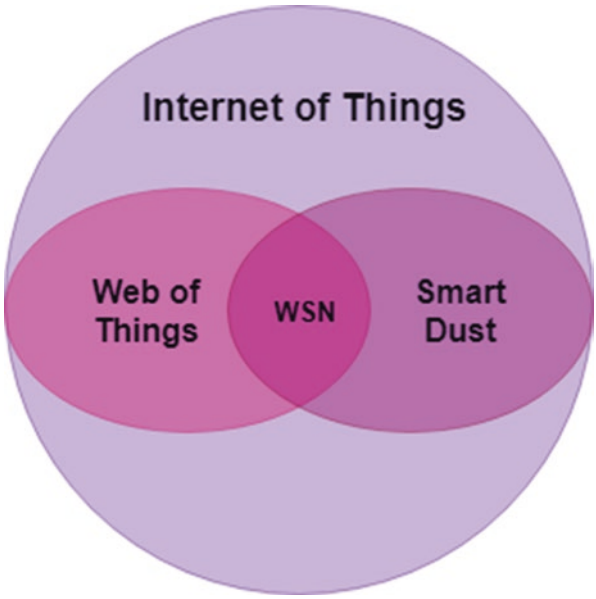


Fig. 5 The relationship between IoT, Web of Things (WoT), wireless sensor network (WSN), and smart dust [20]

Smart dust [8] overcomes the limitations brought by the sizes of surveillance equipment by deploying sensor nodes to a variety of environments and collecting real-time information.

Healthcare is a fast-growing sector and requires much attention with regard to the safety of patients and devices. As the smart city concept is newly emerging, its execution opens up vast areas for discussion. Smart dust technology can be executed in the healthcare surveillance sector in compact forms. It is common for people to go to a hospital for health-related check-ups. As the lifestyle of people has changed considerably in the last century, wearable devices have been proven to be a safe alternative for conducting health check-ups. Micro-electromechanical systems (MEMS) [9] represent mechanical and electromechanical elements at the nano-structure level. They are composed of isotropic and anisotropic etching. Also, they can include components made of thin deposition methods or anodic bonding and other technologies. One example would be microsystems sensor technology which hold an essential role in detecting data; they are low cost and work on low power microcontrollers. The main applications used in healthcare would be inertial measurement units made by accelerometers and gyroscopes. Another example would be an inertial-based system meant for motion analysis. This system is constructed based on a 9-axis complete MEMS inertial module.

The MEMS [10] accelerometers perceive the total accelerations contributed by gravitation acceleration and motion of the sensor relative to an inertial reference frame. The acceleration is detected by measuring the change in capacitance that comes from displacement between silicon microstructures forming capacitance plates. The measured capacitance may then be applied to compute acceleration. The MEMS gyroscopes measure the Coriolis force exerted by a vibrating silicon micromachine mass on its flexible silicon support when the sensor undergoes rotation. Silicon microstructures within the gyroscope use electrostatic forces exerted through capacitive plates to vibrate the suspended proof mass. The Coriolis force, generally referred to as an imaginary force, represents a mass acting on an object moving in a rotating reference frame. Rotation of the sensor includes the Coriolis force leading to a displacement of the proof mass that is proportional to the angular rotational rate.

Activities that require monitoring using MEMS inertial sensors are increasing in number. Reference [11] employs the human walking for gait analysis using two MEMS gyroscopes, one attached to each side of the lower waist. This structure allows the step detection and discrimination from other nonbipedal activities without the need for magnitude thresholds or training. It is also capable of calculating hip rotation angle in the sagittal plane which permits the estimation of step length. In [12], an ambulatory real-time rehabilitation system employs MEMS accelerometers, magnetometers, and gyroscopes to acquire the upper limb motion data of patients and to collect a group of motion quality evaluation indicators of universal significance according to the clinical needs in evaluating patient's upper limb motion quality. A novel and systematic approach [13] using MEMS sensors are estimating limb length, especially for applications such as treatment of leg limb length discrepancy (LLD).

To detect [14, 15] relative position in 3D space, data from inertial sensors require double integration. Thus, the drift and broadband noise present in the MEMS sensor result in rapid accumulation of errors. To meet the stringent accuracy requirements for use in healthcare, algorithms must be developed to reduce the impact of noise on the final result.

4 Environmental Surveillance in Smart Cities Based on IoT Smart Dust

Internet of things (IoT) can add to the commercial development of a nation. Due to the notoriety of IoT, applications identified with IoT have gained interest. Smart dust can be utilized to improve the abilities of IoT gadgets and lead to a decrease in the cost.

When it comes to talking about smart dust based on IoT applications, the basic building block is based on motes. One of the scopes of having these motes in the environment may be to develop some weather challenges, for example, how rain can affect a smart city.

There can be two essential approaches to distribute smart dust in a smart city, namely, Ubiquitous and Critical Zones.

Ubiquitous strategy can be utilized to convey smart dust to cover the entire locale of a smart city, and further, it very well may be isolated into persistent and noncontinuous monitoring.

Critical Zones can be utilized when monitoring is mandatory in zones which are sensitive to environmental activities. This system can help in diminishing establishment cost as it causes only specific zones. On the off chance that a zone is sensitive to the event of environment, at that point, vast-scale organization of the smart dust can bring about more precision in storing, sensing, communicating the events, and processing.

To make a comparison between Critical and Ubiquitous strategies, Ubiquitous is much more expensive because it needs more devices on purpose to cover the whole region.

In general, distribute smart dust is composed of several motes. Every smart dust functions as components with small size, and these are difficult to detect. Figure 6 presents systems of smart dust, which include 25 motes.

CAC or Criminal Activity Controller, helps in collecting and saving data which are transmitted by the smart dust motes.

Regarding the usability of smart dust in a smart city, it is even possible to utilize smart dust to detect microbes. For example, smart dust can be used to reduce different kinds of diseases that spread due to microbes such as fungi or bacteria.

In the future, smart dust will be used in almost every application which includes the environment. They have a huge potential in many fields such as medical, environment, engineering, and military domains.

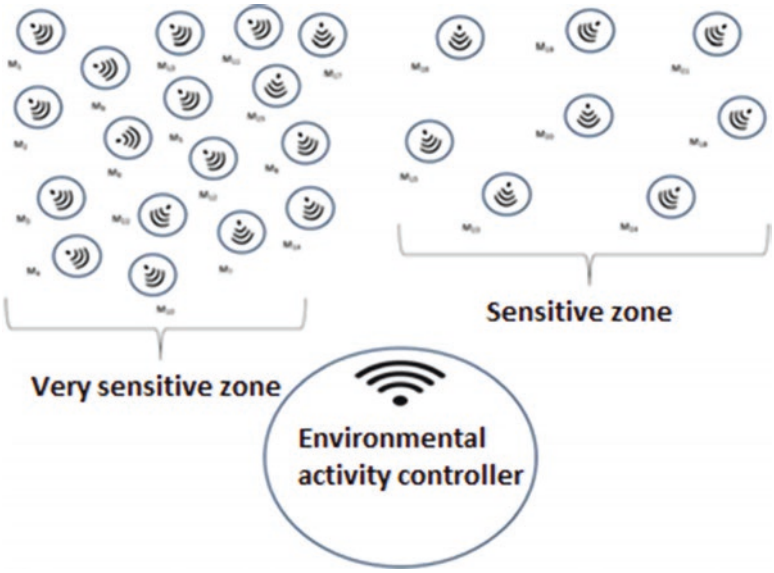


Fig. 6 Organization of smart dust in the environment [15]

On the one hand, Alvin Toffler used smart dust to analyze the environment [16]. On the other hand, Toffler and Christine Peterson [17] believe that criminals use smart dust for invading personal privacy.

Currently, a wide range of scientific authors used smart dust to detect vehicles and thus monitor vehicular activities from a specific region.

In conclusion, researchers came up with the idea that smart dust will be beneficial for the environment and people. Also, according to them, more intelligent dust sensors will improve a system that can be used in any application in a smart city.

5 Security Use Cases Based on IoT Smart Dust for Smart Cities

As a new and rising technology, smart dust brings certain risks in terms of privacy and ethics. By using this technology, data will be stored by IoT devices including smart TVs, smart speakers, toys, wearables, smart appliances, etc. These microscopic sensors which are capable of collecting visual and audio data from anywhere raise several questions about data security, privacy, and storage [18].

Sensors can be used in industrial, commercial, and security fields. Security requirements must be very tight, considering the applicability and size of the sensors and include access control, message authentication, data encryption, and key exchange.

The most sensitive fields concerning security are defense and health. To have a secure transmission of the data collected by the sensors, wireless nodes must have specific certifications and implementations of security standards included, while preserving their features such as reduced computing power and quality of communication [19]. Communication is achieved through a wireless network, more precisely through a broadcast primitive.

The requirements of a smart city include ensuring efficiency and sustainability by integrating infrastructures and services into a complete structure, simultaneously using intelligent devices for control and monitoring, as presented in Fig. 7.

Sensor usage in monitoring public infrastructures can produce more efficient use of resources, based on the collected data. Smart monitoring is valid only when working with a large number of sensors. They must be interconnected to transmit the collected data to a system where intelligent decisions can be taken based on this information.

In terms of Internet of Things (IoT), there are some issues regarding smart sensing. First, by having a large number of sensors, cabling is not a solution to be taken into consideration. Thus, the communication between sensors must be wireless. Second, there is the problem of power consumption. Due to the heterogeneity and also the number of sensors, low power communication standards are necessary.

The primary conditions to be established require sensors to be low-cost and low-powered. The only sensors that match this requirement are smart dust sensors [20]. There are three significant advantages of smart dust sensors:

1. Low system and infrastructure costs
2. Increased productivity
3. Increased safety, efficiency, and compliance levels

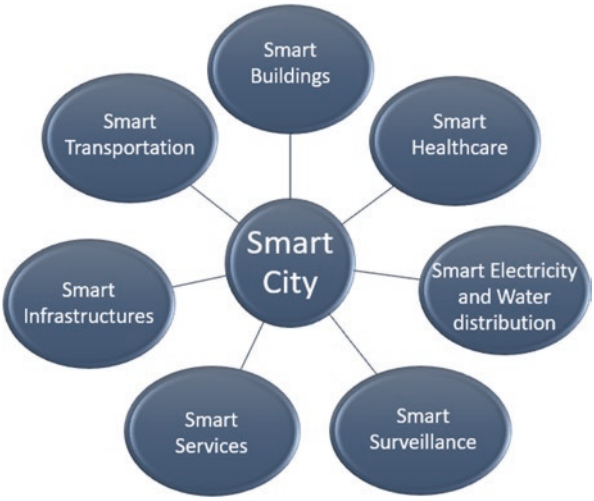


Fig. 7 Sensing in smart cities

In urban areas, smart dust sensors are used to determine traffic congestion areas or, also, can be used to predict the location of an accident if any. They also have the attribute to evaluate the structural soundness of buildings. The procedure is done by incorporating motes into the foundation of the building and checking the level of vibrations, heat, humidity, etc. [21].

Regarding the smart parking use case of smart dust, Customer Streetline Inc. company designs such solutions for cities in the United States. They have embedded sensors on the surfaces of the parking lot. The drivers activate a dashboard system using their passwords, and the system finds the nearest parking spot. With this information, traffic managers can monitor and improve traffic flows and also can boost revenue from parking meters by announcing the managers when a meter has expired.

Another important application for sensors is to monitor the quality of drinking water distribution systems, industrial uses, and surface water in the smart city. The online water quality monitoring sensor is becoming popular in water distribution systems to ensure that drinking water has the required standards. Right next to the development of electrode-based sensors that monitor various water quality parameters (pH, salinity, dissolved oxygen, solubility, temperature, turbidity, etc.), the luminescent-based sensors are gaining more attention due to their reliability, less maintenance, and a longer span of life.

Also, the free chlorine and total organic carbon (TOC) sensors are successful technologies. Application of sensor array also has high potentials for the detection of hydrophobic and highly volatile organic compounds (VOC) in water. With the advancement in sensor technology and computing and pattern recognition facility, several approaches have been reported for the real-time detection of petroleum hydrocarbon and other organic components in water. The digital sensors of monitoring and controlling activated sludge wastewater treatment processes in a full-scale plant are now the backbone of the automatic control system.

For smart cities, air quality monitoring by detecting the gaseous compound in the air is inevitable for the control of air pollution. Several smart gas sensor systems for monitoring environmental changes have been invented over the past decade for this application. This particular smart gas system can sense the complex mixture of volatile substances and perform efficiently over the years with little degradation [22].

Taking into consideration privacy concerns, smart dust networks are equipped with secure encryption and security measures. Therefore, it has been proven that there are no cases of theft of data while using these sensors [23].

However, in the scope of security and privacy of personal data, which are the two most important limitations for the growth of the Internet of Things (IoT) market, the undergoing PARFAIT (Personal dAta pRotection FrAmework for IoT interoperability) project aims to implement a platform for securing personal data within IoT applications and to reduce the complexity of deploying and integrating services in the present IoT technology by offering interoperable software tools, libraries, and SDK components.

6 Privacy Perspectives in the Context of the Internet of Everything, Everywhere (IoEE) in the Smart Cities

The IoEE brings together people, data, processes, and things, network connections gaining significant importance within people's lives, as presented in Fig. 8. With the evolution of IoEE, risks regarding privacy and confidentiality of personal data are becoming a significant concern. For any technology, the privacy rights of citizens should be guaranteed anywhere and anytime. Despite the benefits of smart cities services, privacy breaches are becoming worrisome because smart city applications not only have access to a wide range of privacy-sensitive information from people's lives but also it processes this information, by manipulating it.

Smart city applications raise several concerns and challenges in terms of security and privacy. The sensitive data from smart cities should be protected from unauthorized access, disclosure, disruption, modification, inspection, and deletion, but it is still vulnerable to privacy leakage and information inferring by outside hackers since private information is collected, transmitted, and processed. The disclosed privacy in a smart city may contain a user's identity and location in transportation, a health condition in healthcare, lifestyle inferred from intelligent surveillance, smart energy in homes, offices, and community [1].

In smart cities, privacy and public safety remain a major concern that needs more legal, scientific, and political consideration. It is imperative to fight against cybercrime in smart cities. The countermeasures that can be taken in specific urban sectors and also the threats they face are enumerated in Table 1.

Most smart city services are based on ICTs. Sometimes users (especially teenagers and the elderly) do not experience security issues and become ideal targets for attackers when interacting with their smartphones, tablets, and computers with many smart city services and disclosing information.

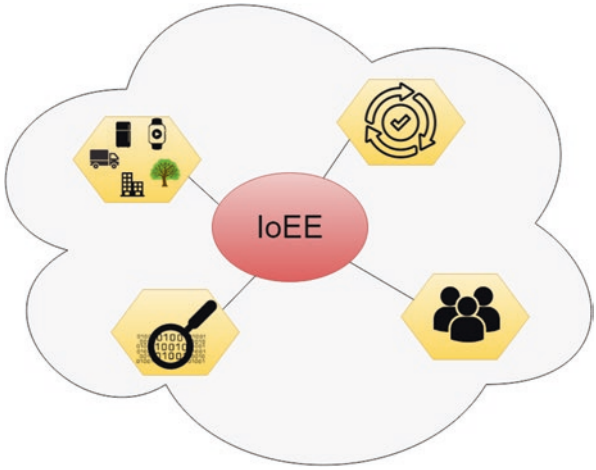


Fig. 8 The IoEE bringing together people, data, processes, and things

Table 1 Security and privacy concerns and countermeasures in smart cities [34]

Sector	Threats	Countermeasures
Smart buildings sector	Infection by malware systems failure Fraud by staff and unauthorized users Controlling the fire system Causing physical damage such as flooding. Disrupting building temperature (overheating or overcooling) Damaging or controlling lifts and escalators Open windows and doors Modifying smart meters Opening parking gates Disabling water and electricity supplies Starting/stopping of irrigation water system Stopping renewable energy systems (RES)	Two-factor authentication and one-time passwords for stronger authentication IoT forensics (DigiCert IoT PKI Solutions, and Symantec solutions) Threat and risk modeling Data backup and recovery solutions to ensure reliability and continuity of services
Transport sector	Sending false emergency messages Disrupting a vehicle's braking system Stopping the vehicle's engine Triggering false displays in the vehicle's dashboard Disrupting the vehicle's emergency response system Changing GPS signals	Public critical infrastructure (PKI), digital certificates (ECDSA), and data encryption solutions (ECIES and AES) Misbehavior detection solutions Pseudorandom identities
Government sector	Preventing of cybercrime Identity theft Disrupting critical infrastructures Fiscal fraud Altered files	Data leakage prevention Risk assessment Insider threat analysis Awareness training
Healthcare sector	Modifying patients record or information Exposing sensitive data unintentionally Disrupting the monitoring system Disrupting the emergency services Sending false information Jamming attacks Sending an emergency alert Eavesdropping sensitive information	Secured Wi-Fi networks to guarantee safe handling of confidential information and personal data (AirTight Networks solutions, Aerohive security solutions) Risk assessment (Rapid solutions, Health Security Solutions, SafeNet's data security solutions, Stanley security solutions, Intel healthcare security solutions)

(continued)

Table 1 (continued)

Sector	Threats	Countermeasures
Energy sector	Spoofing addresses and usernames Unauthorized access and controls Zero-day attacks Botnets (Zeus, ZeroAccess, Conficker, etc.) Denial of service and distributed denial of service (DDoS)	Intrusion detection and prevention techniques Risk assessment Insider threat analysis Cybercrime intelligence
Financial sector	Loss of privacy Accounting fraud Disrupting business processes Accessing confidential company information Accessing confidential customer information Damaging reputation(s) Defacing websites Financial and reputation concerns due to fraud and data leakage Denial of service and DDoS Phishing Mobile banking exploitation SQL injection	Anti-malware solutions Encrypted files and firewalling Fraud detection and prevention techniques Risk assessment (MEHARI, EBIOS) Insurance to mitigate cybercrime risk Cybercrime intelligence

To understand the importance of data protection challenges in smart cities, an example has been cited. The number plate of a vehicle is related to the identity of the vehicle owner. Thus, the trajectory of a vehicle can be easily tracked, even if all communications between the vehicle and the infrastructure are encrypted and each device is authenticated by others. It violates the general notion of privacy, which includes the right of individuals to live their lives in a manner that is somewhat beyond the control of the public. In a smart city, future vehicles will have various communication features, including Internet access, GPS, electronic toll collection (ETC), and radio-frequency identification (RFID). The devices connected in a vehicle store much personal information and have multiple communication functions. In a smart city, the number of connected devices is very high. With data collected by IoT devices, data users can understand the behavior of data owners or use this data to obtain highly personal information, including whereabouts of the individual.

An information system has three primary operations: data transfer, storage, and processing. All of these operations may raise privacy issues affecting the user's behavior. Services may be associated with the user's location, which can create privacy issues. For example, in a smart city, two companies can use data protection procedures to compare their activities without revealing their critical data. It is possible to use an approach based on linear algebra operations, such as matrix multiplication, to solve linear systems and calculate the correlation between distributed

datasets. The proposed solution is efficient and theoretically secure. However, on a large scale, the performance of this solution is unreliable because it depends on a trusted initializer that must send data to the parties involved before running the protocol. Unfortunately, privacy techniques do not address restrictions such as frequent changes to unapproved members and third parties (cloud providers). Therefore, protection of privacy remains a significant challenge [1].

A legislation is essential to ensure privacy in smart cities. The UK Parliament recently passed a bill to give intelligence agencies unlimited access to users' Internet browsing data. Under this law, intelligence agencies can legally intercept and decipher people's communications. Service providers can save users' browsing data for 12 months. Police can also legally hack computers, networks, and mobile phones. However, Microsoft, Facebook, Google, Yahoo, and Twitter rejected this project. Human Rights Watch argued that this type of project is dangerous and too intrusive to the confidentiality of the organization. In France, a new law on surveillance was adopted in July 2015 (Law No. 2015-912 of July 24, 2015). The new law allows intelligence agencies to monitor the communication (e-mails and phone calls) of suspects [1].

7 Use Cases for Communication, Signal Processing, and Low Power Consumption by Energy Harvesting

To transfer data and to provide power, most of today's sensor networks are based on a wired infrastructure. However, this type of configuration for communication and power often leads to costs which are much bigger than the value of the sensors themselves. Moreover, during the recent years, wireless connectivity has been an essential alternative for sensors, because of its reliability. In addition, wireless communication for smart sensors systems has been reduced to cases where it is acceptable to lose occasionally the connectivity and the data. To reduce energy consumption, the technology of passing optical communication for smart dust motes was studied. One of the smallest optical motes (each wireless sensor node) in the present has only 4 mm^3, contains An 8-bit Analog to Digital Converter (ADC), a sensor for light, an accelerometer, a source for power represented by a multi-voltage solar cell, an optical receiver, a corner-cube reflector passive optical transmitter, and a limited computation. A newer version of a sensor mote presents a complete radio-frequency transceiver, an ADC, microprocessor, and a sensor interface.

The Internet revolution has represented an essential aspect of replacing point-to-point wired communications by multi-hop wired communications. The fact which makes the Internet reliable is that the Internet mesh is insensitive to the loss of a node or a path [2].

One of the most critical aspects of the smart dust network is communication between dust nodes. All the motes in the network have to communicate with each other through the base station. While considering all the design constraints due to

size and power limitation, data must be collected from the motes simultaneously, sent to the base station for further action [2].

In downlink (i.e., data propagation from the base station to the dust motes), the base station broadcasts to all the specks in the network at a rate of several kbps. Moreover, in the uplink (i.e., data propagation from motes to the base station), the data transfer rate is of 1 kbps. Hence, if a total number of 1000 dust motes are employed in the network, the data throughput will be 1 Mbps. The data transfer both in uplink and downlink should support distances of a couple of hundred meters [12].

There are other specifications regarding the mote. Dust mote size should be less than 1 mm^3 and must have a power consumption of at the most 1 μW. We also need a secure and reliable transmission method for communication in the network.

The task of the communication system is to send and collect commands to and from motes:

- Radio-frequency transmission
- Optical transmission technique
- Fiber-optic communication

Radio-frequency (RF) technology has advanced a lot in the last few years and is being used widely in different applications. In this method of transmission, radio-frequency signals of range from tens of KiloHertz to hundreds of GigaHertz are used [12].

The main feature which provides the reliability in a multi-hop radio-frequency mesh sensor network is the end-to-end furnishing of time-stamped sensor data with a determined worst-case latency. The main requirement for the reliability of the time-stamping is the choice of radio, the use of spectrum, as well as the network synchronization. Most of the motes operate in large bands which have values from 902 to 928 MHz (in North America) or from 2.4 to 2.458 GHz (most of the world).

Because these kinds of bands are open to transmitters and they put out about 1 W, the motes generally have an output value of 1 mW to extend the life of the battery; in this case, they have to maintain the reliability by avoiding high-power interferers. These kinds of interferers, as well as the unpredictable fading ones, exclude the use in high-reliability applications of fixed-frequency radios. A solution can be considered reliable if it is capable of avoiding or working near the parts of the spectrum that are jammed or very faded [17].

RF communication is a perfect potential candidate for smart dust networks, but at the same time, there are a couple of problems associated with it:

- RF transceivers, it is almost impossible to achieve the low power specification requirements needed for smart dust system.
- One of the issues addressed in antenna design is the size limitation. Size of a fabricated antenna is limited by margins based on the range of its cubic millimeter. An antenna size cannot exceed a quarter of the wavelength of the carrier, and the size shall be defined in the area of very short of the wavelength which results in having an operation which does not necessarily run at efficient power consumption.

- Due to the high number of dust motes, it is necessary to use multiplexing techniques for achieving RF communication; multiplexing techniques, such as code-division multiplexing or time/frequency multiplexing. This means that several kinds of RF circuitry like filters, modulators, and demodulators are needed, and they should be designed for low power consumption.
- Using multiple access techniques such as TDMA or CDMA or similar SDM has their complexity, which is not compatible with the smart dust system.

Optical communication utilizes semiconductor lasers and diode receivers for transferring optical signals. This optical communication method is more compatible with the low power design requirements due to the small size of optical transceivers. In optical communication, we can easily create a 1GHz signal from a millimeter aperture, but to produce the same signal in RF communication an antenna of 100 meters is required (due to the wavelength difference between two transmissions). Concerning power, once again, optical communication is advantageous because it has a simple circuit.

The passive reflective communication consists of a particular device called CCR (corner-cube retroreflector) with three mutually orthogonal mirrors. Light enters the CCR, and the reflection is parallel to its direction [13]. In the case of the MEMS version, there is only one mirror mounted on the device, at an angle that is not perpendicular to the other mirrors [24].

When the mirror is positioned as described above, a value of digital 0 is obtained, because there is only a small amount of light that returns to the source. If a value of digital 1 is desired, we have to apply a voltage between an electrode that is underneath the mirror and on the mirror itself to obtain a position of the mirror perpendicular to the other mirrors. Due to the low mass of the mirror, the CCR device can switch between the 0 value and the 1 value up to thousand times per second, and using a small amount of energy, less than a nanojoule per transition.

In this type of communication, an onboard light source is necessary for the dust mote. However, by using a particular configuration composed of mirrors, it may or may not be possible to reflect the light to a source that is remote. Figure 9 presents the corner-cube retroreflector (CCR) that is utilized to adapt the idea of the smart dust [2].

For the mote-to-mote communication, a system active-steered laser uses an onboard light source to send a light beam to a receiver.

The advantage of this laser communication is its high power density. The density of a 1 milliwatt laser radiating into 1 milliradian is approximately 318 kilowatts per steradian, as opposed to a 100 watt light bulb that radiates 8 watts per steradian isotropically.

A smart dust transmitted beam has a divergence of approximately 1 milliradian, allowing transmission over enormous ranges using milliwatts of power [2].

Every mote carefully weighs the needs to sense, compute, communicate, and evaluate its energy reserve status before allocating nanojoules of energy to turn on its transmitter.

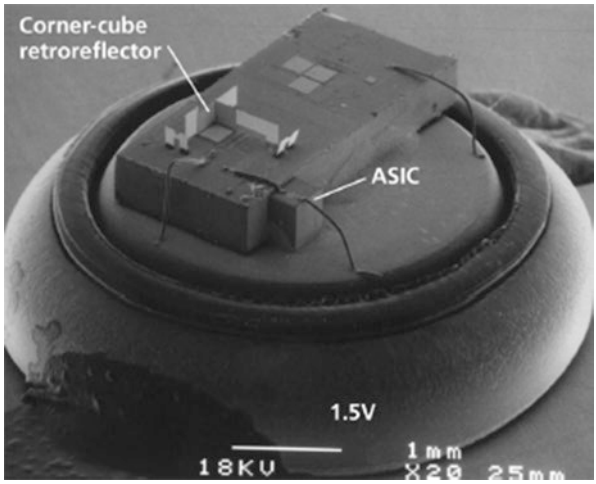


Fig. 9 Autonomous bidirectional communication mote with a MEMS optics chip containing a corner-cube retroreflector on the large die, a CMOS application-specific integrated circuit (ASIC) for control on the 300 × 360 microns die, and a hearing aid battery for power. The total volume is 63 mm^3

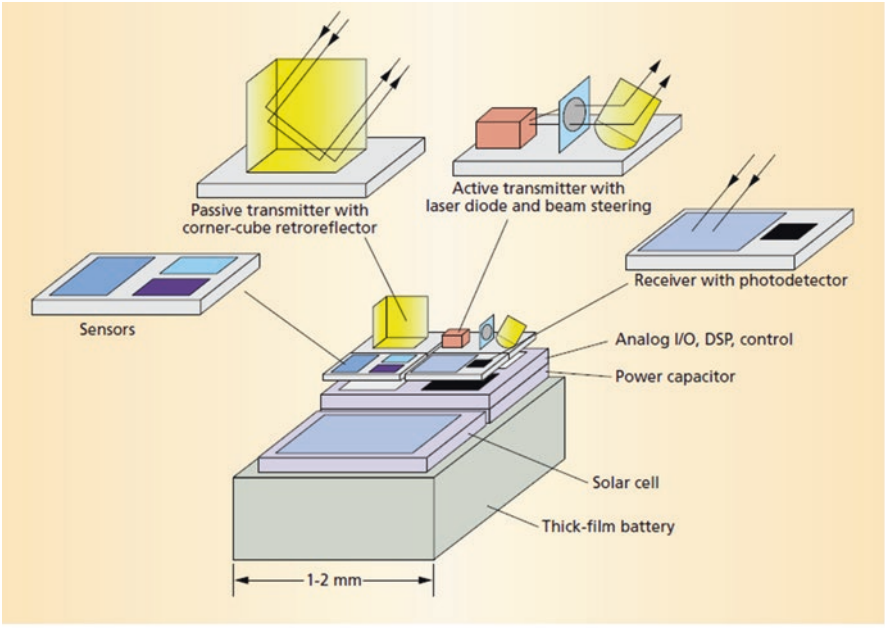


Fig. 10 Power system

Using burst mode transmission, in which the laser operates at up to several tens of Mbps for a few milliseconds, it assures the best energy-efficient method to program this mesh. This system utilizes the energy reserves and minimizes the mote's duty cycle, as shown in Fig. 10.

A semiconductor laser, a fiber cable, and a diode receiver are utilized to generate, transfer, and detect the optical signal. The power consumption is low due to the small size of the optical transceiver, and there is no need for a light source on the dust mote itself [12].

There are some advantages and disadvantages in fiber-optic communication. In fiber-optic communication, there is no need for the line-of-sight, because it uses fiber-optics to transfer and receive optical signals. This method is also safer for human eyes as no laser is involved. An extended range of communication and guaranteed communication between the dust motes and base station are two other advantages.

The fiber-optic cables are the source that limits the movement and mobility of dust motes. Moreover, each dust mote should have a connection to the base station (lots of cables), which makes the design of the base station a complicated task.

Generally, in a smart dust design, the main challenge concerns the minimum energy consumption that is necessary to power the circuits and MEMS devices. Moreover, the primary constraint after fitting the entire mote into 1 mm^3 volume is the energy density of the power supply [2].

Nowadays, most of the applications in the building as well as in the industrial automation require a lifetime which can be measured in years. In this situation, the need of the hour is a battery that has a lifetime from 1 to 10 years, thus avoiding the costs of the replacement of a high-powered battery. Using a battery of type AA that has a charge about 12000 J, an inch-scale mote needs to have an average power consumption that does not exceed a few joules or tens to hundreds of microwatts per day.

To achieve the values mentioned above, and to meet the current consumption of tens of microamps, a deep duty cycle is required. This implies the ability of the hardware to switch quickly from the powered state to the unpowered state (and low leakage) and vice versa. In the digital circuits, especially the SRAM, at shallow duty cycles, the leakage power can dominate the energy of the system.

In a profoundly duty-cycled environment, besides the problem of leakage, there are other significant challenges for multi-hop mesh networking which has radio communication. Most of these challenges concern the development of the algorithms and the software. In this situation, it is preferable to have hardware support that can provide some combination of more-to-more time synchronization, fast radio polling, and also a low-power detection of RF energy [17].

8 System Miniaturization and Architectural Challenges

Miniaturization allows integration of any type of mote into a single device and its functioning with a smart dust system. Size reduction is significant in reducing the cost of the nodes and making its implementation easy.

Smart dust can include hundreds to thousands of dust motes, each containing one or more sensors, analog circuitry, a power supply, bidirectional communication, and a programmable microprocessor.

Advances in miniaturization, integration, and energy management in a digital circuit, micro-electromechanical systems (MEMS) led to the manufacturing of small sensors, optical communication components, and power supplies.

Micro-electromechanical systems consist of extremely tiny mechanical elements, often integrated with electronic circuitry. All these are measured in micrometers, similar to computer chips. In addition to the advantage of making small structures, this manufacturing process can simultaneously fabricate thousands or even millions of system elements. This makes the system highly complex and extremely low in cost.

It is certainly expected that future prototypes of smart dust could be small enough to remain suspended in the air, beyond air currents, sensing and communicating for hours or days on end.

According to the requirements of power constraints in smart dust, the performance is handled this way: a cubic-millimeter battery supports one Joule of energy (1 J/mm^3). With the corner-cube reflector described in Fig. 11, communication costs about 1 nJ/bit, while sensing can be achieved at ~1 nJ/sample. For example, the StrongARM SA1100 processor computes ~1 nJ per instruction.

A smart dust constraint is related to its design for the minimum energy consumption of MEMS devices. The challenge here is to integrate a mote into a 1 mm^3 volume, but the energy density of the power supply is the primary issue. The existent batteries have ~1 J/mm^3 of energy and high series resistance. The existent capacitors can achieve maximum ~10 mJ/mm^3 with a low series resistance [40, 41].

The size of a MEMS is in the range of 1 mm and 1 μm, and the size of a NEMS is in the range of 1 nm to 100 μm. A MEMS/NEMS structure is thin-walled, and it is exposed to mechanical loading, high temperature, and electromagnetic fields. MEMS/NEMS can interact mechanically and thermally with other layers, bases, and elements. This contact is realized with thin heat-conducting layers [2].

A team from the University of Michigan designed the Michigan Micro Mote, which is 2 millimeters wide—the smallest size known. Reducing the size of the

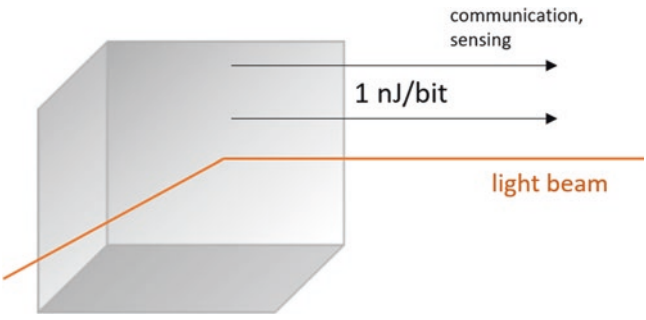


Fig. 11 The corner-cube reflector (CCR) [39]

battery was a great challenge. According to Blaaw, an application is needed that drives the final production of smart dust sensors to remain low cost. Building such an application presented to be a challenge in the smart dust economy [2].

The MEMS cubic device is presented in Fig. 12 [2]. It is structured in an analog I/O and DSP control, a passive transmitter, an active transmitter, a receiver which is a photo-detector, a solar cell, a thick-film battery, and a power capacitor, as shown in Figs. 13, 14, and 15.

The challenge in MEMS microcubes is to maintain low power consumption and to maximize the life of a mote. The total energy stored on average a micro-sized power battery is 1 J. The solution is to keep the total energy consumption under microwatt values and to use solar cells that produce 1 J per day

The architecture presented above is included in the structure of a mote, along with the sensors. Therefore, a mote gathers data from the environment related to

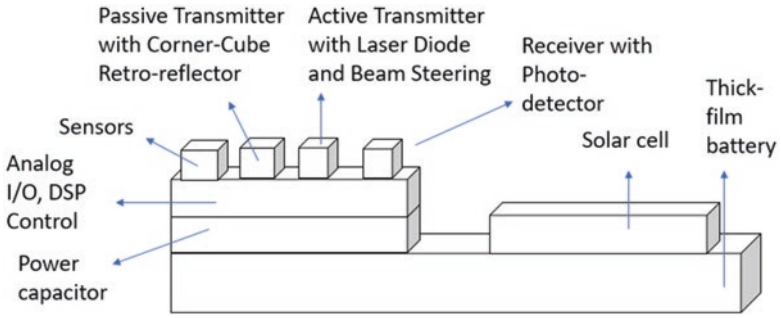
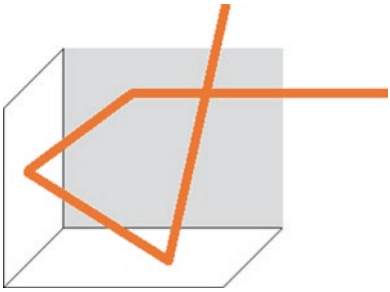


Fig. 12 The MEMS architecture

Fig. 13 The passive transmitter which is a corner-cube retroreflector is hit by a light beam



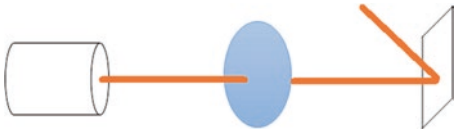


Fig. 14 The active transmitter in which a light beam from a laser diode (left) is being directed through a steer lens, toward a reflector (right)

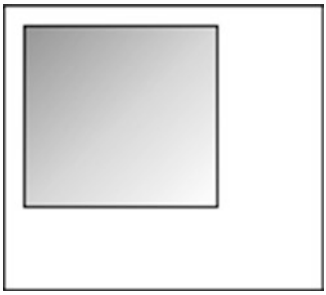


Fig. 15 Receiver with photo-detector

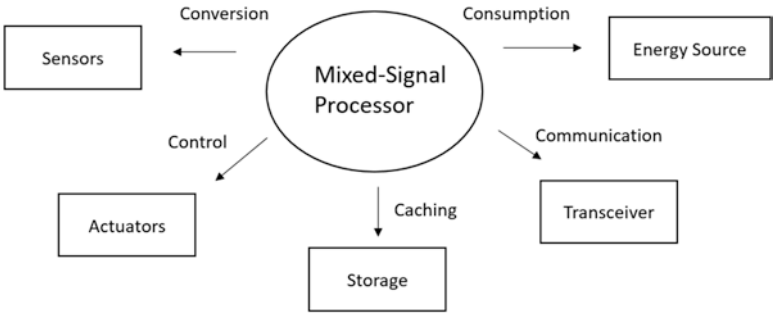


Fig. 16 A wireless body area sensor network

temperature, light, and other parameters, depending on which domain the mote will be installed. The MEMS mote is well suited for air monitoring and video monitoring in a smart city.

Low-cost microsystem sensor technologies are available in healthcare [25] with inexpensive low-power microcontrollers and reliable telemetry modules. These technologies are upgraded versions. MEMS-based sensors have emerged recently. Therefore, inertial measurement unit having accelerometers and gyroscopes in their structure are well known, for example, the 3-axis MEMS accelerometer [21].

A wireless body area sensor network [44] is shown in Fig. 16. This figure highlights how each node of a body area sensor network has an interface with the organic tissue. Each node has an integrated energy source. Nodes can be in the form of sensors with an integrated processor, a sensor with an integrated transceiver, and sometimes data storage or feedback control to body-based actuators, such as an insulin pump or robotic prosthetic.

Signal processing is the main challenge posed by wireless body area sensor network—the way they interconnect, handle energy, and the way sensors gather information from the environment.

In the MEMS application of body area sensor networks, a small-size thermoelectric generator is attached to the skin. For this purpose, a thermoelectric bracelet using commercial BiTe thermopiles is designed and tested. The average energy power is 100 μW, so the sensor layer is connected and sends data. Furthermore, generator parameters can be sent to a PC through a self-powered wireless module [45].

9 Conclusions

Internet of Everything, Everywhere (IoEE) [28, 29] concept represents the basic technology behind connecting smart dust systems in sectors such as healthcare or smart cities. Security, privacy, and safety are also in the scope of this chapter's research, since the sensors which equip a smart dust system collect different types of data from various devices that belong to individuals. Applications related to smart city generally have access to a broad range of people's privacy-sensitive data. Therefore, security breaches are a concern that must be reduced or even eliminated.

Smart dust[26–29] sensors are small dimension sensors used to monitor and collect data for efficient usage of resources. One of the main advantages of these sensors is that they are safe to be used in terms of the designed encryption, knowing that there are no known cases of information theft.

Within smart cities, with numerous entities, such as smart economy, smart environmental control, smart traffic system, smart governance, smart home, smart energy, and also smart healthcare merge together; thus, smart dust [30, 31] technology overcomes the limitations resulting from the size of the surveillance equipment, has low system and infrastructure costs, and also collects real-time information.

Several case studies have been presented, in which the benefits of smart dust technology have made an impact, in terms of healthcare surveillance and environmental surveillance in smart cities[32–37], communication, signal processing, and low power consumption by energy harvesting [42, 43].

As future work, development of smart dust surveillance [38] system will be undertaken in hospitals, to gain better management of patients, bearing in mind their privacy and confidentiality and sensitivity involved.

Acknowledgments This work has been supported in part by UEFISCDI Romania and MCI through projects CitiSim, ESTABLISH, PARFAIT and WINS@HI, funded in part by European Union's Horizon 2020 research and innovation program under grant agreement No. 826452 (Arrowhead Tools), No. 787002 (SAFECARE), No. 777996 (SealedGRID) and No. 813278 (A-WEAR).

References

1. Lyshevski, S.E. (ed.): Nano-and Microscience, Engineering, Technology, and Medicine Series. CRC Press, Boca Raton (2002)
2. Lyshevski, S.E.: MEMS and NEMS: Systems, Devices, and Structures. CRC Press, Boca Raton (2018)
3. Shaik, M., Shaik, N., Shaik, W.: The wireless sensor networks: smart dust. Int. Res. J. Eng. Technol. **3**(6), 910–913 (2016)
4. Sanchez-Rosario, F., Sanchez-Rodriguez, D., Alonso-Hernández, J.B., Travieso-González, C.M., Alonso-González, I., Ley-Bosch, C., Ramírez-Casañas, C., Quintana-Suárez, M.A.: A low consumption real time environmental monitoring system for smart cities based on ZigBee wireless sensor network. In: 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 702–707. IEEE, August 2015

5. Hammi, B., Khatoun, R., Zeadally, S., Fayad, A., Khoukhi, L.: IoT technologies for smart cities. IET Netw. **7**(1), 1–13 (2017)
6. By, G.S.: 2020, More than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things. Publicado em Janeiro (2016)
7. Sánchez López, T., Ranasinghe, D.C., Harrison, M., Mcfarlane, D.: Adding sense to the Internet of Things. Pers. Ubiquit. Comput. **16**(3), 291–308 (2012)
8. Gazis, V., Görtz, M., Huber, M., Leonardi, A., Mathioudakis, K., Wiesmaier, A., Zeiger, F., Vasilomanolakis, E.: A survey of technologies for the Internet of Things. In: 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 1090–1095. IEEE, August 2015
9. Dayarathna, M.: Comparing 11 IoT Development Platforms, IoT Zone (2016)
10. Lea, R. J.: Smart Cities: an overview of the technology trends driving smart cities, IEEE, (2017) https://doi.org/10.13140/RG.2.2.15303.39840
11. Rajab, H., Cinkelr, T.: IoT based smart cities. In: 2018 International Symposium on Networks, Computers and Communications (ISNCC), pp. 1–4. IEEE, June 2018
12. Neyestani, N., Damavandi, M.Y., Shafie-khah, M., Catalão, J.P.: Modeling the PEV traffic pattern in an urban environment with parking lots and charging stations. In: 2015 IEEE Eindhoven PowerTech, pp. 1–6. IEEE, June 2015
13. Hancke, G., Silva, B., Hancke Jr., G.: The role of advanced sensing in smart cities. Sensors. **13**(1), 393–425 (2013)
14. Bibri, S.E.: The IoT for smart sustainable cities of the future: an analytical framework for sensor-based big data applications for environmental sustainability. Sustain. Cities Soc. **38**, 230–253 (2018)
15. Singh, J., Singla, V.: Big data: tools and technologies in big data. Int. J. Comput. Appl. **112**(15), 6–10 (2015)
16. Ghaffarianhoseini, A., AlWaer, H., Ghaffarianhoseini, A., Clements-Croome, D., Berardi, U., Raahemifar, K., Tookey, J.: Intelligent or smart cities and buildings: a critical exposition and a way forward. Intell. Build. Int. **10**(2), 122–129 (2018)
17. Muhammad, G., Alsulaiman, M., Amin, S.U., Ghoneim, A., Alhamid, M.F.: A facial-expression monitoring system for improved healthcare in smart cities. IEEE Access. **5**, 10871–10881 (2017)
18. Mannir, M., Getso, A., Ismail, M.: Internet of things and smartdust: the future of wireless internet of things and smartdust. Int. J. Inf. Syst. Eng. **5**(1), 13–23 (2017). https://doi.org/10.24924/ijise/2017.04/v5.iss1/13.23
19. Lee, J., Sung, Y., Park, J.: Lightweight sensor authentication scheme for energy efficiency in ubiquitous computing environments. Sensors. **16**(12), 2044 (2016)
20. Dasarathan, S.: Distributed Inference Using Bounded Transmissions. Arizona State University, University of Arizona Press (2013)
21. Ciuti, G., Ricotti, L., Menciassi, A., Dario, P.: MEMS sensor technologies for human centred applications in healthcare, physical activities, safety and environmental sensing: a review on research activities in Italy. Sensors. **15**(3), 6441–6468 (2015)
22. Wang, Y., Ashktorab, M., Chang, H.I., Wu, X., Pottie, G., Kaiser, W.: Wearable motion sensing devices and algorithms for precise healthcare diagnostics and guidance. In: Mobile Health, pp. 203–218. Springer, Cham (2017)
23. Nasr, A.: Novel Technique for Gait Analysis Using Two Waist Mounted Gyroscopes, Master of Science, Old Dominion University (2018)
24. Tao, G., Sun, Y., Huang, Z., Wu, J.: A real-time micro-sensor upper limb rehabilitation system for post-stroke patients. In: 2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES), pp. 232–235. IEEE, August 2015
25. Maddumage, S.K., Li, S., Pathirana, P., Williams, G.: Entropy-based method to quantify limb length discrepancy using inertial sensors. IET Wirel. Sens. Syst. **8**(1), 10–16 (2017)

26. Jain, S.K., Kesswani, N.: Smart judiciary system: a smart dust based IoT application. In: International Conference on Emerging Technologies in Computer Engineering, pp. 128–140. Springer, Singapore, February 2019
27. Smart Dust Future: Online Available: https://www.nanowerk.com/news/newsid=8535.php (2008). Accessed 14 Jan 2019
28. Ilyas, M., Mahgoub, I.: Smart Dust: Sensor Network Applications, Architecture and Design. CRC press, Hoboken (2018)
29. Kabir, M.N.: Technologies of the future. In: Knowledge-Based Social Entrepreneurship, pp. 91–133. Palgrave Macmillan, New York (2019)
30. Cook, B.W., Lanzisera, S., Pister, K.S.J.: SoC issues for RF smart dust. Proc. IEEE. **94**(6), 1177–1196 (2006)
31. Warneke, B., Last, M., Liebowitz, B., Pister, K.S.: Smart dust: communicating with a cubic-millimeter computer. Computer. **34**(1), 44–51 (2001)
32. Shamsir, S., Mahbub, I., Islam, S.K., Rahman, A.: Applications of sensing technology for smart cities. In: 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 1150–1153. IEEE, August 2017
33. Kahn, J.M., Katz, R.H., Pister, K.S.: Emerging challenges: mobile networking for "smart dust". J. Commun. Netw. **2**(3), 188–196 (2000)
34. Bora, A.A., Kapsikar, S., Kelani, P.: Security and privacy in smart city applications: challenges and solutions. Int. J. Electron. Commun. Soft Comput. Sci. Eng. (IJECSCSE). 165–169 (2018)
35. Khatoun, R., Zeadally, S.: Cybersecurity and privacy solutions in smart cities. IEEE Commun. Mag. **55**(3), 51–59 (2017)
36. Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G., Suciu, V.: Smart cities built on resilient cloud computing and secure Internet of Things. In: 2013 19th International Conference on Control Systems and Computer Science (2013)
37. Kumar, H., Singh, M.K., Gupta, M.P., Madaan, J.: Moving towards smart cities: solutions that lead to the smart city transformation framework. Technol. Forecast. Soc. Chang. 119281 (2018)
38. Hanson, M.: Study on Smart Dust Networks, Dissertation Thesis, Linköping University (2016)
39. O'brien, D.C., Liu, J.J., Faulkner, G.E., Sivathasan, S., Yuan, W.W., Collins, S., Elston, S.J., Pithamiron, V.: Design and implementation of optical wireless communications with optically powered smart dust motes. IEEE J. Sel. Areas Commun. **27**(9), 1646–1653 (2009)
40. Warneke, B., Bhave, S.: Smart Dust Mote Core Architecture. Project report, Berkeley Sensor and Actuator Center, Berkeley, CA. Available at: http://bwrc.eecs.berkeley.edu/Classes/CS252/Projects/Reports/warnke.pdf (2000)
41. Niccolai, L., Bassetto, M., Quarta, A.A., Mengali, G.: A review of Smart Dust architecture, dynamics, and mission applications. Prog. Aerosp. Sci. **106**, 1 (2019)
42. Czenkanski, A., Zozulya, V. V.: A Higher Order Theory of Beams and Its Application to the Mems/Nems Analysis and Simulations, CSME International Congress, Toronto, Canada (2018)
43. Goldsmith, C.: Microscopic 'smart dust' sensors are set to revolutionise a range of sectors, online available: https://www.theneweconomy.com/technology/microscopic-smart-dust-sensors-are-set-to-revolutionise-a-range-of-sectors. Accessed 16 Mar 2019
44. Hanson, M.A., Powell Jr., H.C., Barth, A.T., Ringgenberg, K., Calhoun, B.H., Aylor, J.H., Lach, J.: Body area sensor networks: challenges and opportunities. Computer. **42**(1), 58–65 (2009)
45. Leonov, V., Fiorini, P., Sedky, S., Torfs, T., Van Hoof, C.: Thermoelectric MEMS generators as a power supply for a body area network. Solid State Sens. Actuators Microsyst. **1**, 291–294 (2005)

Raluca Maria Aileni is scientific researcher of third degree in computer science and has obtained her Ph.D. in industrial engineering at Technical University "Gheorghe Asachi" of Iasi in 2012. She did her Ph.D. at the Department of Electronics, Telecommunication, and Information Technology, Politehnica University of Bucharest. She graduated in Textile Leather and Industrial Engineering Management and of Computer Science. In 2010, during her Ph.D., she obtained a research fellowship for doctoral studies at ENSAIT-Lille University of Science and Technology, France, where she specialized in 3D modeling and simulation for textiles, using the Kawabata system, 2D-3D Design Concept for the design and simulation of technical textile articles. In 2015, she obtained the Excellence Fellowship Grant for doctoral studies in Belgium, Mons University.

George Suciu is a senior researcher of third degree, with more than 15 years of experience in R&D projects. He graduated from the Department of Electronics, Telecommunications, and Information Technology at the University POLITEHNICA of Bucharest, where he also received his M.Sc. He holds a Ph.D. in cloud communications from the same university. Also, he holds a MBA in Informatics Project Management and IPR from the Department of Cybernetics, Statistics, and Economic Informatics of the Academy of Economic Studies Bucharest, and currently, his post-doc research work is focused on the field of cloud communications, blockchain, big data, and IoT/M2M. George has experience as coordinator and WP leader for over 30 R&D projects (FP7, H2020, Eureka/Eurostars, etc.) and is involved currently in over 10 international and five national projects. He has both authored and co-authored over 150 journal articles and scientific papers presented at various international conferences, holding over five patents. He is R&D and Innovation Manager at BEIA Consult International from 2008, having previously worked as ICT Solutions Manager from 1998.

Martin Serrano Dr. Serrano is a recognized IoT expert on Semantic Interoperability, Data Modeling, and Distributed Data Systems Design, an also an End-to-End Solutions Architect with a strong background in Applied Semantics and Information Systems Interoperability, Smart Technology, Services and Network Management and Communications Management Systems. He leads the Internet of Things, Stream Processing and Intelligent Systems Research Unit (UIoT) at the Insight Centre for Data Analytics. He holds a M.Sc. and a PhD from the Technical University of Catalonia (UPC Tech), Spain and before joining academia, he worked in industry as Senior Engineer Supervisor at KME/National Panasonic in Tamana-Taimei, prefecture of Kumamoto in Japan..

R. Maheswar completed his B.E (ECE) from Madras University in 1999, M.E (Applied Electronics) from Bharathiar University in 2002, and Ph.D. in the field of Wireless Sensor Network from Anna University in 2012. He has about 17 years of teaching experience at various levels and presently working as an associate professor in the School of EEE, VIT Bhopal University, Bhopal. He has published 40 papers at international journals and international conferences. His research interest includes wireless sensor network, IoT, queueing theory, and performance evaluation.

Carlos Alberto Valderrama Sakuyama obtained Ph.D. in Microelectronics at the INPG/TIMA lab in Grenoble, France, as member of the Brazilian government R&D program in 1998. In 1989, he graduated as electric-electronics engineer from the UNC, in Cordoba, Argentina. Since September 2004, he is leading the Electronics and Microelectronics Department of the Polytechnic Faculty of Mons FPMs, in Mons, Belgium. Between 1999 and 2004, he was leading the CoWare NV. Hardware Flow team located in Belgium. He was also invited professor in two Brazilian universities, in 2004 at the Federal University of Pernambuco UFPE and in 1998 at the Federal University of Rio Grande do Norte UFRN.

Sever Pasca is Director of Department of Applied Electronics and Information Engineering, in Faculty of Electronics, Telecommunication and Information Technology, Politehnica University of Bucharest. He is Doctor of Engineering in Electronics and Telecommunications, Medical Informatics. Prof. Dr. Eng. Sever Pasca designed and built 56 systems, programs, devices, and appliances for various contracts, within the framework of research projects in collaboration or for self-endowment. He is main designer of the only Chemiluminometer made in the Eastern Bloc (The Eastern Bloc was the former communist states of Central and Eastern Europe). He has an important contribution in designing, building, and homologation of the prototype and of the fabrication of the complex Stimulator for anesthesia through electro-acupuncture, a device with two brevets.

A Novel Scheme for an IoT-Based Weather Monitoring System Using a Wireless Sensor Network

A. Sampathkumar, S. Murugan, Ahmed A. Elngar, Lalit Garg, R. Kanmani, and A. Christy Jeba Malar

1 Introduction

Following the variety of environmental parameters to decide the nature of our environment is facile. The most often observed parameters include temperature, humidity, precipitation, air pressure, UV index, air quality, and toxins, for example, CO_2, CO, SOx, and unstable natural mixes. One of the prompt advantages brought about by the procurement of such physical decencies, similar to soil dampness, temperature, and saltiness, can be found in agribusiness, where critical water asset reserve funds can be accomplished [1]. The gathered information includes significant subtleties for an assortment of associations and organizations. With monitoring results, governments can take educated decisions regarding the effects of the environment on society and how society influences the environment [22].

Wireless sensor networks (WSNs) are becoming commonplace worldwide because of the improvement of minimal effort and low control wireless innovation.

A. Sampathkumar (✉)
School of Computing Science and Engineering, VIT Bhopal University, Bhopal, India
e-mail: sampath.kumar@vitbhopal.ac.in

S. Murugan
Department of Computer Science and Engineering, Mewar University, Chittorgarh, India

A. A. Elngar
Faculty of Computers & Artificial Intelligence, Beni-Suef University, Beni Suef, Egypt

L. Garg
Department Computer Information Systems, Faculty of Information & Communication Technology, University of Malta, Msida, Malta
e-mail: lalit.garg@um.edu.mt

R. Kanmani · A. C. J. Malar
Department of IT, Sri Krishna College of Technology, Coimbatore, India
e-mail: r.kanmani@skct.edu.in; a.christyjebamalar@skct.edu.in

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3_10

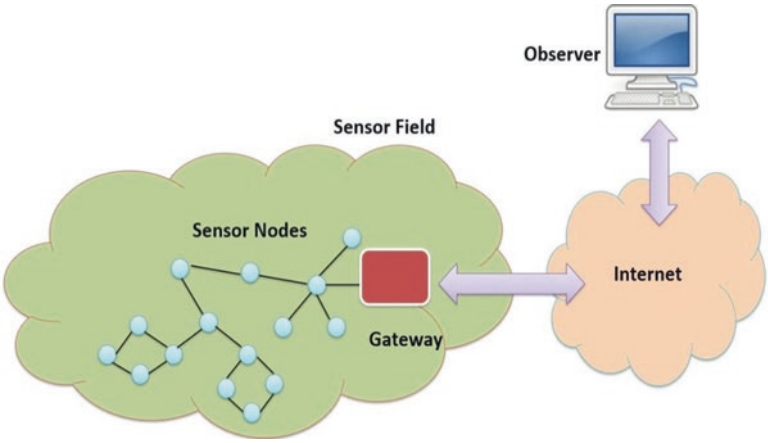


Fig. 1 Wireless sensor network architecture

WSNs are a gathering of spatially deployed detecting hubs with low upkeep necessities that can consequently screen environmental parameters and move information to a primary database by means of a wireless system administrator through a door. There are various applications for WSNs. Most monitoring applications depend on WSNs, which have the undeniably favorable circumstances of lower costs because of link substitution, variable system topologies, versatility, and lower support costs. Wireless sensors and sensor systems have been utilized effectively in arrangements in different fields, including environmental monitoring, catastrophic event anticipation, current utilization monitoring in huge structures, and radiology monitoring frameworks for restorative applications [2] (Fig. 1).

WSNs for IoT environmental observation applications are being attempted. High trustworthiness, insignificant strain, and long maintenance free movement, are a few central functions of WSNs, whereas the nodes often present a variable and crazy climate. The IoT [2] has created changes in the info trade. Wireless sensor networks [3] depend upon pattern setting advancements during which we tend to speak with the surroundings by distinguishing the properties nature. The rule utilization of WSN sensors customarily screens physical or environmental conditions, for example, temperature, weight, and sound, and their information passes through the framework to a vital location [4].

To satisfactorily accumulate and sort the information at IoT finish nodes, a straightforward information exploit structure is basic in most IoT systems. Whole deal mechanical environmental information support uses a WSN [5]. In this chapter, another system for surroundings observation structure subject to development of a WSN is proposed. A WSN is usually depicted as a briefing of nodes that supportively sense and manage the surroundings, sanctioning joint effort between people or PCs and therefore the close surroundings. The current WSNs fuse device nodes, mechanism nodes, entries, and shoppers. Indeterminable device nodes are com-

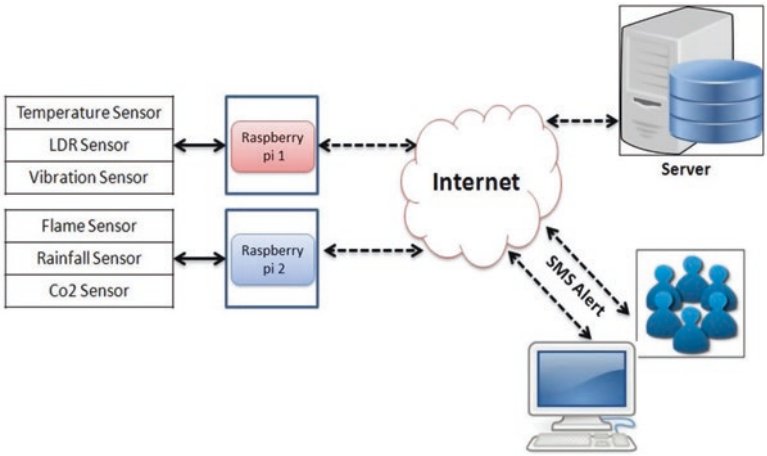


Fig. 2 Overall system architecture of the IoT for environmental monitoring

pleted indiscriminately within or close to the observation zone (sensor field), with the assistance of self-affiliation. The assembled information transmits to different device nodes by skipping through sensor nodes (Fig. 2).

To get to the gateway node after multi-bounce directing, and finally arrive at the administration node through the web or satellite, observed information is passed on by different nodes; this procedure is finished during transmission. The job of the client is to arrange and deal with the WSN with the administration node, distribute monitoring missions and accumulation of the observed information.

2 Related Works

The focal point of this chapter is on radio recurrence (RF) vitality collecting for versatile wireless multiuser multicarrier systems. Specifically, joint information and vitality improvement systems are created to control portable wireless gadgets using RF vitality. For every client, two kinds of collecting capacities are possible: one only gathers from committed RF signals; the other partially recovers from both devoted and environmental RF signals [6].

The authors present a modified plan of an environment monitoring framework for the Internet of Things (IoT) for temperature, humidity, and CO_2. Information is sent from the transmitter node to the beneficiary node in the created framework. The information received at the collector node is observed and recorded through a graphical UI (GUI) in an exceed expectations sheet on a PC made in LabVIEW. An Android application has likewise been created to move information from LabVIEW to a PDA for remote information monitoring [7].

The authors present a paper on the contextual analysis of a shrewd environment dependent on continuous information gathered by the city of Aarhus, Denmark. They examined the air contamination levels so as to distinguish unfortunate or abnormal areas dependent on the Air Quality Index (AQI). An AI system for twofold [20, 21] and multi-class issues, specifically a neural system, neuro-fluffy strategy, and bolster vector machines, has been utilized to identify irregular areas in the contamination database [19]. MATLAB recreation results demonstrate that AI methods are dependable as far as precision and tedious for shrewd environments [8].

This paper proposes an indoor or open air quality monitoring web data framework and a wireless sensor network. Two distinctive brilliant organizer models dependent on a Raspberry Pi, with and without a Jenni inserted PC and wireless system facilitator Ethernet fringe switch, have been actualized [9].

3 Proposed Methodology

The climate conditions in the outside surroundings of a home or any structure are checked and information is transmitted to the cloud server. The advantages are this framework will consequently transmit the ongoing environmental information. The information can be seen from anyplace in the world. This application is to watch and routinely update the environmental conditions, and if they become strange, variations from the norm can be noted in the cloud and vital activity to decrease those anomalies should be possible.

Pseudo code for Proposed Environmental Monitoring System

- Step 1: Start the process
- Step 2: Collect the input data from the sensor nodes attached in the environment
- Step 3: Make sure the data collected from the sensor node is related to temperature, gas, and sound.
- Step 4: Iteration 1: Make a decision whether the data is related to temperature; if yes send the data to the device. If not check whether the data received is related to gas or sound.
- Step 5: Iteration 2: Make a decision whether the data is related to gas; if yes send the data to the device. If not check whether the data received is related to temperature or sound.
- Step 6: Iteration 3: Make a decision whether the data is related to sound; if yes send the data to the device. If not check whether the data received is related to temperature or gas.
- Step7: Gather all the data from the respective nodes and send it to the device to alert the users.
- Step 8: Stop the process (Fig. 3)

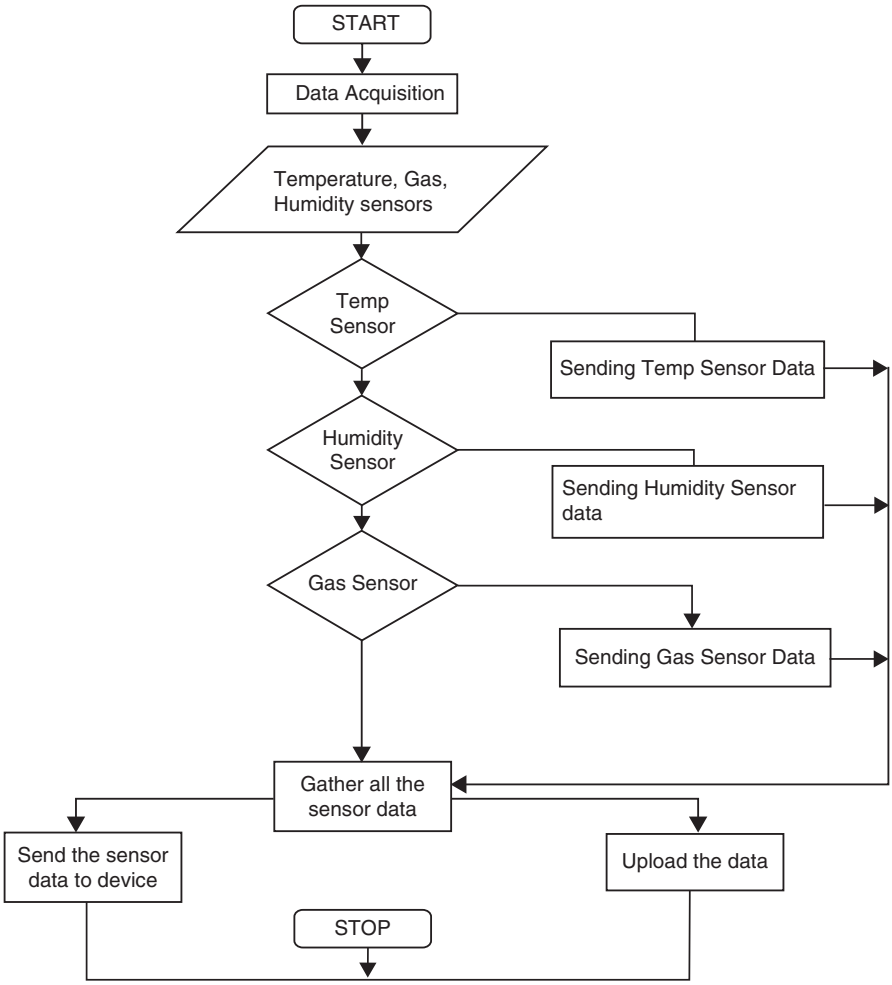


Fig. 3 Flowchart for proposed system

3.1 Environment Monitoring System

Environment tracking condition checking is an IoT application that serves to monitor environmental conditions of any domain and the circumstances can be seen by everyone with the help of the Internet. This software is coherently persuasive and quickly gives the circumstantial conditions [6]. The framework offers a machine the chance to check the circumstance and adjustments happens over the wrapping. This structure makes use of Arduino, sound sensor, gasoline sensor, temperature sensor, humidity sensor, and IoT module [20]. The temperature and saturation sensors screen and give the encounters with respect to the climatic adjustments, and they are

extremely useful to the agribusiness industry. The gas and sound sensors are applied to observe the debasement of circumstances [10]. Using this module, we can find the polluted zone and direct attention toward the humans residing in the sullied area. Changes in the climatic structure cannot always be defined correctly nor is risk always portrayed, but the use of an IoT module can depict gradual differences in a site and they will be processed inside the cloud. There are numerous modules used in this system as discussed later.

3.2 Sensor Module

An IoT board is necessary to fulfill an association of online software essentials with unquestionable high-quality situations that allow the embedded machine maker to efficaciously, quickly, and faultlessly add net machines to their programs [11] (Fig. 4).

The module's UART replacement characteristic and website page control make it ideal for online far off programs, for example, environmental sensors and records from a smaller battery worked with faraway sensor arrange gadgets [12–14].

The proposed coordinated gadget monitors temperature, humidity, weight, radiant power, sound force, and CO level in the air to make the environment canny or intuitive with items utilizing wireless correspondence [15–18]. The proposed model is shown in Fig. 3, which is more qualified to the monitoring of environmental parameters. The proposed architecture is represented in a 4-tier/level model with the functions of each module developed. Level 1 corresponds to the environment, level 2 sensors and sensor data collection, level 3 decision making, and level 4 intelligent environment. Level 2 is designed for sensors with appropriate characteristics. Each of these sensors is operated and controlled within their sensitivity and detection range. Between levels 2 and 3, the actions required for detection and monitoring are performed under conditions such as threshold value determination, detection frequency, and messages (alarm or signal or LED).

The graph in Fig. 5(a) shows the sound intensity levels during day time at regular time intervals. The graph in Fig. 5(b) shows the sound intensity levels at night time. The graph in Fig. 5(c) shows the average sound intensity levels throughout the entire day. The threshold value is dependent on the average value (Fig. 5a–c). The graph in Fig. 5(d) shows the average CO levels throughout the entire day. After completing the analysis on sensed data, the threshold value will be set for necessary controlling actions.

4 Conclusion

Incorporating gadgets into the environment and monitoring them gives self-insurance (smart environment) for the environment. These sensors should be placed in an environment of need to gather information for examination. By actualizing sensors in the

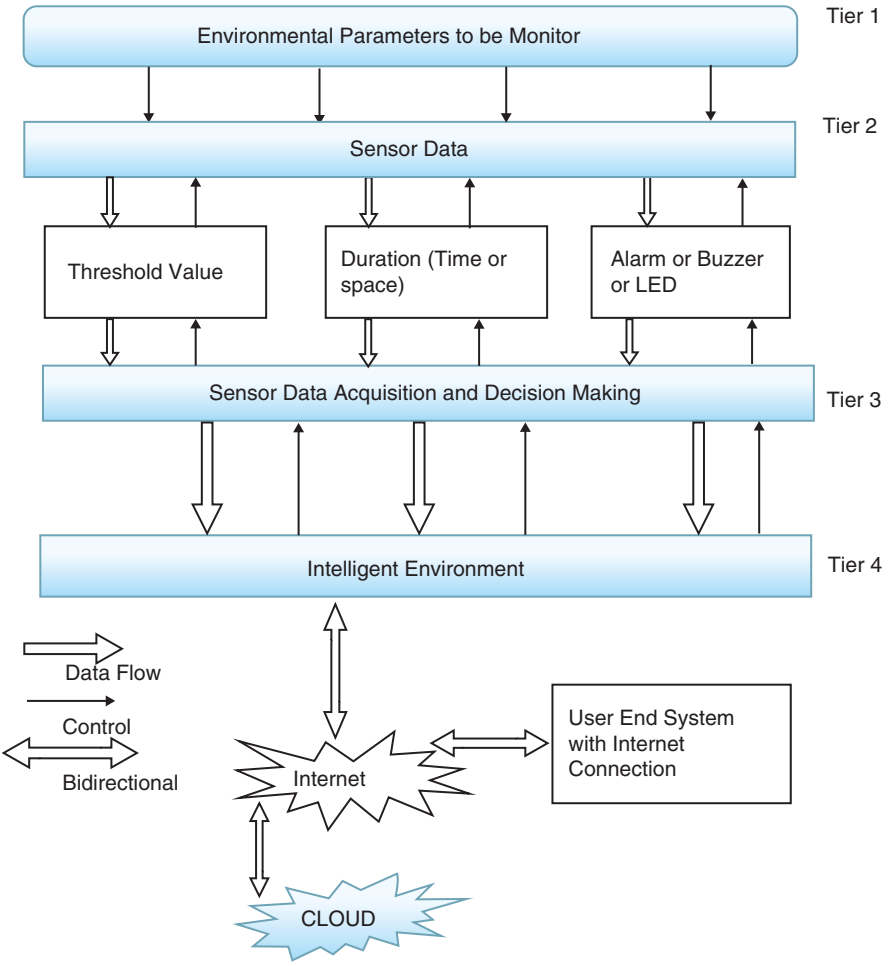


Fig. 4 Proposed system architecture

environment, we can indicate the environment, that is, it can speak with different items through the system. The gathered information and the aftereffects of the examination utilizing Wi-Fi are then accessible to the end client. This chapter presents smart environmental monitoring and an effective and cheap incorporated framework. The proposed design discussed the elements of various modules. Tentatively, the idea of respective sound and air contamination monitoring frameworks with IoT to screen two parameters has been analyzed. After that, sensor settings were sent to the cloud (Google Spread Sheets). This information is helpful for further investigation and can be effectively imparted to opposite end clients. This model can be expanded to screen contamination in urban areas and create mechanical territories. To ensure general wellbeing against contamination, this model offers a successful and modest answer for ceaseless environmental monitoring.

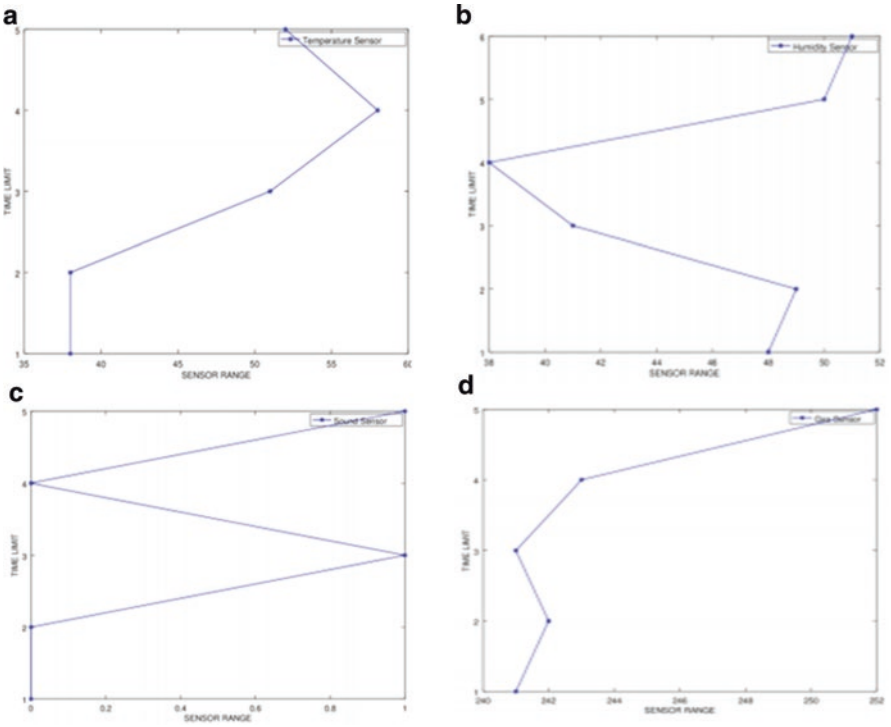


Fig. 5 (**a**) Temperature sensor graph. (**b**) Humidity sensor graph figure. (**c**) Sound sensor graph. (**d**) Gas sensor graph

References

1. Vujović, V., Maksimović, M.: Raspberry Pi as a wireless sensor node: performances and constraints. In: 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, pp. 1013–1018 (2014)
2. Mois, G., Folea, S., Sanislav, T.: Analysis of three IoT-based wireless sensors for environmental monitoring. IEEE Trans. Instrum. Meas. **PP**(99), 1–9 (2017)
3. Nikhade, S.G.: Wireless sensor network system using Raspberry Pi and zigbee for environmental monitoring applications. In: 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Chennai, pp. 376–381 (2015)
4. Shete, R., Agrawal, S.: IoT based urban climate monitoring using Raspberry Pi. In: International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, pp. 2008–2012 (2016)
5. Khalfi, B., Hamdaoui, B., Ben-Ghorbel, M., Guizani, M., Zhang, X., Zorba, N.: Optimizing joint data and power transfer in energy harvesting multiuser wireless networks. IEEE Trans. Veh. Technol. **PP**(99), 1 (2017)

6. Shah, J., Mishra, B.: IoT enabled environmental monitoring system for smart cities. In: International Conference on Internet of Things and Applications (IOTA), Pune, pp. 383–388 (2016)
7. Jain, R., Shah, H.: An anomaly detection in smart cities modeled as wireless sensor network. In: International Conference on Signal and Information Processing (IConSIP), Vishnupuri, pp. 1–5 (2016)
8. Teixeira, A.F., Postolache, O.: Wireless sensor network and web based information system for asthma trigger factors monitoring. In: 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings, Montevideo, pp. 1388–1393 (2014)
9. Mukhopadhyay, S.: Research activities on sensing, instrumentation, and measurement: New Zealand perspective. IEEE Instrum. Meas. Mag. **19**(2), 32–38 (2016)
10. Lazarescu, M.T.: Design of a WSN platform for long-term environmental monitoring for IoT applications. IEEE J. Emerg. Sel. Topics Circuits Syst. **3**(1), 4554 (2013)
11. Ram, K.S.S., Gupta, A.N.P.S.: IoT based data logger system for weather monitoring using wireless sensor networks. Int. J. Eng. Trends Technol. **32**(2), 71–75 (2016)
12. Chen, S., Wang, Y.: Capacity of data collection in arbitrary wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **23**(1), 5260 (2012)
13. Harrow, P., Das, R.: Wireless Sensor Networks 2010–2020. DitchELtd, Cambridge, UK (2010)
14. Romer, K., Matter, F.: The design space of wireless sensor networks. IEEE Wirel. Commun. **11**(6), 54–61 (2004)
15. Hasler, A., Talzi, I., Tschudin, C., Gruber, S.: Wireless sensor networks in permafrost research —Concept, requirements, implementation and challenges. In: Proceedings of 9th International Conference on Permafrost, vol. 1, pp. 669–674 (2008)
16. Beutel, J., Gruber, S., Hasler, A., Lim, R., Meier, A., Plessl, C., Talzi, I., Thiele, L., Tschudin, C., Woehrle, M., Yuecel, M.: Perma DAQ: Ascientific ins trument for precision sensing and data recovery in environmental extremes. In: Information Processing in Sensor and Networks, pp. 265–276 (2009)
17. Yang, J., Li, X.: Design and implementation of low-power wireless sensor networks for environmental monitoring. In: Wireless Communications, Networking and Information Security, pp. 593–597, (2010)
18. Burris, N., von Rickenbach, P., Wattenhofer, R.: Dozer: ultra-low power data gathering in sensor networks. In: Information Processing in Sensor Networks, pp. 450–459 (2007)
19. Sampathkumar, A., Vivekanandan, P.: Gene selection using multiple queen colonies in large scale machine learning. Int. J. Electr. Eng. **9**(6), 97–111 (2018)
20. Ramana, T.V., Pandian, A., Ellammal, C., Jarin, T., Zaki Rashed, A.N., Sampathkumar, A.: Numerical analysis of circularly polarized modes in coreless photonic crystal fiber. Results Phys., Elsevier. **13**, 102140 (2019)
21. Sampathkumar, A., Vivekanandan, P.: Gene selection using PLOA method in microarray data for cancer classification. J. Med. Imaging Health Inform. **9**(6), 1294–1300 (2019)
22. Madhavan, P., Thamizharasi, V., Ranjith Kumar, M.V., Suresh Kumar, A., Jabin, M.A., Sampathkumar, A.: Numerical investigation of temperature dependent water infiltrated D-shaped dual core photonic crystal fiber (D-DC-PCF) for sensing applications. Results Phys., Elsevier. **13**, 102289 (2019)

A. Sampathkumar received his Bachelor in Information Technology, Master in Mainframe Technology, and Ph.D. at Anna University Chennai. He is currently working as an Assistant Professor in the School of Computing Science and Engineering at VIT Bhopal University. He has published several articles in peer-reviewed journals and is a member of CSI societies. His research interests include Artificial Intelligence, Data Mining, Machine Learning, Data Analytic, and Optimization Techniques.

S. Murugan obtained his Bachelor degree from the department of Computer Science and Engineering at Mailam Engineering College, Anna University. Then he obtained his post graduate degree from the Department of Computer Science and Engineering at Hindustan University, Chennai. Currently, he is pursuing his Ph.D at Mewar University, Rajasthan. His specializations include Wireless sensor networks, Network security, Cryptography, Database management systems, and Data mining. He has published papers in SCi Indexed, Scopus Indexed, and other international journals and conferences.

Ahmed A. Elngar is an Assistant Professor of Computer Science at the Faculty of Computers & Artificial Intelligence Beni-Suef University, Egypt, the Founder and Chair of the Scientific Innovation Research Group (SIRG), Director of Technological and Informatics Studies Center Managing, Editor of the Journal of Cybersecurity and Information Management (JCIM). He is a Director of the Technological and Informatics Studies Center (TISC), Faculty of Computers and Information, Beni-Suef University. He is a Managing Editor of the Journal of Cybersecurity and Information Management (JCIM). He has more than 25 scientific research papers published in prestigious international journals and over 5 books covering such diverse topics as data mining, intelligent systems, social networks and smart environment. Research works and publications: He is a collaborative researcher. He is a member of the Egyptian Mathematical Society (EMS) and International Rough Set Society (IRSS). His other research areas include the Internet of Things (IoT), Network Security, Intrusion Detection, Machine Learning, Data Mining, Artificial Intelligence, Big Data, Authentication, Cryptology, Healthcare Systems, Automation Systems. He is an Editor and Reviewer of many international journals around the world. He has won several awards including, the “Young Researcher in Computer Science Engineering”, from Global Outreach Education Summit and Awards 2019 at Delhi, India. He was awarded the “Best Young Researcher Award”, Global Education

and Corporate Leadership Awards (GECL-2018), Plot No-8, Shivaji Park, Alwar, Rajasthan-301,001, India. Also, he has an Intellectual Property Rights called "ElDahshan Authentication Protocol", Information Technology Industry Development Agency (ITIDA), Technical Report, 2016. He has done a great many activities in the community and environmental service, including organizing 12 workshops hosted by a large number of universities in almost all governorates of Egypt. He has done a workshop on Smartphone's techniques and their role in the development of visually impaired skills in various walks of life.

Lalit Garg is a Lecturer in Computer Information Systems at the University of Malta, Malta. He is also an honorary lecturer at the University of Liverpool, UK. He has also worked as a researcher at the Nanyang Technological University, Singapore and at the University of Ulster, UK. He received his first degree in electronics and communication engineering from the Barkatullah University, Bhopal, India, in 1999, and his postgraduate in information technology from the ABV-Indian Institute of Information Technology and Management (IIITM), Gwalior, India, in 2001. He received his PhD from the University of Ulster, Coleraine, UK, in 2010. His research interests are Missing data handling, Machine learning, Data mining, Mathematical and stochastic modeling, and Operational research, and their applications, especially in the healthcare domain. He has published over 80 technical papers in high impact journals, conferences, and books and has more than 550 citation count to his publications.

R. Kanmani received her Bachelor degree in Electronics and Communication Engineering in 2000, Master degree in Communication Systems in 2005, and PhD in Information and Communication Engineering in 2015. She is currently an Associate Professor in the Department of Information Technology in Sri Krishna College of Technology, Coimbatore. Her main research interests include Wireless Network, IoT, and Optical Network.

A. Christy Jeba Malar currently works as an Associate Professor in the Department of Information Technology at Sri Krishna College of Technology, Coimbatore. She received her Master degree from Anna University, Coimbatore in 2009 and her Ph.D in 2019. Her research interests mainly focus on Pervasive Computing and Wireless indoor localization systems.

Index

S. Rani et al. (eds.), *Integration of WSN and IoT for Smart Cities*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-38516-3