Chapter 24
Research Challenges in the Internet of Things (IoTs)

Seema Begum, Yao Nianmin, Syed Bilal Hussain Shah, Inam Ullah Khan, and Satish Anamalamudi

Abstract In the age of the technology and in the field of Computer Networking, devices integrated with the Internet of Things (IoT) resulted in a variety of popular E-Health, E-Commerce and E-Home. The Internet of Things will be next revolutionary term in the today internet. An important function of the IoT is to create various types of technologies, standards and then to integrate them. Today, the capacities of IoT are improving by establishing security for both small and large applications. To help and determine the direction of future research, IoT security challenges and privacy issues will be highlighted in this chapter. The chapter analyzes compares and consolidates the existing research, presents new findings and discusses innovations in the security of the IoT. The challenges in this chapter must be addressed, if the full potential of IoT is to be realized.

S. Begum · Y. Nianmin
School of Computer Science and Technology, Dalian University of Technology, Dalian, P.R. China
e-mail: lucos@dlut.edu.cn

S. B. H. Shah (✉)
School of Information and Communication Engineering, Dalian University of Technology, Dalian, P.R. China
e-mail: bilalshah@mail.dlut.edu.cn

I. U. Khan
Isra University, Islamabad Campus, School of Engineering and Applied Sciences (SEAS), Islamabad, Pakistan

S. Anamalamudi
Faculty of Computer Science and Engineering, SRM University, Chennai, India

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_24

24.1 Introduction

To begin let us define the Internet of Things (IoT). "The Internet of Things (IoT) is the network of physical objects-devices, vehicles, buildings and other items that are embedded with electronics, software, sensors and network connectivity, which enables these objects to collect and exchange data."

The IoT is a new and evolving concept as shown in Fig. 24.6 the investment details that is expected to be widely used in future [1]. The IoT allows the Internet to connect with applications and users by first connecting with objects. The IoT can be implemented in various domains such as retail, agriculture, home, schools and transportation, which can be accessed remotely with the use of the internet. IoT is also able to act without the human involvement in the system. The concept of the IoT is related to the remote sensor networks and remote personal area networks. Communication in IoT is through computing machines and sensors embedded in the systems. The goal of IoT is to provide a good infrastructure based on all things present in the world and also to inform users about the state of things. The evolution of the IoT will be evolving along with communication between machines. This machine-to-machine communication will occur in a variety of domains, such as smart cities, smart homes, smart schools and smart agriculture. Basically, IoT products operate on old fashioned and closed embedded operating system software. Network access needs to be restricted to improve the security terms of the IoT. The segment of the network should monitor for potential traffic and improper activities, then take action if any problem occurs. Many companies have embraced IoT technologies for their potential impact. According to Cisco, there will be 50 billion objects (i.e., devices embedded with technology) connected to the IoT by 2020, as Fig. 24.1 illustrates the world market [1].

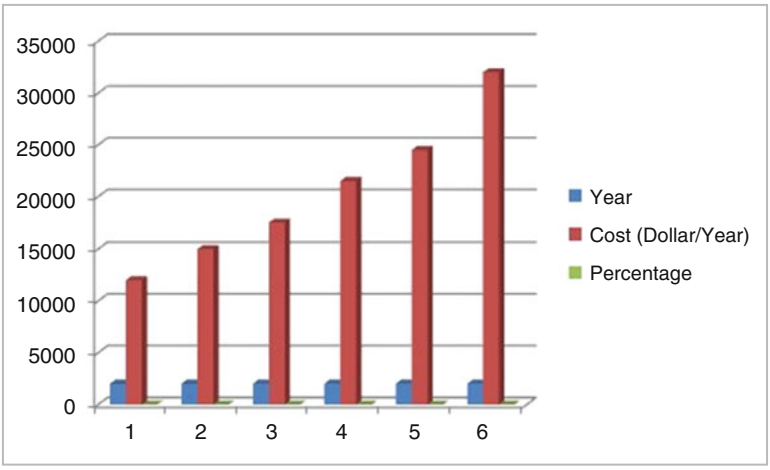

Fig. 24.1 World market for integrated equipment in IoTs

Because of this, privacy has been a hot topic in the research on the different types of technology that enable IoT.

This chapter was written to help internet companies navigate the perils and promises of IoT. We will discuss the unique aspects of the IoT in relation to the informational technology of the internet.

The rest of the chapter describes the resources needed for IoT technology based on the location where it is used. Each section focuses on security and related challenges. The topics discussed include IoT in supermarket Agriculture, schools the home, and traffic management.

24.2 IoT in Super Market

Point of sale (POS) systems are used in the super markets to provide powerful features such as warehouse hosting interfaces, enhanced reporting, file maintenance and inventory control. POS software in supermarkets is used for stock maintenance, expiry, provisioning, reordering wastage and return management. However, these POS systems have some problems including insufficient customization, intensive human resources and inefficient settlement. Currently, many super markets are using IoT technology.

The technology includes radio Frequency Identification (RFID), as shown in Fig. 24.2, smart shopping guides, self-checkout, logistics tracking, wireless and ad-hoc communication with automatic identification, and mobile advertisement [2].

Fig. 24.2 Different designs of RFID cards

24.3 Challenges of Supermarket IoT

At present, manual stock frameworks are used for stocking, and buying items, which are then recorded in a book. Such a system is prone to errors and may lack information needed for proper operations. Data may not be appropriately recorded or managed. From the wholesaler to retailer information on charges, tickets, vouchers, and receipts are recorded in books; however, this system may not facilitate optimal operations. Thus, it is troublesome to prepare, overhaul and manage.

The issues associated with these systems include the following

1. Time consumption
2. Physical counts
3. Supply requests
4. Lack of automatic maintenance
5. Lack of proper management

24.4 IoT in Agriculture

The world of agribusiness is experiencing industrialization, but it is imperative to also to create cooperation within the industry for advancement throughout the world. Rural farmers have been concerned with improvements to advance agrarian community and increase profits.

After many years of hard work positive outcomes have been seen in horticulture framework advancements. These frameworks have the benefits of collecting and tracking rural data. For example, more emphasis has been placed on equipment than programming, without any data to address the production of needs of farmers. Furthermore, available data are not adequately used by ranchers, so the impact of data on horticulture, agriculturists and rural ranches has been minimal.

To change this situation and quickly improve farming conditions; it is important to develop a horticultural cloud data that use IoT and RFID innovations [3].

An environmental control system could incorporate water quality monitoring, programmed water quality, accurate compost treatments, soil quality and moisture monitoring, and environmental condition (e.g., air, light) monitoring. A rural asset control subsystem could incorporate an intelligent nursery that is able to program and maintain a uniform temperature, control a water system that can dispense and converse water, monitor of contamination and vermin, monitor plant and animal health, and ensure the quality product [4–6].

24.5 Different Challenges in IoT

Some of the major difficulties that should be considered when designing an IoT based system including mechanical, social, legal, financial and business issues, with an end goal to get wide acceptance from users. Guidelines and interoperability standards are critical to create markets for new advancements. When gadgets by different manufacturers are not compatible, interoperability is more troublesome, and requires additional efforts to incorporate the different standards. Furthermore, customers may tend to only purchase from a single manufacturer to avoid these comparability issues if user cannot easily exchange information when they replace a gadget with another from a different manufacturer, they will lose any benefits that occurred from aggregating their information for some time. Security allows for effective usage of the IoT with the help of inexpensive devices/gadgets to connect one or many device together. However, these additional layers of programming, middle ware, APIs, machine-to-machine communication results in more complicated setup and new security dangers. Manufactures need to address these issues with strategy driven ways to improve security and provisioning. With such a variety of players required with the IoT, there will undoubtedly be turf wars as legacy organizations attempt to protect their restrictive frameworks and as defenders of open frameworks attempt to create new principles. New models may be developed in light of requirements controlled by gadget class, control prerequisites, abilities and usage. This presents opportunities for stage sellers and open-source promoters to contribute and influence future principles [7].

24.6 IoT in Schools

The fast progression of information and Communication technologies has led to IoT advancement in schools as well [8]. School campus may be composed of many buildings constructed for different purposes. Each block of building has separate systems for air conditioning, heating, ventilation and elevators, among others as shown in Fig. 24.3. To manage these systems, IoT plays a major role in maintain their correct working order. Sensing and control units allow for better maintenance. For example RFID units can monitor the air ventilation by detecting the surrounding climate and environmental changes. If any changes to the ventilation systems are required, then the information can be automatically transmitted to the information-gathering unit that is located in each block, i.e. the wireless central control unit. Depending on the information received, the control unit may increase or decrease the air conditioning Supply [9].

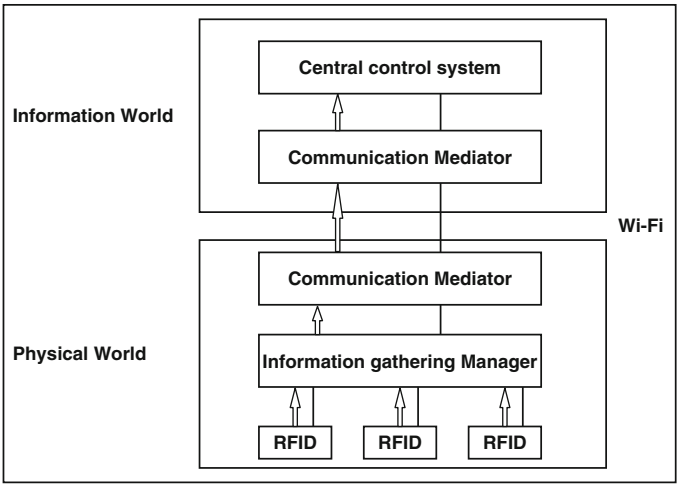

Fig. 24.3 School facilities system

24.6.1 Challenges of School-Based IoT

With the IoT, school can provide instructive results through richer learning experiences and increase access to knowledge for students [10, 11].

An increasing number of students are learning with the assistance of a remote gadget, whether it is a table brought from home or a school-issued laptop. Online lessons can also be arranged to include captivating content. However, these devices may "crash" outdated web systems in schools. To prepare, schools must upgrade to secure and fast remote systems that can handle the data transmission from complex projects being run on a large number of gadgets.

This preparation will pay off in spades. With e-learning applications, students can work at their own pace, which allows the teacher to provide one-on-one instruction to students who most require it. In addition, evaluations can be more consistent, less manual and less time-consuming. Teachers no longer need to review each examination or feed Scranton sheets into a machine. Finally, when associated with the cloud, these e-learning advancements can collect information on student progress, which can be used to enhance lesson plans for subsequent academic years [12].

24.6.1.1 Enhanced Operational Efficiency

Instructive organizations are included many moving parts. So as to prevail at what they do, they should have the capacity to monitor understudies, staff and assets; all while holding costs in line. This is conceivable by utilizing empowering

advancements that can without much of a stretch monitor individuals, resources and exercises. Beforehand tricky assets, for example, projectors or lab gear—can be outfitted with RFID peruses so that their whereabouts are unmistakable at all circumstances. Ongoing deceivability implies instructors no longer need to invest significant energy searching for these things and can rather concentrate on more critical errands like educating and arranging educational module. Furthermore, teachers can screen the state of their assets progressively so that if need be, things can be supplanted with negligible disturbance to the school day. GPS beacons can guarantee that understudies are represented progressively, minimizing tedious exercises like recording participation. With RFID prepared rucksacks, understudies can be consequently checked in as they board the transport. Likewise, the multiplication of brilliant ID cards and wristbands implies understudies can be naturally checked "present" when they stroll through the classroom entryway. With portable registering arrangements, operational barricades can be managed continuously. A support laborer who discovers a broken candy machine can utilize a handheld gadget to advise school authorities of the issue arrange the parts required as well as demand extra repair administrations—while in the field.

24.6.1.2 More Secure Campus Designs

School authorities are under expanded weight to guarantee their grounds are safe. A surge in school crises in the course of the most recent quite a long while, alongside the developing feelings of trepidation over harassing and savagery, mean it's more critical than any time in recent memory to protect understudies. The IoT's capacity to track items, understudies and staff, what's more, to interface gadgets crosswise over campuses brings another level of security to establishments.

A GPS-empowered transport framework implies that transport courses can be followed, so that guardians and chairmen can know where a given transport is at any given time. Notwithstanding making the school travel more secure for understudies (and significantly less unpleasant for guardians), understudies can be advised when the transport is close to their pickup area; not any more sitting tight outside for a late transport. ID cards and wristbands permit instructive associations to store the last-known area of an understudy or guest, making a difference to guarantee the ideal individuals are getting to the correct territories on grounds. They additionally empower cashless installments at the school cafeteria or grounds store, which makes a more streamlined exchange and can possibly demoralize tormenting and burglary. At long last, the meeting of grounds correspondences permits staff to respond all the more rapidly in a crisis circumstance. By associating portable workstations, cell phones and two-way radios, staff can in a split second talk, message or send an email to some other gadget in the system. For instance, a security monitor who spots a battle can tell instructors and chairmen promptly, with one straightforward activity. Presently, can come right away, and an acceleration of brutality can be maintained a strategic distance.

The IoT stands to significantly change the way organizations work, ensuring important resources and improving understudy learning at each level. Notwithstanding the quick advantages plot above, instructive establishments can tackle long haul esteem from these advancements by investigating the subsequent information to better arrangement asset portion, educational module and security methodology in the years to come. Challenges and Open Issues.

24.7 IoT in the Home

IoT applications are available in the market for consumer needs. IoT technology is an emerging innovation for society that will change the ways that consumers interact with other markets, such as energy, health, and transportation.

Implementation of this technology in the home will be described in this section, along with its applications, security, and potential needs of users [13, 14].

The design, installation, and setup of a professional smart home system are available only after smart electronic appliances have been integrated into the home. As such, the IoT at home is likely to be added piece by piece as the need arises. However these systems provide good insights energy savings, reducing the cost of the home improving efficiency. The functioning of this technology in the home can run in the background or foreground. The background activity of the home, can automatically process everyday tasks in a smart energy system. For example, it can adjust heating levels, by of sensing the people present in the home. When more heat is required, the energy consumed by all devices is recorded and calculated for each device separately, with approximate billing cost provided.

Security and safety can be controlled by users' smart phones. The system can also monitor for and alert users about unwanted behavior. Smoke detectors can be remotely monitored for continuous connection: the customer can remotely verify that devices are receiving powered and are turned on. Connected appliances will be operating in the foreground, with their performance increased based on previous usage. The system can provide safety and security for home that is connected with the IoT technology. When integrated into the home, this system can provide a fully automated process to control the home a true smart home as Fig. 24.4 clearly shows [15].

24.7.1 Challenges of Home-Based IoT

IoT manufacturers can demonstrate their commitment to buyers by designing and building trustworthy devices. This technology can create an advantage over other products by increasing the security and safety of users. They can also create an effective process and provide a positive customer experience that meets users' needs.

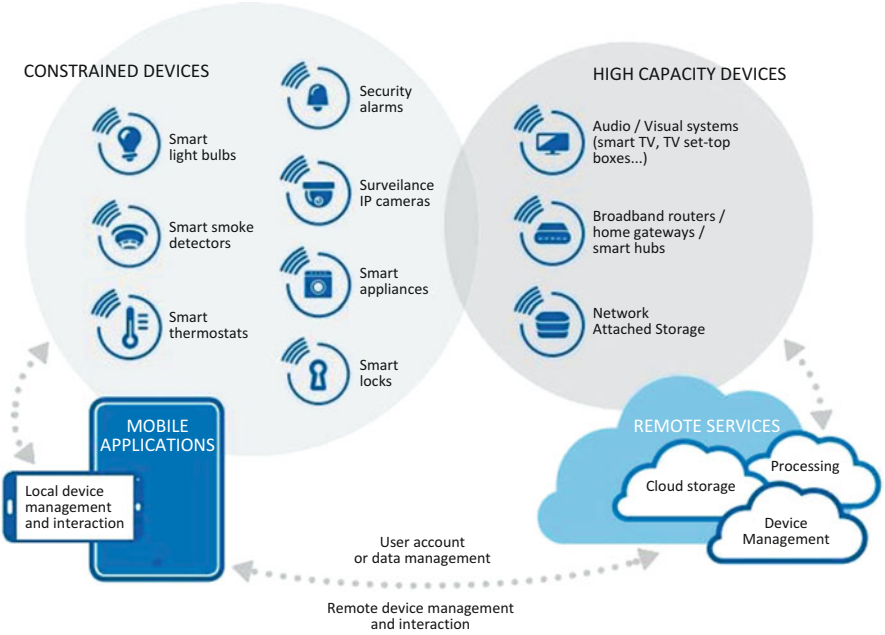

Fig. 24.4 Smart home system

24.8 IoT in Traffic Management Systems

The IoT plays a major role in intelligent traffic information systems by predicting traffic flow conditions, current traffic operations and future traffic flows. This traffic system allows drivers to find optimal routes to reduce their travel time. IoT technology provides additional benefits for an intelligent traffic system, such as high reliability, improved traffic conditions, information weather conditions, between traffic safety, reduced traffic management costs and less traffic jam. An IoT based traffic management system can be intelligent to collect of all traffic related information to support the processing and analysis of traffic information. Such a traffic system uses a number of different devices, including a global positioning system, infrared sensors, laser sensors and RFID sensors [16–32].

An intelligent traffic management system using the IoT consists of three layers: As shown in Fig. 24.5.

- Application layer
- Network layer
- Acquisition layer

Application Layer	Intelligent Traffic Management	Intelligent Driver Management	Information Collection & Monitoring	Information Services
Network Layer	Internet	WiFi, 3G/4G	WiMax	GPS, GPRS
Acquisition Layer	RFID	RFID Reader	WSN	Intelligent Terminals

Fig. 24.5 The framework of the intelligent traffic management system

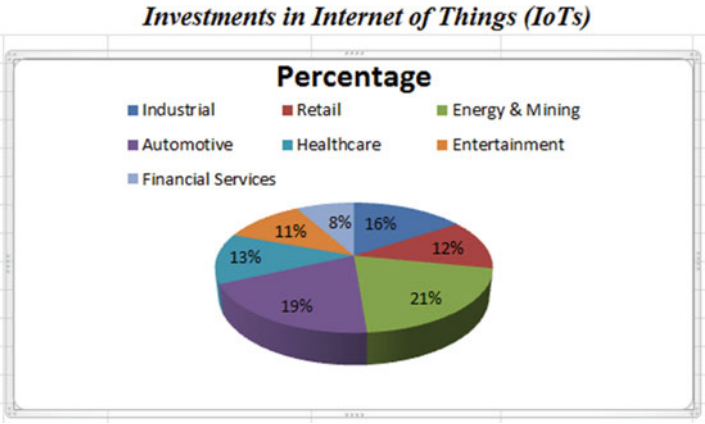

Fig. 24.6 Companies wants to invest in IoTs

24.8.1 Challenges of IoT-Based Traffic Management Systems

Due to the mobility of devices, radio frequency link variability and intermittent connectivity, the mobile devices on the IoTs may have difficulty connecting other devices on a network. For example, internet-connected cars are required to receive and send data at different locations of gateway sensor nodes. The cars need to keep the information while changing locations. To do this, IoT network paradigms should incorporate concepts from delay-tolerant networks and mobile ad-hoc networks [8, 16] (Fig. 24.6).

24.9 Conclusion

This paper has discussed IoT emerging technology in a variety of locations, where people work and study. The benefits of these technologies were summarized. When implemented correctly, they will efficiently and effectively improve the lifestyles of

the user and provide benefits for society as whole. The chapter also described the security issues and challenges associated with applications integrated in IoT. Smart technology based on the IoT has great potential. By ensuring the integration of safety and security features, manufacturer can increase the confidence of consumer while advancing society.

References

1. Archive.org. (2016). *Full text of "International Journal of Science and Research (IJSR)"*. [online] Retrieved December 26, 2016, from https://archive.org/stream/MTMwOTEzMDI/MTIwMTMzNg==_djvu.txt
2. Dlodlo, N., & Kalezhi, J. (2015). *The Internet of Things in agriculture for sustainable rural development*. [online] Retrieved December 26, 2016, from https://www.researchgate.net/publication/277713549
3. Garg, G., Goyal, D., Aggarwal, H., Baindail, K., & Verma, G. (2016). Controlling home appliances in IOT environment. *International Journal of Smart Home, 10*(8), 11–18.
4. Hongyan, L. (2015). Design and realization of smart home terminal applications based on IOT technology. *International Journal of Smart Home, 9*(8), 123–132.
5. http://citeseerx.ist.psu.edu/. (2016). *Intelligent traffic information system based on integration of Internet of Things and agent technology*. [online] Retrieved December 26, 2016, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.2856&rep=rep1&type=pdf
6. https://www.uio.no. (2016). *RFID and IOT: An overview*. [online] Retrieved December 26, 2016, from https://www.uio.no/studier/emner/matnat/ifi/INF5910CPS/h10/undervisningsmateriale/RFID-IoT.pdf
7. Iot.ieee.org. (2016). *Research challenges in the internet of mobile things - IEEE Internet of Things*. [online] Retrieved December 26, 2016, from http://iot.ieee.org/newsletter/march-2016/research-challenges-in-the-internet-of-mobile-things.html
8. Jain, D., & Krishna, P. (n.d.). *A study on Internet of Things based applications*. [online] Retrieved December 26, 2016, from https://arxiv.org/ftp/arxiv/papers/1206/1206.3891.pdf
9. Journal, R. (2016). *What would be the best way for a local supermarket to transition to RFID technology?*. [online] Rfidjournal.com. Retrieved December 26, 2016, from http://www.rfidjournal.com/blogs/experts/entry?11504
10. Kim, W. (2016). The business model of IoT information sharing open market for promoting IoT service. *Journal of the Korea Society of IT Services, 15*(3), 195–209.
11. Lin, H., & Bergmann, N. (2016). IoT privacy and security challenges for smart home environments. *Information, 7*(3), 44.
12. Mehta, A., & Patel, S. (2016). IoT based smart agriculture research opportunities and challenges. *International Journal for Technological Research in Engineering ISSN (Online), 4*(3), 2347–4718. [online] Retrieved December 26, 2016, from http://www.ijtre.com/images/scripts/2016040325.pdf.
13. Rahul, G., & Patel, S. (2016). *A review of smart shopping systems*. [online] https://www.irjet.net. Retrieved December 26, 2016, from https://www.irjet.net/archives/V3/i5/IRJET-V3I5441.pdf
14. Shiryaev. (2016). *RFID technology and Internet of Things*. [online] Slideshare.net. Retrieved December 26, 2016, from http://www.slideshare.net/rushtek/rfid-and-internet-of-things
15. Vujovic, V., & Maksimovic, M. (2015). *The impact of the 'Internet of Things' on engineering education*. University of East Sarajevo Lukavica, Bosnia and Herzegovina. [online] Retrieved December 26, 2016, from http://www.citethisforme.com/cite/journal
16. Alam, M., Trapps, P., Mumtaz, S., & Rodriguez, J. (2016). Context-aware cooperative testbed for energy analysis in beyond 4G networks. *Telecommunication Systems*. https://doi.org/10.1007/s11235-016-0171-5

17. Khan, F., Rahman, F., Khan, S., & Kamal, S. A. (2018). Performance analysis of transport protocols for multimedia traffic over mobile Wi-Max network under Nakagami fading. In *Information technology-New generations* (pp. 101–110). Cham: Springer.
18. Alam, M., Albano, M., Radwan, A., & Rodriguez, J. (2013). CANDi: Context-aware node discovery for short-range cooperation. *Transactions on Emerging Telecommunications Technologies, 26*(5), 861–875. https://doi.org/10.1002/ett.2763
19. Khan, F., & Nakagawa, K. (2013). Comparative study of spectrum sensing techniques in cognitive radio networks. In *2013 World Congress on Computer and Information Technology (WCCIT)* (pp. 1–8). IEEE.
20. Zebra Technology. (n.d.). *How the Internet of Things is transforming education*. [online] Retrieved December 26, 2016, from https://www.zebra.com/ap/en.html
21. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2014). PASCCC: Priority-based application-specific congestion control clustering protocol. *Computer Networks, 74*, 92–102.
22. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2015, August). A Sybil attack detection scheme for a centralized clustering-based hierarchical network. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 318–325). IEEE.
23. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)* (pp. 1–6). IEEE.
24. Jan, M. A., Nanda, P., He, X., Tan, Z., & Liu, R. P. (2014, September). A robust authentication scheme for observing resources in the internet of things environment. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 205–211). IEEE.
25. Jan, M., Nanda, P., Usman, M., & He, X. (2017). PAWN: A payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience, 29*(17).
26. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2013, November). Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network. In *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC)* (pp. 1400–1407). IEEE.
27. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2018). A Sybil attack detection scheme for a forest wildfire monitoring application. *Future Generation Computer Systems, 80*, 613–626.
28. Jan, M. A., Nanda, P., & He, X. (2013, June). Energy evaluation model for an improved centralized clustering hierarchical algorithm in WSN. In *International Conference on Wired/Wireless Internet Communication* (pp. 154–167). Berlin, Heidelberg: Springer.
29. Usman, M., Jan, M. A., & He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. *Information Sciences, 387*, 90–102.
30. Usman, M., Jan, M. A., He, X., & Nanda, P. (2016, August). Data sharing in secure multimedia wireless sensor networks. In *2016 IEEE Trustcom/BigDataSE/ISPA* (pp. 590–597). IEEE.
31. Jan, M. A., Usman, M., He, X., & Rehman, A. U. (2018). SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2848284
32. Jan, M. A., Jan, S. R., Usman, M., & Alam, M. (2018). State-of-the-art congestion control protocols in WSN: A survey. *IoT EAI*. https://doi.org/10.4108/eai.26-3-2018.154379