Wireless Personal Communications (2020) 113:747–771
https://doi.org/10.1007/s11277-020-07251-z

Cloud Integrated IoT Enabled Sensor Network Security: Research Issues and Solutions

R. Geetha[1] · A. K. Suntheya[1] · G. Umarani Srikanth[2]

Published online: 4 April 2020

Abstract
Security of cloud computing and Internet of things (IoT) enabled sensor networks are two significant areas of research that have a great impact in developing numerous societal applications such as smart healthcare, smart city, smart agriculture etc. in a secure manner. The devices involved in these technologies are exposed to vulnerabilities since they are distributed in nature and moreover they try to fetch real-time information and forward it to cloud for processing. Cloud computing offers a platform for storing and processing the data sensed and sent by the sensor devices. In the previous literature, many researchers have studied the security issues and challenges of IoT and Cloud separately. Still, there is a gap in the literature and it is required to explore the integrated security issues in the Cloud integrated IoT environment. Analyzing the integrated security issues of the existing technologies is of much importance and novel idea for their successful implementation. In this paper we focused on exploring the vulnerabilities of the integrated environment. In addition, we had presented the security issues and challenges in the cloud and IoT enabled sensor environment.

Keywords Internet of things (IoT) · Cloud computing · Sensor network · Security

1 Introduction

In telecommunication field Internet of Things (IoT) [1] is considered to be one of the growing technologies where the network enabled devices access upon the pervasive environment in a ubiquitous manner. This technology mainly consists of various set of things, objects, vehicles, and sensors for transferring the information from one or other devices in the network [2]. Thus it is very beneficial for communication purpose over the environment as machine to machine, machine to human, human to human communication. The data is transferred consistently among the users. IoT is mainly considered to be the set of networks consisting of physical objects or things embedded with electronics, software, sensors and

✉ R. Geetha
geetha@saec.ac.in

[1] Department of Computer Science and Engineering, S.A. Engineering College, Chennai, India

[2] Department of Computer Science, St. Peters College of Engineering and Technology, Chennai, India

network connectivity which enables these object to collect and transmit the data accordingly. This is also referred as Internet of Everything (IoE) [3], since it process upon the network enabled devices in order to collect and transmit the data by using processors, sensors and hardware which are used for communicating purposes. It is also known for its unique process and also referred as "smart devices" where devices will communicate and transfer data for processing [4]. When the communication takes place between the machine to machine it is also called as Machine to Machine communication (M2M) [5].

The stages of IoT involves (a) Collecting data for processing (can be accessed upon everywhere such as office, house, etc.). (b) Transfer data for communication process (can be home based network, data center, desired platform) (c) analyze data for processing (d) implement data according to required information (will be sent through m2m, sms, email, text, m2m communication). The problems being faced by IoT are Exploitation of IoT devices, infiltration of data, information fusion, occurrence of errors—space and time complexity, inefficient infrastructure and inefficient data collection.

Wireless Sensor Network (WSN) [6] is considered to be most prominent technology in the current world. It can be defined as a set of embedded devices which is used for communication purpose by gathering required information from the set of monitored field through wireless links [7]. It consists of spatially dispersed clusters with required sensors for checking consistency, monitoring and recording the conditions such as temperature, sound, wind etc. of the surroundings. The nodes are interconnected through set of gateway nodes with the wireless Ethernet. The main advantage of WSN is the replacement of wired technologies [5]. It mainly communicates with the environment through wireless manner. With the help of this technology we can overcome the wired environment issues and can enable the network to process in a decentralized manner [5].

The various set of topologies for communicating purpose are [8]: (a) star topology where all nodes in the network are connected through a gateway, here every node cannot send and receive messages to each other (b) mesh topology where within radio transmission range the nodes can able to communicate with each other (c) tree topology in which nodes are connected in a hierarchical manner, placed higher manner and those nodes connected through a gateway. The various types of sensor networks are as follows [9]: (a) terrestrial WSNs that helps these nodes to communicate with the base station effectively among hundreds and thousands of nodes in a structured or unstructured manner (b) underground WSNs that help the nodes to communicate in underground level for communication purpose but it is difficult to recharge. It also leads to larger issue since attenuation and loss of signal (c) underwater WSNs that mainly consists of limited set of power and cannot be recharged or replaced (d) multimedia WSNs that used for monitoring and tracking the events in the form multimedia such as image, video or audio (e) mobile WSNs where nodes communicate in a mobile manner and can be interacted with physical environment effectively.

The challenges faced by sensor networks are unauthorized intruders, reduction in loyalty of data center, low power consumption, storage area, dynamic nature of network, corruption of data, less efficiency, larger consumption of energy, retransmission of data packets, less secure over sensor nodes, inaccurate prediction, potential security issues, challenges over IPv6 in wireless personal area network, two way communication between wireless and active sensor, no prior knowledge about assets, undesired emails, zero day attacks, non-traceable source of the issue, forensic challenges, operational challenges and technical issues.

Cloud computing technology is considered to be one of the fast developing technologies; it can be accessed through a set of data with the help of hardware and software at anywhere and anytime in the environment. Thus data in the environment is stored in an abundant manner and can be processed whenever it is required [5, 10]. It is the process of using both software and hardware requirements in order to provide the services over the network. With the help of this technology we can access the files and use applications in the presence of a pervasive environment. Thus the method of using the network of remote servers hosted on the internet to store, manage and process data other than a local server or personal computer. The cloud computing technologies mainly make use of the following cloud deployment models [11].

The models that come under the cloud deployment category [12] are: (a) *Public cloud* which can be processed according to pay per user basis. It is mainly owned by the Cloud Service Providers (CSP) and is obtainable through a subscription (b) *Private cloud* that provides a flexible environment for the local users and results in delivering more efficient and convenient cloud services (c) *Hybrid cloud that is* made of with both private and public clouds. The hybrid cloud is majorly accessed for using the big data operations such as non-sensitive data that is kept in public cloud whereas sensitive data that is kept in private cloud environment (d) *Community cloud* which is the recent variation of private cloud model for business communities. The business related information is shared by the service providers for the software and development tools which are required to meet the community needs.

Cloud computing technology has various cloud based services [11, 13] like (a) *Infrastructure as a Service (IaaS)* that is used for accessing the process of storage, computing and networking with the help of virtualized IT resources. The services over this model are based upon the rented cloud infrastructure according to their chosen OS environment (b) *Software as a Service (SaaS)* that is used for accessing software applications as a service over cloud environment by providing lower cost by the provider side and no initial investment on customer side for servers or software license (c) *Platform as a Service (PaaS)* that is used for the process of developing, deploying and managing the execution of applications in a cloud platform with a proper software environment. It mainly consists of an operating system and a library support [14]. Nowadays the applications that are based on cloud depends on the time-critical processing of data or throughput of the network. These applications requires the ability to reconfigure the given infrastructure on demand as well as whenever there is a change in condition [15]. Cloud based time-critical applications such as early warning systems have constraints on the quality of service that affects the proper delivery of data on time [16].

With IoT enabled sensors in WSN and cloud computing, the process of integrating IoT smart devices with set of cloud technologies it is considered to be Claudio (or) [17] Cloud of Things [18]. It is also known as IoT Cloud computing for the purpose of computing in this environment [19]. Access upon the various business resources over cloud environment for better accessing is possible in this hybrid environment. Since the process of accessing data take place in a smart environment and devices will communicate in a peer-to-peer manner, data can be stored and accessed whenever it is required [11, 20]. This hybrid technology is related with several security issues since it is used in various set of applications such as smart city, health monitoring, smart agriculture, smart home, wearable, connected cars and even more. Fog or edge computing with mobility aware framework using IoT Systems based on cloud is gaining popularity in the recent research field. These sorts of real-time frameworks make use of different layers for IoT, Edge, Fog and Cloud [21].

Smart Cities Example applications like the street light can be automatically turned on whenever the user is in need of it, otherwise it can be turned off. In case of smart parking, vehicles can be located through web and help the users to park vehicles in the available area [22, 23]. *Smart Home* In case of smart home sensor devices sense automatically to open the doors, alert in case of non-availability of stocks in refrigerator, turning of light whenever it is not required, preheat the showers when it is required [24, 25]. *Wearable* It is mainly used to access data in the environment with set of wearable devices such as chip, smart watches, dashbon masks etc. With the help of smart watches, users can be tracked out; with dashbon mask the users can listen, play and watch entire movie and TV collection over the internet [26]. *Health Monitoring* In case of emergency, it will alert the neighborhood by calling ambulance, patients can be treated in nearby hospitals and report their families in the emergency period automatically. It also monitors patient's record through wireless manner over the internet [27]. Figure 1 shows various applications based on Cloud integrated IoT enabled sensors.

As the technology evolves day by day, we need to provide a well secured environment for data and it is inevitable to notice that larger number of attackers arise to access vital information. Thus it is proposed to investigate various types of attacks in IoT enabled cloud computing environment and preventive measures for securing our data in the cloud surroundings.

The rest of the paper is organized as follows. Section 2 presents various levels of security in cloud architecture and related attacks. Section 3 discusses security of integrated environment of IoT enabled WSN infrastructure in different layers with its related attacks. Section 4 presents detailed related research work of Cloud Security and IoT enabled WSN Security along with research issues and solutions followed by the comparative analysis. Finally conclusion of the security of integrated environment review is presented.

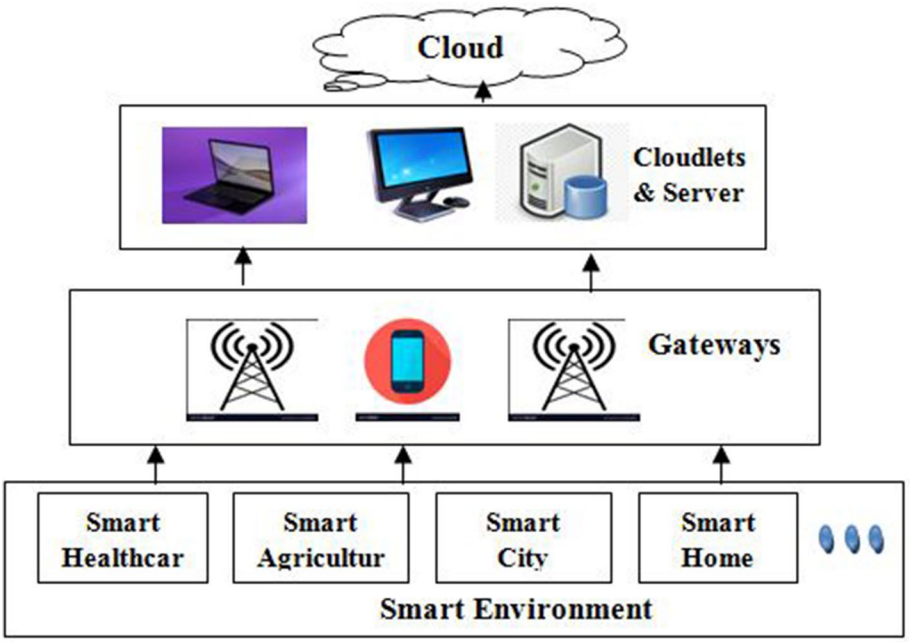

Fig. 1 Applications based on cloud integrated IoT enabled sensors

2 Cloud Infrastructure Security

Cloud computing environment implements the following security services at infrastructure level basis. The security services at various levels are as follows [28]:

2.1 Network Level Security

It provides confidentiality and integrity over data among the organizations for transmitting and receiving information from public cloud provider ensures services with proper access control (authentication, authorization, and auditing) for resources available in the cloud environment and replaces the established network zones and tiers with domains.

2.2 Host Level Security

It provides host security services over PaaS and SaaS level and these services hide the host operating system from end users. The responsibilities of host level security at SaaS and PaaS are transferred to CSP which ensures virtualization software security that includes hypervisor security, threats: Blue pill attack on the hypervisor, Customer guest OS or virtual server security: attacks to the guest OS such as stealing keys used to access and manage the host based services.

2.3 Application Level Security

It is responsible for both CSP and customer. The application level security includes security at the cloud services level basis as follows: *IaaS level security* keeps the customer applications in a well secured manner, not responsible for application level security. *PaaS level security* provides a safer environment over the platform and customer related applications on the PaaS platform. *SaaS level security* accesses the information in a well secured manner between service provider and customer.

Though cloud computing process a larger database, it leads to several issues in accessing and results in number of threats in this domain [29]. These are the following threats in cloud environment as shown in Fig. 2.

2.4 Denial of Service (DoS)

Denial of Service (DoS) is a significant attack in cloud environment, in which attackers cannot access the services of authorized users. The attackers send larger number of messages to access the authentication request with the invalid return address. The DoS attacks lead to the problems like ineffective services in the network, non-accessibility of services and disturbance of network traffic and connection interference.

In *malware injection attack* the attackers place incorrect codes or services which results like services are placed priory in the network. This attack is also known as “driven by downloading” or “meta data spoofing”. The intruders provide an illusion environment to make the users to download software or opening up the spam mails and steal information from the system. Malware injection attacks leads to problems like

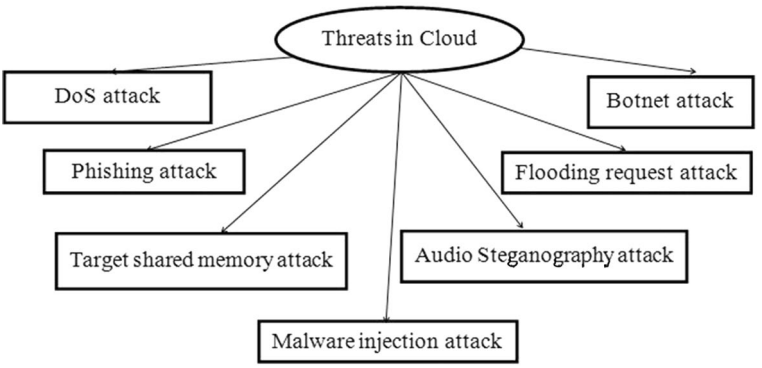

Fig. 2 Threats in cloud environment

users downloading malicious software, creating an illusion environment to make users to believe, minimizing access by the user and implementing the malicious activity in cloud and gain access on the targeted services.

Target shared memory attacks provide advantage of memory sharing, the combination of both physical and virtual memory. This attack leads to side channeling and malware injection attack. The attackers gain unauthorized access to database such as retrieving the total number of running process, count of users who were logged in the specific system. The problems faced by target shared memory attacks are malware injection, side channel attack and attackers gaining access upon the services.

Phishing attack leads to the issue of retrieving personal information of the user by sending unwanted emails, webpage links and false messages repeatedly. This attack creates real working environment as it comes from authenticated person by providing false access location. Phishing attacks leads to problems like accessing sensitive information of the user and results in longer recovery time from the attack.

Botnet attack process distributed DoS attacks, steals their personal information and makes the intruders to gain access to the system and their connection. The master can able to control the botnet by using the command and control software in the system. The attackers who control over the botnets are known as "bot masters".

In *audio stenography attacks* the users store their confidential messages in audio format and send their secret messages through audio files and the attackers make use of this method to access the authorized files.

Data stealing attack is the process of accessing the confidential information in unauthorized manner from the unknown targeted system. The possible ways of data stealing methods are used in applications like e-commerce, password cracking, eavesdropping and laptop theft.

Flooding request attack is one of the types of DoS attacks, used to service down with larger amount of traffic. This attack occurs when service of the network weighed down with the packets initiated with incomplete connection requests.

3 IoT Enabled WSN Infrastructure Security

WSNs attack leads to several kinds of threats. It is further divided into three types of attacks based upon [30–32] attackers capability (outsider attacks vs insider attacks, passive attacks vs active attacks, moteclass vs Laptop class), information in transit (software compromise, network based attacks) and protocol stack (physical layer, data link layer, network layer, transport layer, application layer). Figure 3 shows the types of attacks in IoT enabled sensor network.

Physical layer faces attacks such as *jamming* that cause the communication channel busy by protecting other nodes involving in communication and *radio interference* where the interference is produced in large in amount.

Data link layer leads to the attacks like *continuous channel access* where the media access control is continuously disturbed with the malicious node by transmitting and receiving over the channel and *collision* where when two nodes attempt to access upon the same frequency range.

Network layer faces attacks such as *sinkhole attack* with fake routing update where the compromised node will attack network traffic, *hello flood attack* with the periodic disturbance of network security by the malicious nodes sending the hello packets with more signal strength and *man in the middle attack* where the third party interrupts the system and generate false information.

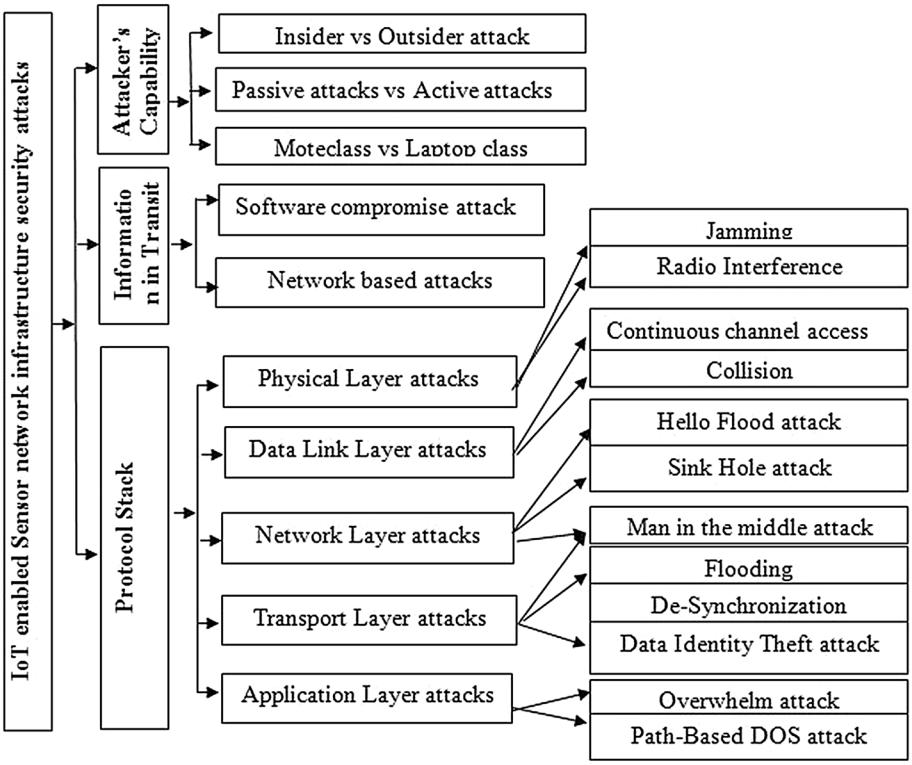

Fig. 3 Types of attacks in IoT enabled sensor network

Transport layer leads to attacks such as *flooding* where the desired node cannot be accessed in time due to multiple connection requests by the attackers, *De-Synchronization* where the intruder continuously sends the false messages to both endpoints in getting the essential data and nodes requests for the missed frames and *data identity theft* which involves accessing upon someone's personal information such as credit card number, name, etc.

Application layer faces attacks like *overwhelm attack* where the base station receives large number of traffic due to overwhelm network node with sensor stimuli and *path-based DOS attack* where the leaf nodes inject the replayed set of packets that create starvation of network with large number of traffic.

4 Related Research Review

4.1 Cloud Security Issues and Solutions

Liu et al. [33] have discussed the problem with well-known features of attacks in physical sensor node and virtual sensor node. The significant issue is that cloud computing environment is prone to various attacks. The key challenge was to accomplish the lower storage for the virtual sensor service nodes and to maintain energy consistency over the physical sensor node. Sensor cloud is prone to attacks through the characteristics of both physical and virtual sensor nodes by periodic occurrence and reduction of false alarms. To overcome this problem the authors had suggested a game theoretic approach, which was used for accessing variety of decision making strategies. Thus the intrusion detection system installed over both physical and virtual sensor nodes can able to make decisions on their own and send the alarms to the gateway nodes. It also reduced the burden of managing the intrusion detection system and energy consistency thus resulting in generating the evolutionary stable strategy.

Sahi et al. [34] have discussed about the effects of Distributed DoS (DDoS) TCP flood attacks and provided an idea to overcome those attacks through a newer method known as Classifier System (CS_DDoS) system. DDoS TCP attacks are very much difficult to identify the authenticated users since the attackers send the packets from the undesired users and make the server too busy for a longer time. Thus it increases bandwidth usage and majorly this attacks lead to the financial losses. The CS_DDoS approach is one of the classification models and used to identify the desired attacks from where they are generating in the network. The classification was done with the basic process such as distinguishing, classifying and differentiating the larger number of multiple objects. The classification includes the Least Square Support Vector Machine (LS-SVM), Naive Bayes, K-nearest and multilayer perception. In turn it is used to identify the packets source within a time frame, in order to identify that the packets that have been generated from the desired nodes.

Cheng et al. [35] have discussed that cloud computing environment is not secure by using the traditional privacy process, due to the openness and abundant storage of the data in the network. They had implemented accountable privacy preserving mechanism based upon the issues such as data integrity problem, data protection problem, lock-in problem and governance problem. Since cloud environment is used to store larger volume of data it is well known prone to attacks in this domain and also possess good data center for accessing various sources of data in the network. These are the reasons why the cloud environment is more vulnerable to attacks. Accountable privacy preserving mechanism is

significantly used for concentrating the illegal behavior of network in order to secure the participants in the cloud environment and also to overcome the description logic for defining the privacy concepts. The authors provided the desired results and potential accountability implementation.

Anglano et al. [36] discussed about the security concern in the data outsourced cloud environment. There are many malicious entities that affect the cloud environment, but they considered about the pollution related attacks and their preventive measures. The malicious entities attempt to overwrite the stored data which affect the security in the cloud environment. Thus the pollution attacks lead to most dangerous issue over the data integrity problem which was subdivided into separate parts and then encoded to process with the fragmented codes, in this case two problems arises: (a) sequence of bits are valid coded fragments (b) it is not very easy to understand which coded fragments received by the users are polluted. Thus with the help of the rate less codes the authors were able to create an early pollution detection algorithm, in order to identify an intruder when fetching the data from the cloud storage. The alarm trigger procedure was used to locate the polluting nodes with the help of proposed system algorithm and also locates the intruders to permanently remove them from the system. Thus the authors provided an analytical model to identify the overall attackers in the cloud storage and desired levels of robustness were achieved during the realistic storage of disk.

Li et al. [37] have discussed about the attribute –based encryption method which is used to solve the security threat in the cloud environment. It reduced the threats using the cryptographic primitive known as Attribute based encryption scheme with outsourcing key issuing and outsourcing decryption that in return access the Keyword Search Function (KSF-OABE).The significant problem here is that it deals with openness and access of larger number of users in cloud environment which states the data in cloud to be less protective with great computational cost. They have implemented Keyword search function using (KSF-OABE) which can partially decrypt the cipher text without the knowledge of plain text with the help of Cloud Service Provider. This method mainly consists of two schemes ABE namely KP-ABE: Key-Policy ABE and CP-ABE: Cipher text policy. It is very simple approach since it downloads only the partial decryption of the cipher text according to the desired keyword. Thus it results in lesser time consumption and also computational cost is compatible between both the trusted authorities and users.

Al Hamid et al. [38] have discussed about severe security threats over the healthcare data in cloud environment and have implemented a security protection of data in cloud environment with the help of fog computing technology. The major issue faced in this environment was security breaches due to following criteria namely larger storage, lack of transparency and cyber security. They provided solution for multimedia data over the cloud environment using the Fog computing technology by providing two photo galleries such as DMBD and OMBD. The OMBD was placed secretly over the environment, was accessed only upon the authorized users and DMBD acted like a honeypot. Thus data in the medical database was placed very much protective over the environment.

Win et al. [39] have discussed about the virtualized infrastructure which provides a way for cyber attackers to launch new attacks in the cloud environment. The author proposed a Big-Data based Security Analytics (BDSA) process to discover the forth coming attacks priorly. The significant drawback in this virtualized infrastructure is based upon the mandatory issues in the cloud environment such as Scalability and Virtualized infrastructure. Thus the identification of malware detection can be done by the following steps: Monitoring the hooks and Signature based attacks updation. This paper provided a solution by implementing the BDSA approach in the following consecutive process (a) guest VM's

network logs and the user application is mainly collected and stored in the HDFS periodically. (b) Machine learning is mainly used to identify the presence of attack. (c) Logistic regression is mainly used for calculating the conditional probabilities of attacks with respect to the individual attributes. The features of attacks are extracted by the correlation graph and Map reduce phrase. Thus BDSA approach provides an advantage of distributed HDFS and real time access to Map Reduce.

Yan et al. [40] have discussed about DDoS attacks in the cloud environment. This was identified using the advancement in the technology related in cloud computing and those attacks can be overcome through the Software-Defined Networking (SDN). SDN is capable of handling software based traffic analysis, centralized control over the network, enriched view of network, dynamic updating of forwarding the rules and identify as well as react to DDoS attacks. It also faces significant challenges in cloud due its performance, availability, scalability and security. DDoS attacks in cloud lead to on-demand self-service which causes Botnets outbreak, broad network access and rapid elasticity. Resource pooling leads to victims more vulnerable to DDoS attacks, rapid elasticity and new breed of DDoS attacks. These can be overcome by the mechanisms such as source based mechanism, network based mechanism, destination based mechanisms and hybrid mechanisms.

Chen et al. [41] have discussed about the security of data protection in cloud with the searchable cloud storage by using public-key encryption technique namely keyword search (PEKS), and resulted in failure since it was prone to Keyword Guessing Attack (KGA). To overcome this failure they have implemented new PEKS framework known as Dussal-Server Public Key Encryption using Keyword Search (DS-PEKS) and a new variant of Smooth Projective Hash Functions (SPHFs) named as Linear and Homomorphic SPHF (LH-SPHF). The main problem they have discussed was the Keyword Guessing Attack (KGA), this process accessed the required text by trial and error method by guessing the correct word which has been in the encrypted form. For generic construction of DS-PEKS it was done by the method of new variant linear and homomorphic SPHF.

Wang et al. [42] have discussed about the Searchable Encryption (SE) which have been addressed in both academic and in the industrial area for the research basis. For better security purposes they have implemented Searchable Symmetric Encryption (SSE) with higher security strength called IDcrypt. The significant problem discussed was the inference attacks in the cloud environment, like query recovery attack which converts the opaque query intruders into the desired keywords. These schemas require some changes in modification of existing applications, those results in less practical, weak in usage and hard to implement. Another main issue was the multiple indexing of the query and transferring the data among multiple users. This work provided secure concern over the Searchable encryption of data in cloud with the comparison among Index-based SE and Token-based SE. For the better encrypted search, ID Crypt makes over the indexes at proxies along with the identifiers. The token-adjustment search scheme access different indexes. For sharing the encrypted data they have used two layered encryption scheme. They also stated that for better indexing of data it is required to map more number of protocols in the cloud environment.

Wang et al. [43] have discussed the significant problem in the Outsourced Database Model (ODB) which reduced the cost of maintenance by delegating the database from the data owners to the CSP. It also resulted in various challenges, such as secrecy, verifiability, lack of correctness and completeness. To overcome these problems the authors made use of new verifiable auditing scheme, which processed the correctness and completeness of data at the same time. The process was secured in case of semi-honest-but-curious server model, which provides confidentiality in processing the data. This method can be

implemented in dynamic database with the knowledge of the verifiable database with set of tuples. This methodology also let us to the dynamic database by incorporating with the updated verifiable database.

Wang et al. [44] have proposed a model to overcome fault tolerance and analyzed about the reasons behind the failure occurrence in the model. They have provided solutions by continuous monitoring, checkpoint, restart and replication. They have discussed about the Byzantine failures which is significant fault tolerance methods in the cloud computing. This kind of failure makes the system to behave in an abnormal manner and produce inappropriate outcomes. To overcome the fault tolerance it is necessary to do the periodic steps with the continuous repetition of checking, monitoring and reporting. They have also illustrated the following methodologies in these fault tolerance namely: same clusters having multiple machines, data center having the multiple clusters, more number of data centers. The faults in cloud can be handled in cost effective and efficient manner. Thus it makes the process in a more reliable manner and it also reduced the system failure and helped in a progressive mode of accessing the data over the cloud.

Elhoseny et al. [45] have discussed about the overview of most vulnerability existing in hardware, software and network layers. Then stated the critiques of existing state-of-the-art mitigation techniques and the problem faced by the technique is also presented elaborately in the following manner as: Increase in number of cyber-attacks due to exponential growth of internet interconnections, Malware is the primary choice of weapon to carry out malicious intents in cyberspace. The above mentioned problems are overcome by assigning new attack patterns in emerging technologies is discussed. Eg: Social media, smart phone technology, critical infrastructure, various tracking techniques and the process for future research is given. It also access upon the malware attacks in the existing applications in order to safeguard the confidentiality resources.

Juliadotter and Choo [46] discussed about various methodologies of cloud computing technologies and risk assessment factors over the cloud environment. They have summarized cloud attacks and provided solutions to overcome those attacks by defining root cause of the attack till their defensive mechanisms. The major problems that they have discussed were the lack of security guards over the resources in the cloud domain upon the authorized users. DDoS attacks are significant reasons for vulnerabilities over cloud domain since it makes the server busy with the false assurance over the data. The solutions they have discussed was about identifying the vector for exploiting the resources over the cloud and also accessing the target that resulting in providing the defensive mechanism by source, vector, target, impact and defense. By the use of OWASP they were able to assign a parameter value between low risk (1) and high risk (9). The authors calculated the average through the likelihood of the impact of cloud environment. According to the different set of threats over the cloud they achieved strategies, policies and resources in desired time duration.

Shaik and Mandal [47] have discussed about the important kind of attacks such as web security attacks, browser security attacks, cloud malware injection attacks and flooding attacks. The authors have provided solutions for severe attacks and took preventive measures as following: *web security attacks:* This kind of attack can be overcome through the WS-Security, XML signatures and XML encryption. *Browser Security attacks:* They have overcome this attack using X.509 Certificate with the wrapping SAML token. *Cloud Malware Injection attacks:* This attack is overcome by the integrity checks and accessing the data over the hash value over the resources. *Flooding attacks:* This attack can be overcome with the installation of the firewall over the network or with the Intrusion Detection System (IDS). The authors have concluded with the above preventive measures for the significant

cloud attacks in the cloud domain. Table 1 shows the comparison of the cloud security issues and solutions.

4.2 Iot Enabled WSN Security Issues And Solutions

Vacca [48] discussed about the outsourcing decryption of data which enables authorized users to retrieve desired data without computing the decryption process. The author had used on-key policy attribute-based encryption which they found that it was not secured, since the reduction in loyalty of the data center. Hence he implemented novel partiality outsourcing decryption to achieve data security and computational efficiency. The significant problem discussed here was the outsourcing of data encryption based upon two issues namely (a) *The untrusted public cloud data center*: In this case they can modify the data and reduce the storage space according to their continence. (b) *Unauthorized intruders*: In this case the unauthorized users can access the data without any knowledge of the desired user. To overcome this problem the author has introduced key-policy attribute based encryption which resulted in lower computational cost and higher security protection.

Elhoseny [45] had discussed about clustering techniques. The nature of cluster is said to be dynamic, limited memory spacing and lower power processing which has been considered to be a significant drawback. To overcome this problem he has proposed a "Novel Encryption Algorithm" for the secured data transmission in the network flow, which leverages elliptic curve cryptography algorithm to propagate binary strings for each sensor and also combines with node id, cluster head, and index of the transmission to form a unique 176-bit encryption keys. The encryption and decryption process were effectively achieved using the exclusive-OR, substitution and permutation operations. The work was significantly highlighted by these two parts namely (a) Novel-encryption key generation which randomly selects the secret key for accessing the network. (b) No decryption process was required in data aggregation of cluster heads, which also eliminated recovery of data from the nodes of the cluster.

Chen et al. [49] discussed about very large scale integration circuit design for IoT enabled WSN with Micro Control Unit (MCU). They provided a sustained monitoring, mobile health, self-health management and biological analysis in the home care management. This system was mainly used for protecting the physical management of wireless information over the network. To overcome the problems faced by the network, they have implemented novel hardware sharing filter design which used transmission powerlessness compressor, an adaptive trending predictor and extensible hybrid entropy. The additional asymmetric architecture was provided to protect the confidential information over the transmission. This resulted in increased of benefits over the process with higher comparison rate and higher security for losses data transmission over the wireless network medium.

Lu et al. [50] have discussed about the attacks due to the limited computational energy, storage resources, and sensor nodes. They have implemented with a proposed methodology such as the Wireless authentication center (WAC) with mixed encryption known as "MEWAC". It was based upon the MCU and Wi-Fi (Wireless Fidelity) which makes use of the following algorithms such as RSA, Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) for deriving high performance authentication protocol and encryption of data services on sensor nodes. They have discussed about the security threats related in IoT enabled WSN. They also discussed about the following parameters to be achieved: consumption of energy, retransmission of the data packets, and larger storage of the data. To improve the security the authors had implemented wireless authentication center with

Table 1 Comparison of the cloud security issues and solutions

Paper nos	Algorithm/methodology	Security solution	Application	Pros	Cons
[33]	Game theoretic approach	Improving decision making strategy	Sensor clouds	Efficient energy consumption	Complexity of data is larger
[34]	Classifier system distributed DoS	Identifying the packets source within the time frame	Cloud computing	Provide accuracy over the data and reduces the time complexity	Consumes more bandwidth
[35]	Accountable privacy preserving mechanism	Focusing on the illegal behavior	Cloud computing	Identification of illegal network behavior	Less security over the storage of data in cloud
[36]	Securing coding based cloud storage	Detect the simple pollution attack	Cloud computing	Able to separate the attackers and crackers	Third party can corrupt the data
[37]	Keyword search function: outsourced attribute based encryption	Partially decrypt the cipher text without the knowledge of plaintext	Cloud computing	Can perform partial decryption task and efficient in query Processing	Less security over the encrypted data
[39]	Big data based security analytics	Monitoring the hooks and Signature based attacks updating	Big-data and cloud computing	Detect the advanced attacks	Regular signature updating in detecting zero day attack
[40]	Source, Destination, network based and hybrid mechanisms	Secure the cloud from the malicious attacks	Software defined network, Cloud computing	Dynamically automated and trusted device mechanisms. and the reductionin DDoS attack	Lack of Trustworthiness and access upon the unauthorized users
[41]	Dual-Server Public Key Encryption using Keyword Search (DS-PEKS)	Overcome the keyword guessing attack	Cloud computing	Provides strong security over the keyword guessing attack	Lack of data privacy and suffers from complicated secret key distribution
[42]	Symmetric encryption	ID-crypt	Cloud computing	Search efficiency search and more security protection through key sharing scheme	Leakage of the data without the prior knowledge of the users
[43]	Verifiable auditing	Process the correctness and the completeness	Cloud computing	Supports dynamic databases with updating of verifiable database	Lack of support in correctness and completeness for query results
[44]	Fault tolerance methodology	Continuous repetition of checking monitoring and reporting	Cloud computing	Faults in cloud can be handled with lower cost and efficient access of the data	Difficult to access larger data in cloud and hard to find the source of the attack

Table 1 (continued)

Paper nos	Algorithm/methodology	Security solution	Application	Pros	Cons
[46]	CIA (Confidentiality, Integrity, Authentication) Criteria	Newer attack patterns and state of art mitigation techniques	Cloud computing, social media	Trust worthy environment is ensured	Defects in the infrastructure and the vulnerabilities in the protocol

mixed encryption "MEWAC". It mainly reduced DoS attacks, tampering, overhead, and retransmission. It not only resulted in lower power consumption, cost compatible and good performance but achieved advancement protection in sensor nodes.

Sofwan et al. [51] discussed about the problem of load on the slope grows due to increase in water content in the soil during the rainy season which leads to landslide. To overcome this problem they have provided the following sequential steps for processing (a) Arduino ATMega 2560 microcontroller which was used to collect data from the sensors which were placed in different geographical regions (b) Sensed data was transmitted into cloud through GSM communication modem. The authors provided the network design in case of the landslide with the two types of data values: measured value and actual value in order to access the system with the more protective manner with respect to slope, temperature, humidity and soil moisture over the IoT enabled WSN for the secure and accurate progress of data.

Khalil et al. [52] have discussed about the strong level of complexity in case of considering the interoperability between the heterogeneous internet things, with the set of mobile handheld devices and wireless sensors in the internet. They have provided a real world test bed deployment WSNs in IOT and provided some set of integration over the networks. The significant set of problems they have discussed was the control over the electrical appliances in case of smart building by: (a) identification of the challenges in the deployment of IPv6 over 6LoWPAN with the interface associated with IPv4 networks. (b) Identification of the challenges in the deployment with the two way communication between wireless sensors and internet users. They provided the system with the integrating WSNs into IOT with the essential blocks over the WSN, Gateway server, Middleware and mobile client. They have implemented the system in reliable manner and the level of performance over the system.

Ivana et al. [53] discussed about the applications and also stated the pervasiveness over the cloud environment and also provides the security over the internal and external data. The significant problem they have discussed is with the potential security issues over the sensor networks based upon the privacy, data integrity and availability over the cloud resources in the network. In the previous cases they have just identified the results over the security challenges and the causes for the threat in the IOT. According to the threats they have analyzed various set of attacks over the wireless domain with the respective of the layered architecture in WSN by the various attacks such as Eavesdropping, Intelligent jamming, Selective forwarding, Data integrity and attacks on reliability. In addition to that they have stated with the implementation of Cooja, security module for the evaluation of the network performance.

D'Orazio et al. [54] said that the accessibility of big data and storage of data in a range of IOT devices is increasing widely. They have demonstrated how an attacker could exfilterate data from IOS devices. The issues were exploitation of IoT devices, software and OS due to unhealthy pairing and Exfilteration of data from a paired iOS devices by abusing a library and a command line tool distributed with iTunes. To overcome these issues they made preventive measures for device manufacturers and for device users. The significant contribution of this paper was to provide a concept application to demonstrate the practical approach with better understanding capabilities of attackers over the iOS devices using the trusted computers.

Zhou et al. [55] discussed about the significant drawback as the Information fusion which can decrease the throughput of transmitted information in internet of vehicles by compressing the redundant information to improve the wireless resource efficiency. To overcome this issue they have suggested the following calculative steps: (a) Spatio

temporal correlation status parameters of different vehicles are calculated by Cauchy's equation. (b) The probability of status parameters is obtained through Bajarktarevic mean function. (c).The time and location parameter sets are fused by Dempster fusion rule respectively. Thus with the use of the Cauchy's equation it provides an improved efficiency over the correlation decision and reduces the concept of probability function over the metric process. Finally it also reduces the complexity and ensure with reliability progress over the process.

Cheng et al. [56] have discussed about the concurrent data collection trees specifically designed for IOT applications and comparison of existing single-user data collection structure systems with proposed tree structures. This system mitigated the yield of the concurrent data collection process. The significant issues were as follows (a) low effectiveness in the data collection process in IOT systems. (b) Challenges in the design of efficient data collection process. These issues can be overcome through the following process (a) performance of proposed network structure was analyzed using computer simulations-MATLAB. (b) A delay-aware network structure specifically designed for concurrent data collection process in IOT systems. This resulted in providing interconnected systems over the different parties for accessing the multiple resources among variety of user with the same set of IOT devices and reduction in the delays of the collection process over the concurrent data.

Bouabdellah et al [57] have mainly classified the various attacks that targets network layer functionalities, existing detection techniques and countermeasures that highlight the main security challenges for such networks. They have provided the results in analyzing the attacks which have been targeted to access upon the network layer functions by introducing the existing attacks in traditional wireless networks and analyzed the feasibility study over the progress.

Smith [58] discussed about securing data over the network which was really very confidential process, since it is bonded with larger number of resources over the interconnected network domain thus results in larger vulnerability to the attacks by the unauthorized users. This mainly follows the CIA criteria over the process. The significant reason for these attacks is access of unauthorized users over the network makes the information to be less protective over the internet. It safeguards the network using the firewall methodologies over the network. Thus the threats over the network should be identified initially and allow the authorized persons to have access upon the resources over the network. It resulted in safeguarding over the information in the network domain and ensured the data in a confidential manner.

Xiong et al. [59] introduced an efficient and multi-level conditional privacy preservation authentication protocol based on ring signature. The process of producing secure vehicular communications was demonstrated through extensive analysis. The significant challenges analyzed here proved that the previous methods were insecure and also expensive in case of tracking an issue and high storage requirements that were needed in existing protocol. They have overcome above challenges by conditional privacy preservation authentication. The authors have arrived desired solutions of progressing the resources in the wireless domain with the process of authentication mechanism over the secured information. Table 2 shows the Comparison of IOT enabled WSN Security issues and solutions.

Table 3 shows the Comparison of the Cloud integrated IoT enabled Sensor network Security Issues and the possible Solutions.

Table 2 Comparison of IOT enabled WSN security issues and solutions

Paper nos	Algorithm/methodology	Security solution	Pros	Cons
[48]	Symmetric encryption	Encrypt the data according to the KP-ABE and finally send the cipher text to the data center	Access the data with the help of secret key and computational cost is low	Security of data is less in outsourced database
[45]	Symmetric encryption	Secure data transmission the network flow	Improved network lifetime and overcame several security attacks such as brute-force attack, HELLO flood attack, etc	Less security and larger energy consumption
[49]	Asymmetric encryption	Decrease the transmission power losses and an adaptive trending predictor	Efficient in monitoring the physical signals	Limited access of the bandwidth and computational speed is very low
[58]	Authentication center with mixed encryption	Upgrading the performance speed and reducing the power consumption in the sensor network	Provides higher authentication and Encryption of data	Limited storage of the resources and less computational cost
[51]	Ardunio AT Mega2560 microcontroller	To access the system in a more protective manner	For the real time determination of the natural disasters	The data cannot be accessed without the pervasive environment
[52]	Sensing data, Sink packet forwarding	Integrating WSN into IOT with the essential blocks	Collection of the sensing data and keep track of energy consumption	Maintenance of the data is difficult
[53]	Cyber physical systems	Use of IEEE802.15.4, B-MAC, 6LoWPAN, RPL, BCP, CTP	Reduced disruption of the data	Less protective over the confidential data and modification of data by unauthorized users
[54]	iOS Data Extrfiltration, iOS pairing	Understanding capabilities of attackers over the iOS devices using the trusted computers	Reduces the number of attack vectors	Unauthorized access over the data
[55]	Fusion algorithm	Improved efficiency and reduces the concept of probability function	Improves the performance reliability and error occurrence is reduced	Decrease in wireless resources efficiency
[56]	Concurrent data collection tress	Reduction in the delay of the collection process over the concurrent data	Feasible transmission of data	Data collection will be large for the single extraction
[60]	Security techniques	Periodic testing over the vulnerabilities, audit and recovery over the failures	Data are kept in secured manner	Users must have the knowledge between the cracker and the hacker

Table 2 (continued)

Paper nos	Algorithm/methodology	Security solution	Pros	Cons
[57]	Cognitive radio	Solve the Problem of spectrum scarcity	The attacks are identified with the help of trust frameworks spectrum scarcity	Network maintenance is difficult
[59]	CIA criteria	Maintain the required data in a redundant manner	Safeguarding the data using firewall methodologies	Vulnerabilities over the zero day attacks
[47]	Multilevel privacy preserving communication protocol	Conditional privacy preservation authentication	It provides a conditional privacy preservation authentication and verification of messages	Access over the unreliable messages will be in danger

Table 3 Cloud integrated IoT enabled Sensor network-Security issues and solutions

Sl. no	Problem/issues	Possible solutions
1	Periodic occurrence and the reduction of false alarm	Game theoretic approach—variety of decision making
2	Difficult to identify the authenticated user which leads to financial loss	CS_DDOS approach to identify the desired attacks from the network regardless of origin of packet generation from the desired node
3	Openness and storage	Accountable privacy preserving mechanism—identification of illegal behavior of the system
4	Pollution attacks	The alarm trigger procedure issued to locate the polluting nodes with the help of proposed system algorithm
5	Security issues	Keyword search function: Outsourced Attribute Based Encryption,(KSF-OABE) this method can partially decrypt the cipher text without the knowledge of plain text with the help of Cloud Service Provider(CSP)
6	Large storage, lack of transparency, cyber security	MBD Medical Big Data to secure the patients information in the cloud environment
7	Scalability and virtualized infrastructure	Monitoring the hooks and Signature based attacks updating
8	Cyber attackers	Monitoring the hooks, Signature based attacks updating
9	DDoS attacks	Source based mechanism, network based mechanism, destination based mechanism, hybrid mechanisms
10	Keyword guessing attack	Dual Server Public Key Encryption with Keyword Search (DS-PEKS)in order to address the security protection
11	Outsourced database model secrecy, verifiability	New verifiable auditing scheme, which process the correctness and the completeness at the same time
12	The untrusted public cloud data center, unauthorized intruders	Novel based method by providing a transformation key by the authorized users and the decryption of data is done by datacenter without any original knowledge of the data
13	Security based transmission	Novel Encryption Algorithm-dynamic nature of the data, larger cluster configurations
14	More power consumption, Mis-corruptions of data, Less efficiency over larger volume of the data and also include of attackers over the transmission of the data path	Novel hardware sharing filter design, asymmetric architecture, Novel hardware sharing filter design in order to decrease the transmission power
15	Consumption of energy, retransmission of the data packets, larger storage of the data, sensor nodes	Wireless authentication center with mixed encryption

Table 3 (continued)

Sl. no	Problem/issues	Possible solutions
16	Crash Faults and Byzanite Failures	Continuous repetition of checking monitoring and reporting
17	The untrusted public cloud data center, Unauthorized intruders	Key-policy attribute based encryption.The outsourcingdatabase encryption is processed using the novel based method by providing a transformation key by the authorized users and the decryption of data is one by data center without any original knowledge of the data
18	Lower processing speed, less storage area, dynamic nature of network	Novel encryption algorithm to overcome challenges in the network such as dynamic nature of the data, larger cluster configurations in order to have a secured environment
19	Consumption of energy is more, retransmission of the data packets, Larger storage of the data	Wireless authentication center with mixed encryption "MEWAC". It mainly reduces the DoS attacks, tampering, overhead, and retransmission
20	Identification of the challenges in the deployment of IPv6 over 6LoWPAN with the interface associated with IPv4 networks and the deployment with the two way communication between the wireless sensors and the internet users	Integrating WSNs into IOT with the essential blocks over the wireless sensor network (WSN), Gateway server, Middleware, Mobile client
21	Potential security issues	Solutions according to the set of WSN Protocols like IEEE802.15.4, B-MAC, 6LoWPAN, RPL, BCP, CTP
22	Web security attack, Browser Security attack, Cloud malware injection attack, Flooding attack	WS-Security and XML signatures and XML encryption, X.509 Certificate with the wrapping SAML token, integrity checks and the accessing the data over the hash value over the resources, the installation of the firewall over the network or with the intrusion detection system
23	Exploitation of the IoT devices, software and OS due to unhealthy pairing, and Exfiltration of data from a paired iOS devices by using a library and a command line tool distributed with iTunes	Device manufacturers should provide mechanisms that allow users to selectively authorize client software to access the device resources, Users should be practiced with security hygiene-apps must not be installed from unknown origin
24	Low effectiveness in the data collection process in IoT systems, Challenges in the design of efficient data collection process	A delay-aware network structure specifically designed for concurrent data collection process in IOT systems
25	Wireless sniffers, Packet sniffers, Portscanners, Port knocking, Key stroke loggers and even many more	List out the forms of resources need to be kept in a secure manner, Count over the confidential user over the network, Calculate the accessing time for each and every user in the network, analyze the risk assessment

Table 3 (continued)

Sl. no	Problem/issues	Possible solutions
26	Due to increasing number of Mobile devices, spectrum scarcity is emerging in the medium and the functionalities	New functionalities in physical medium, media access control and network layers of the TCP/IP protocol stack to be introduced. Cognitive Radio is the promising technology that solves the problem of spectrum scarcity
27	Sending the confidential information over the undesired emails mistakenly, Security vulnerabilities which results in zero day attacks, The network results in lack of defense in the path	Confidentiality, Integrity and availability to be strictly enforced

5 Conclusion

IoT is a collection of devices enabled with internet and the devices are more often sensors that sense/measure the real time environmental parameters and transfer the parameters to cloud environment for processing through IoT. Unfortunately the aforementioned paradigm suffers from a variety of vulnerabilities since their devices are exposed in nature. This paper presents a survey on the security issues and challenges faced by the cloud assisted IOT enabled sensor networks. This integrated paradigm is of more important in providing solutions to various real time problems. We conclude that this survey has more significance in recent years and we have identified the various security issues faced by the Cloud integrated IoT enabled sensor network environment and the possible solutions provided in the recent literature. Since security of integrating these two important technologies is of more significance, better solutions can be proposed to mitigate the security issues in future. The security issues reviewed in this paper can be utilized to propose better solutions.

References

1. Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). *Internet of things security: A top-down survey.*. https://doi.org/10.1016/j.comnet.2018.03.012.
2. Tewari, A., & Gupta, B. B. (2018). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.04.027.
3. Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University Computer and Information Sciences, 30*(3), 3. https://doi.org/10.1016/j.jksuci.2016.10.003.
4. Internet-of-things-definition. (2016). https://iot-analytics.com/internet-of-things-definition/(iotintro).
5. El, H., & azharyaba., (2019). Internet of Things (IoT) mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms Disambiguation and research directions. *Journal of Network and Computer Applications, 28*, 105–140. https://doi.org/10.1016/j.jnca.2018.10.021.
6. Ketshabetswe, L. K., Zungeru, A. M., Mangwala, M., Chuma, J. M., & Sigweni, B. (2019). Communication protocols for wireless sensor networks: A survey and comparison. *Heliyon*. https://doi.org/10.1016/j.heliyon.2019.e01591.
7. Wireless_sensor_network. (2016). https://en.wikipedia.org/wiki/Wireless_sensor_network(intro)
8. Rastko, R., Selmic, P., Serwadda, V. V. (2016). Wireless sensor networks security, coverage, and localization. https://link.springer.com/chapter/10.1007/978-3-319-46769-6_2.
9. Tarun Agarwal. (2019). https://www.elprocus.com/introduction-to-wireless-sensor-networks-types-and-applications.
10. Cloud Computing. (2017). https://en.wikipedia.org/wiki/Cloud_computing.
11. Stergio, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964–975. https://doi.org/10.1016/j.future.2016.11.031.
12. Hovhannesavoyan. (2016). https://www.monitis.com/blog/3-types-of-cloud-services/(cloudservices).
13. Di Martino, B., Pascarella, J., Nacchia, S., Maisto, S. A., Iannucci, P., & Cerri, F. (2018). Cloud services categories identification from requirements specifications. In *32nd international conference on advanced information networking and applications workshops (WAINA), Krakow* (pp. 436–441). https://doi.org/10.1109/WAINA.2018.00125.
14. Tyagi, A., Kushwah, J., & Bhalla, M. (2017). Threats to security of Wireless Sensor Networks. In *7th international conference on cloud computing, data science & engineering—Confluence, Noida* (pp. 402–405). https://doi.org/10.1109/CONFLUENCE.2017.7943183.
15. Evans, K., Jones, A., Preece, A., Quevedo, F., Rogers, D., Spasić, I., Taylor, I., Stankovski, V. Taherizadeh, S., Trnkoczy, J., Suciu, G., Suciu, V., Martin, P. N., Wang, J., & Zhao, Z. (2015). Dynamically reconfigurable workflows for time-critical applications. In *WORKS '15: proceedings of the 10th workshop on workflows in support of large-scale science* (pp. 1–10). https://doi.org/10.1145/2822332.2822339.
16. Štefanič, P., Cigale, M., Jones, A. C., Knight, L., Taylor, I., Istrate, C., et al. (2019). SWITCH workbench: A novel approach for the development and deployment of time-critical microservice-based

cloud-native applications. *Future Generation Computer Systems, 99*, 197–212. https://doi.org/10.1016/j.future.2019.04.008.
17. Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, *56*, 684–700. https://doi.org/10.1016/j.future.2015.09.021.
18. Aazam, M., & Huh, E.-N.(2014). Fog computing and smart gateway based communication for cloud of things. In *International conference on future internet of things and cloud (FiCloud)* (pp. 464–470). https://doi.org/10.1109/FiCloud.2014.83.
19. Serrano, M., Hauswirth, M., & Soldatos, J. (2014). Design principles for utility-driven services and cloud-based computing modelling for the internet of things. *International Journal of Web and Grid Services*, *10*(2–3), 139–167. https://doi.org/10.1504/IJWGS.2014.060254.
20. Deogirikar, J., & Vidhate, A. (2017). Security attacks in IoT: A survey. In *International conference on I-SMAC (IoT in social, mobile, analytics and cloud) (I-SMAC), Palladam* (pp. 32–37). https://doi.org/10.1109/I-SMAC.2017.8058363.
21. Ghosh, S., Mukherjee, A., Ghosh, S. K., & Buyya, R. (2019). Mobi-IoST: Mobility-aware cloud-fog-edge-IoT collaborative framework for time-critical applications. *IEEE Transactions on Network Science and Engineering*. https://doi.org/10.1109/TNSE.2019.2941754.
22. Haddad Pajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2019). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*. https://doi.org/10.1016/j.iot.2019.100129.
23. Margaret Rouse. (2016). https://internetofthingsagenda.techtarget.com/definition/smart-city.
24. Home_automation. (2018) .https://en.wikipedia.org/wiki/Home_automation.
25. Smart-home-or-building. (2017). https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building.
26. Knud Lasse Lueth. (2015). https://iot-analytics.com/10-internet-of-things-applications.
27. Gómez, J., Oviedo, B., & Zhuma, E. (2016). Patient monitoring system based on internet of things. *Procedia Computer Science, 83*, 90–97. https://doi.org/10.1016/j.procs.2016.04.103.
28. Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. *Applied Computing and Informatics, 13*(1), 57–65. https://doi.org/10.1016/j.aci.2016.03.001.
29. Alshammari, A., Alhaidari, S., Alharbi, A., & Zohdy, M. (2018). Security threats and challenges in cloud computing. In *IEEE 4th international conference on cyber security and cloud computing (CSCloud), New York. NY* (pp. 46–51). https://doi.org/10.1109/CSCloud.2017.59.
30. Singh, R., et al. (2016). Attacks on wireless sensor network: A survey. *International Journal of Computer Science and Mobile Computing, 5*(5), 10–16.
31. Al-Shayeji, M., & Ebrahime, F. (2019). A secure and energy-efficient platform for the integration of Wireless Sensor Networks and Mobile Cloud Computing. *Computer Networks*. https://doi.org/10.1016/j.comnet.2019.106956.
32. Gaware, A., & Dhonde, S. B. (2016). A survey on security attacks in wireless sensor networks. In *3rd international conference on computing for sustainable global development (INDIACom), New Delhi* (pp. 536–539).
33. Liu, J., Yu, J., & Shen, S. (2017). Energy-efficient two-layer cooperative defense scheme to secure sensor-clouds. *IEEE Transactions on Information Forensics and Security*. https://doi.org/10.1109/TIFS.20172756344.
34. Sahi, A., Lal, D., Li, Y., & Diykh, M. (2017). An efficient DDos TCP flood attack detection and prevention system in a cloud environment. *IEEE Access*. https://doi.org/10.1109/Access.2017.2688460.
35. Cheng, H., Rong, C., Qian, M., & Wang, W. (2018). Accountable privacy-preserving mechanism for cloud computing based on identify-based encryption. *IEEE Access*. https://doi.org/10.1109/Access.2018.2851599.
36. Anglano, C., Gaeta, R., & Grangetto, M. (2016). Securing coding-based cloud storage against pollution attacks. *IEEE Transactions on Parallel and Distributed Systems*. https://doi.org/10.1109/TPDS.2016.2619686.
37. Li, J., Lin, X., Zhang, Y., & Han, J. (2016). IEEE KSF-OABE: Outsourced attributed-based encryption with keyword search function for cloud storage. *IEEE Transaction on Services Computing*. https://doi.org/10.1109/TSC.2016.2542813.
38. Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access*. https://doi.org/10.1109/access.2017.2757844.

39. Win, T. Y., Tianfield, H., & Mair, Q. (2017). Big data based security analytics for protecting virtualized infrastructures in cloud computing. *IEEE Transactions on Big Data*. https://doi.org/10.1109/TBDATA.2017.2715335.
40. Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2015). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/COMST.2015.2487361.
41. Chen, R., Mu, Y., Yang, G., Guo, F., & Wang, X. (2015). Dual-server public-key encryption with keyword search for secure cloud storage. *IEEE Transactions on Information Forensics Security*. https://doi.org/10.1109/TIPS.2015.2510822.
42. Wang, G., Liu, C., Dong, Y., Pan, H., & Fang, B. (2017). IDCrypt: A multi-user searchable symmetric encryption scheme for cloud applications. *IEEE Access*. https://doi.org/10.1109/Access.2017.2786026.
43. Wang, J., Chen, X., Huang, X., You, I., & Xiang, Y. (2015). Verifiable auditing for outsourced database in cloud computing. *IEEE Transaction on Computers*. https://doi.org/10.1109/TC.2015.2401036.
44. Wang, Q., Yu, C. W., Li, F., Wang, H., & Cao, L. (2016). A group key-policy attribute-based encryption with partial outsourcing decryption in wireless sensor networks. *Security and Communication Networks*. https://doi.org/10.1002/sec.1594.
45. Elhoseny, M., Yuan, X., El-Minir, H. K., & Riad, A. M. (2018). An energy efficient encryption method for secure dynamic WSN Research article. *Security and Communication Networks*. https://doi.org/10.1002/sec.1459.
46. Juliadotter, N. V., & Choo, K. K. R. (2015). Cloud attack and risk assessment taxonomy. *IEEE Cloud Computing Society, 2*, 14–20.
47. Shaik, A. A., & Mandal, M. M. (2016). Attacks on cloud computing and its countermeasures. In *International conference on signal processing, communication, power and embedded system (SCOPES)*.
48. Vacca, J. R. (2013). *Computer and information security handbook* (2nd ed.). Amsterdam: Elsevier.
49. Chen, S. L., Tuan, M. C., Lee, H.-Y., & Lin, T.-L. (2017). IEEE VLSI implementation of a cost-efficient micro control unit with an asymmetric encryption for wireless body sensor networks. *IEEE Access*. https://doi.org/10.1109/Access.2017.2679123.
50. Lu, Y., Zhai, J., Zhu, R., & Qin, J. (2016). Study of wireless authentication center with mixed encryption in WSN. *Journal of Sensors*. https://doi.org/10.1155/2016/9297562.
51. Sofwan, A., Ridho, M., & Goni, A. (2017). Wireless sensor network design for landslide warning system in IoT Architecture (ICITACEE). In *4th international conference on information technology, computer, and electrical engineering (ICITACEE)*. https://doi.org/10.1109/ICITACEE.2017.8257718.
52. Khail, N., Abid, M. R., Benhaddu, D., & Gerndt, M. (2014). *Wireless sensors networks for internet of things* (pp. 21–24). Singapore: ISSNIP.
53. Ivana, T., & McCann, J. A. (2017). A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2017.2749883.
54. D'Orazio, C. J., Choo, K. K. R., & Yang, L. T. (2017). Data exfiltration from internet of things devices iOS devices as case studies. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2016.2569094.
55. Zhou, Y., Qiu, G., & Qiu, Y. (2016). An improved traffic safety information fusion algorithm in internet of vehicles. *IEEE Internet of Things journal*. https://doi.org/10.1109/ICCS.2016.7833610.
56. Cheng, C.-T., Ganganath, N., & Fok, K.-Y. (2017). Concurrent data collection trees for IoT applications. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2016.2610139.
57. Bouabdellah, M., Kaabouch, N., El Bouanani, F., & Ben-Azza, H. (2017). Network layer attacks and countermeasures in cognitive radio networks: A survey. *Journal of Information Security and Applications*. https://doi.org/10.1016/j.jisa-2017.11.010.
58. Smith, R. E. (2016). *Elementary information security* (2nd ed.). Burlington: Jones and Bartlett Learning.
59. Xiong, H., Chen, Z., & Li, F. (2012). Efficient and multi-level privacy-preserving communication protocol fog vanet. *Computers & Electrical Engineering*. https://doi.org/10.1016/j.compeleceng.2011.11.009.
60. Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005.

Dr. R. Geetha received B.E. degree in Computer Science and Engineering from Madras University in 1999, M.E. in Computer Science and Engineering from Anna University in 2006 and Ph.D., in 2017 from School of Computing and Information Technology, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology (Vel Tech Dr. RR & Dr. SR Technical University), India. She has over 20 years of teaching experience and working currently in S.A. Engineering College as Professor. Her research interests include Wireless Networks, Security Schemes in Wireless networks, Internet of Things. She is a Life member of Indian Society for Technical Education (ISTE) and member of Computer Society of India (CSI). She is the author/coauthor of several research papers in international conferences and journals.

A. K. Suntheya received her B.E. degree in Computer Science and Engineering from Jaya Sakthi Engineering college in 2017, M.E. degree in Computer Science and Engineering from S.A. Engineering College in 2019. Her areas of interest include Wireless Sensor Networks, Cloud Computing. She has published several research papers in international conferences and journals.

Dr. G. Umarani Srikanth received B.E. degree in Electronics and communication from Madras University, M.E., degree in Computer Science and Engineering from Bharathidasan University in 1996 and Ph.D., in Computer Science from Anna University in 2013. She has over 28 years of teaching experience and working currently in St. Peters College of Engineering and Technology as Professor. Her research interests include Soft Computing, Internet of Things, Sensor Networks. She is a Life member of Indian Society for Technical Education (ISTE) and member of Computer Society of India (CSI). She is the author/coauthor of several research papers in international conferences and journals.