Journal of Network and Computer Applications 168 (2020) 102761

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics

Mobasshir Mahbub [a,b,*]

[a] Department of Electrical and Electronic Engineering, Ahsanullah University of Science and Technology, Dhaka, Bangladesh
[b] Department of Electronics and Communications Engineering, East West University, Dhaka, Bangladesh

ARTICLE INFO

Keywords:
IoT
Vulnerability
Security
Cryptography
Fog computing
Edge computing
Machine learning

ABSTRACT

The IoT is the upcoming one of the major networking technologies. Using the IoT, different items or devices can be allowed to continuously generate, obtain, and exchange information. Different IoT applications nowadays are centered on computerizing various errands and are attempting to engage the inanimate physical items to act without direct supervision of a human. The current and forthcoming IoT services are exceptionally encouraging to build the degree of solace, proficiency, and automation for the clients. To obtain the option to actualize such a world in a continuously developing manner requires high security, protection, verification, and recuperation from assaults. Right now, incorporating the requisite changes in IoT systems engineering to achieve end-to-end, stable IoT infrastructure is paramount. In this research, a comprehensive analysis is incorporated into the security-relevant problems and threat wellsprings in IoT resources or applications. Specific that and current advancements based on maintaining a high degree of confidence in IoT apps are addressed while looking at the security issues. Four distinct developments are investigated, including cryptography, fog computing, edge computing, and ML (Machine Learning), to extend the degree of IoT security.

1. Introduction

An increasing number of objects or items are being associated with the Internet at an unprecedented rate understanding the possibility of the Internet of Things (IoT). A fundamental case of such items incorporates thermostats, indoor regulators, and HVAC observing and control frameworks that empower intelligent homes. There are additionally different areas and situations in which the IoT can assume a wonderful job and improve the conditions of our lives. These applications incorporate transportation, e-healthcare, industrial mechanization, and crisis response to regular and man-made debacles where the human dynamics are troublesome. The IoT empowers objects to watch, sense, compute and perform roles by having them "talk" together, to share data, and to make decisions. The IoT changes these items from being customary to intelligent by exploiting its basic advancements, for example, omnipresent and pervasive computing, communication technologies, embedded gadgets, sensing systems, Internet protocols, and services. Smart devices alongside their alleged errands establish space explicit applications (vertical markets) while pervasive computing and scientific approaches form an application platform for autonomous services (horizontal markets). Fig. 1 will show an illustration of IoT.

The growth of interfacing physical gadgets around us to the Internet is expanding quickly. According to Gartner's study, by 2020 there will be at least 8.4 billion connected devices worldwide. This number is expected to increase to 20.4 billion by 2022. The usage of IoT technologies is growing through all areas of the globe. Asia, North America, and China are the main moving nations right now. The machine-to-machine (M2M) connections count is expected to grow from 5.6 billion in 2016 to 27 billion in 2024 (Kumar et al., 2019). This leap in numbers itself proclaims IoT as one of the leading derivative markets that might build a base for the developed economy. It is estimated that the IoT sector will raise sales from $892 billion (2018) to $4 trillion (2025) (Ray, 2018). M2M interfaces cover a broad variety of applications such as smart towns, smart grids, intelligent management of the climate, smart shopping, smart harvesting, and so forth (Mehta et al., 2018). Gadgets are not only supposed to be connected with the internet and other surrounding gadgets in the future, but are often required to legally communicate on the phone with various gadgets. Aside from the hardware or related items, the notion of social IoT (SIoT) is also growing. SIoT will empower diverse social networking clients to be associated with gadgets and clients can share the gadgets over the Internet (Pathan et al., 2019; Imran et al., 2019). Figs. 2 and 3 will visualize the current and future scenarios of IoT.

* Department of Electrical and Electronic Engineering, Ahsanullah University of Science and Technology, Dhaka, Bangladesh.
E-mail address: mbsrmhb@gmail.com.

https://doi.org/10.1016/j.jnca.2020.102761
Received 26 April 2020; Received in revised form 5 June 2020; Accepted 1 July 2020
Available online 17 July 2020

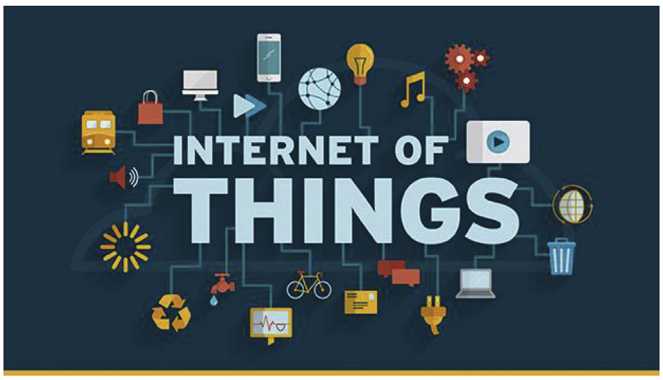

Fig. 1. An illustration on IoT.

With this tremendous range of IoT applications or services, the issue of security and protection arises as well. Without integrating a trustworthy and an interoperable IoT network, creating IoT applications cannot attain success and can lose all of their latent ability. In addition to the security problems posed by the internet, telecommunication networks, and WSANs or WSNs, IoT often has its security concerns, such as problems of safety, management issues, authentication issues, data storage, etc. These are considerably more challenging than securing ordinary IT gadgets. Because of these concerns and vulnerabilities, IoT applications make a prolific ground for various types of digital threats. There are lots of examples of different cyber assaults on the current IoT applications around the world. The Mirai malware was reported to taint about 2.5 million Internet-related gadgets and deploy DDoS assaults in the last span of 2016. After Mirai, two other major botnet assaults are Hajime and Reaper, driven toward a large amount of IoT gadgets (Ande et al., 2020). Recently in April 2020 a new botnet malware attack against IoT gadgets named Dark Nexus spotted by cybersecurity researchers. It leverages vulnerable IoT gadgets to perform a DDoS attack. So far the attack comprises around 1372 bots, performed as a reverse proxy, and spanned to China, Thailand, Brazil, South Korea, and Russia (The Hacker News, 2020). IoT gadgets, being low power and comparatively less secured, give a door to the enemies for accessing into IoT systems, in this way giving simple access to the client's information. In the same way, the

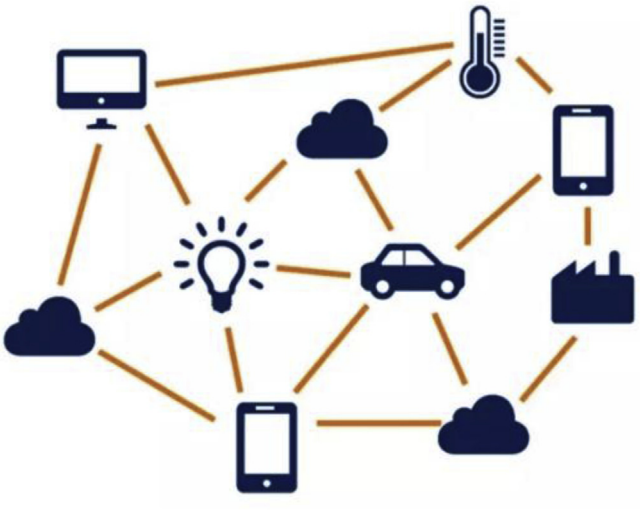

Fig. 3. Future IoT concept.

IoT space expands beyond basic objects or products. Various successful attempts have been made to insert IoT gadgets into the human body to track the live status of various organs (Silvera-Tawil et al., 2020). Assailants target these gadgets to pursue a particular person or misrepresented details to the exact spot. Such an assault has not happened at this point, in actuality, but when these devices are compromised it can be particularly dangerous. CPS (Cyber-Physical Systems) is another sector that is benefiting from IoT growth. In the field, artifacts or machines are detected in CPS, and movements are rendered depending on the physical adjustments. Because CPS envelops infrastructure of vital significance (e.g. power grids, transportation, etc.), risks to protection and privacy in these systems have significant implications. Security risks to CPS, though, have their particular natures which are outside this paper's reach. There are four major levels within each IoT network. The primary layer integrates the usage of different sensors and actuators to gather data to perform various functionalities. Because of this, a coordination device is used in the corresponding layer to relay the data obtained. The overwhelming majority of progressing IoT systems is communicating the

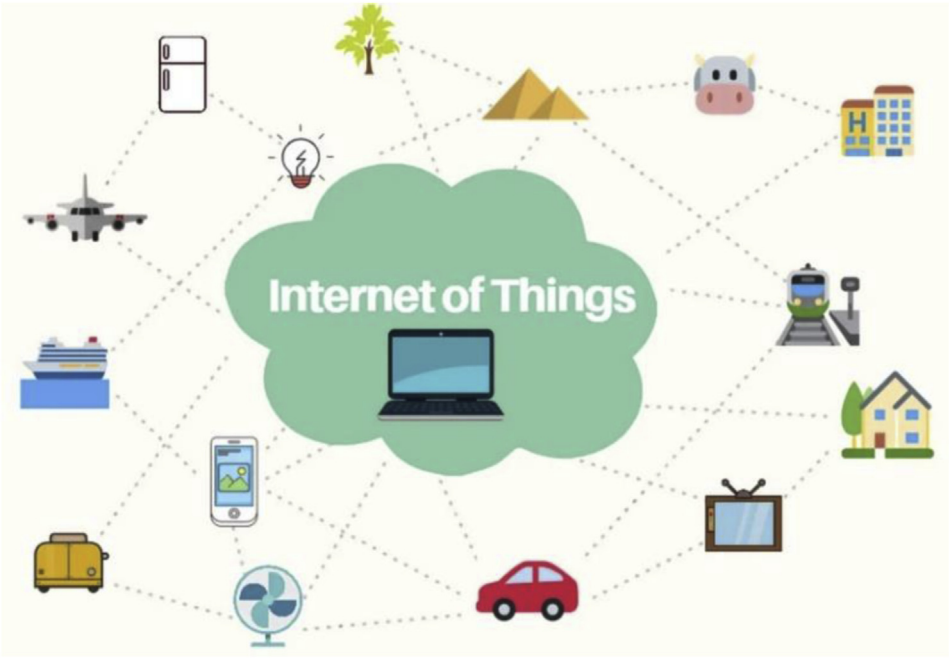

Fig. 2. Current IoT scenario.

third layer, called a middle-ware system, as a scaffold between the networking and application layer. Finally, it falls the fourth sheet, for example, there are numerous IoT-aided systems, such as smart grids, smart cars, smart processing plants, etc. Such four levels have clear protection concerns about them. Apart from these levels, various inputs or gateways connect certain levels and assist in data flow or movement. There are so many privacy issues explicit to these gateways also. In this work, a definitive study of IoT security arrangements in the current works, surveys, and literature is introduced. Most importantly, the principal limitations to accomplish elevated levels for security in IoT services are introduced. The goal of this research is to showcase current and potential IoT protection solutions. Furthermore, the four main types of IoT security arrangements are featured: (1) cryptography-aided arrangements; (2) fog computing-aided arrangements; (3) ML-aided arrangements, and (4) edge computing-based arrangements.

2. Related surveys and literature

There are numerous IoT protection and privacy surveys currently underway. The table (Table 1) underneath will show the considered review and survey topics.

Cerny et al. (2018) performed a survey on the management of identity, authorization, and authentication in terms of the application layer. Yang et al. (2017) have summarized different issues regarding security in IoT applications. Hu et al. (2020) worked on data provenance on their work. Authors of Chen et al. (2017) have talked about the security issues explicit to location-aware services in IoT. They have focused on the specific issues identified with localization and positioning of IoT gadgets. Aufner (2019) has tried to find out security gaps on common threat models designed for IoT. The main purpose of Noor et al. (2018a) is to provide a review of ongoing IoT security research. In this paper Ammar et al. (2018), authors have surveyed the privacy issues of the primary IoT frameworks. For each framework, the authors depicted the prescribed architecture, the necessity of implementing third-party applications, the relevant hardware or equipment, and security features. Neshenko et al. (2019) have performed survey of vulnerabilities in internet-level IoT. Farris et al. (2019) have analyzed security measures introduced by SDN and NFV to reshape the protection systems of IoT describing the core strategies to supervise, protect, and respond against threats. Also compared these security approaches with the conventional approaches. Then discussed the open challenges on NFV and SDN based IoT security to assist future research. In Yu et al. (2018a) the corresponding authors have contrasted edge computing frameworks and the customary cloud frameworks to secure IoT infrastructure. Menegheilo et al. (2019) have discussed practical security threats against IoT gadgets. Yu et al. (2019a) have analyzed and compared different security elements of the IoT platforms to find out the gaps and make the IoT system more secure. Lin et al. (2017) have talked about the possibilities of fog computing-based IoT. A portion of the security issues identified with fog computing has additionally been talked about. Cho et al. (2019a) have discussed Blockchain-based security approaches for IoT. Chaabouni et al. (2019) have performed an analysis of the IoT NIDS (Network Intrusion Detection Systems). They have analyzed several relevant tools and data sets as well as open-source network sniffing software. Then the work surveys several NIDS proposals on IoT in terms of architecture, detection procedures, validation techniques, and algorithms incorporated in those systems. It also analyzed both traditional and ML-based NIDS's. In this work Tschofenig et al. (2019) a survey has been performed on the internet protocol suite for IoT security. Ngu et al. (2017) have performed an analysis on issues and enabling technologies of IoT middleware also analyzed the capabilities of the current middleware and adaptability and security aspects in the IoT system. Benkhelifa et al. (2018) have performed an inclusive review of the IDS (Intrusion Detection Systems) for IoT focusing on design architecture. A proposition for future research on IDS is presented and evaluated as well. The work has included suggestions to develop a secure and optimized intrusion detection system for IoT also. Carracedo et al. (2018) have performed a survey on the utilization of cryptography for security assurance in IoT. Xie et al. (2019) have classified threats against WSN (Wireless Sensor Networks) dependent on the protocol stack. The work also researched on attack detection approaches by observing mainstream attacks. Then elaborated core advantages and drawbacks of current detection approaches and highlighted problems. The authors have finished their work by defining further research grounds. This work Borgohain et al. (2015) mostly specifies the Denial of Service (DoS) assaults on different layers of WSN and some security vulnerabilities in RFID. It doesn't give instances of such assaults representing the vulnerabilities exploited and lacks the recommendation of security assurance efforts against the referenced assaults. Corresponding authors in Granjal et al. (2015), likewise briefly examine the security issues in IoT focusing on some open issues. The article comprehensively covers a portion of the generalized security issues including inner and outer attacks, DoS attacks, physical threats, and so on. Authors likewise feature a portion of privacy and security challenges to IoT, for example, client security, authentication, trust management, access control, and authorization. Hou et al. (2019) performed an analysis of IoT security from the data perspective, summarized challenges and issues, and suggested several directions for future research. In this work Jing et al. (2014), the authors represented an IoT security framework involving three layers: perception, transport, and the application layer. Samaila et al. (2018) have elaborated issues of securing IoT gadgets. El-Hajj et al. (2019) have surveyed on authentication schemes for IoT. Das et al. (2018) analyzed security protocols for IoT and discuss their taxonomy. Since numerous reviews and survey articles such as Zhou et al. (2019a), Thakore et al. (2019), Noor et al. (2018b), Hamamreh et al. (2019) and Lu et al. (2019) have been published to put an overview on

Table 1
Considered literature and research topics.

Authors	Research Topic
Cerny et al. (2018)	The management of identity, authorization, and authentication in terms of the application layer.
Yang et al. (2017)	Issues regarding security in IoT applications.
Hu et al. (2020)	IoT data provenance
Chen et al. (2017)	Security issues explicit to location-aware services in IoT
Aufner (2019)	Security gaps on common threat models designed for IoT.
Noor et al. (2018a)	Reviewed ongoing IoT security research
Ammar et al. (2018)	Privacy issues of the primary IoT frameworks
Neshenko et al. (2019)	Vulnerabilities and exploitations on internet-level IoT
Farris et al. (2019)	SDN and NFV based protection systems for IoT
Yu et al. (2018a)	Edge computing to secure IoT infrastructure
Menegheilo et al. (2019)	Practical security threats against IoT devices
Yu et al. (2019a)	Security elements of the IoT platforms
Lin et al. (2017)	Fog computing-based secure IoT
Cho et al. (2019a)	Blockchain-based security approaches for IoT
Chaabouni et al. (2019)	Machine learning-based IoT network intrusion detection systems
Tschofenig et al. (2019)	Internet protocol suite for IoT security
Ngu et al. (2017)	Issues and enabling technologies of IoT middleware
Benkhelifa et al. (2018)	IDS (Intrusion Detection Systems) for IoT focusing on design architecture
Carracedo et al. (2018)	Cryptography for security assurance in IoT
Xie et al. (2019)	Threats against WSN dependent on the protocol stack
Borgohain et al. (2015)	Denial of Service (DoS) assaults on different layers of WSN and security vulnerabilities in RFID
Granjal et al. (2015)	Privacy and security challenges to IoT
Hou et al. (2019)	IoT security from the data perspective
Jing et al. (2014)	IoT security framework involving three layer architecture
Samaila et al. (2018)	Issues of securing IoT gadgets
El-Hajj et al. (2019)	Authentication schemes for IoT
Das et al. (2018)	Analyzed security protocols for IoT and discusses their taxonomy

the issues regarding IoT security. However, they are unable to put focus on the overall issues of IoT security. A portion of the present work centers on a couple of viewpoints and leaves the rest. This paper will help the audience gain deep information and insight into cutting edge IoT protection and offer them a deeper understanding of the subject. In the following section the key contributions of this work are added:

- The classification of various IoT applications and explicit privacy and security issues identified with those applications.
- Provided a significant explanation of complex security origins in various IoT layers.
- Detailed and concrete recommendations for expanding the IoT architecture to facilitate safe contact.
- Reviewed the safety enhancement methods introduced to address IoT security problems.
- An evaluation of the available problems, challenges, and directions for research to build stable IoT applications.

The table (Table 2) below will summarize the related works and the contribution of this work.

Novel Contribution of This Work: There are many reviews and surveys regarding IoT security in many scholarly research databases. They have quite similar kinds of review or survey papers like this work. But this work has extended the research on IoT security concept by incorporating the following terms review of ongoing IoT security research, review of intrusion detection mechanisms, application-layer security, middleware security, network layer security, gateway security, sensing layer security, threat modeling, details of vulnerable IoT architecture, privacy issues in IoT framework, vulnerabilities of Internet IoT, vulnerable IoT applications, security threats against IoT gadgets and applications, security in location-aware IoT, cryptography based security, machine learning-based IoT security, fog computing-based security, edge computing-based security, client security, authentication, trust, access control, authorization, detail security framework, challenges, issues, and future. Most importantly the previous researches such as reviews and surveys do not cover all of those topics. Moreover, this work has given a broader elaboration of the aforementioned topics which is not available in most of the previous works. Another important matter is that the research is performed based on the very recent articles (2014–2020) published on the IoT security concept.

3. IoT elements

The realization of the IoT infrastructure assists to obtain superior knowledge into the genuine importance and usefulness of the IoT. In this segment, the work will talk about the core components of the IoT.

3.1. Identification

Recognition is urgent for the IoT to name and match administrations with their interest. Numerous recognition strategies are accessible for the IoT, for example, EPC (electronic item codes) and uCode (ubiquitous codes) (Meng et al., 2019). Addressing the IoT artifacts is often important to distinguish the entity ID from its position. Item or system ID eludes its tag, for example, Temp1 refers to its position in a communications network for a particular temperature sensor and the position of an entity. In comparison, IPv4 (Skoberne et al., 2014) and IPv6 (Al-Ani et al., 2020) implement addressing approaches for IoT artifacts. 6LoWPAN (Al-Kaseem et al., 2019) enables the method of compression over IPv6 headers which allows IPv6 addressing suitable for remote low power systems. Recognition and address-separation of artifacts are important because the recognition methods are not all-around new, but addressing allows the identification of objects in a fascinating way. Besides, artifacts or machines inside the network can be using open, not proprietary, IPs. Recognition techniques are used to ensure that any item within the device has a correct identity.

3.2. Sensing

IoT detection or sensing requires gathering information from similar instruments within the network and transmitting it to a delivery center, archive, or cloud for details. The gathered information is broke down to take explicit activities depending on the required services. The IoT sensing systems can incorporate intelligent sensors, actuators, and wearable detecting gadgets. For instance, organizations such as like-Wemo, revolv, and SmartThings offer versatile applications that empower individuals to screen and control a large number of smart and intelligent gadgets and apparatuses inside buildings utilizing their cell phones (Ayaz et al., 2018; Liu et al., 2019a). Single-board computers (SBCs) (Da Rocha et al., 2019) equipped with sensors and tacit TCP/IP (Ahmad et al., 2019) and authentication protocols are widely used to identify IoT devices (for instance, Arduino Super, Arduino Uno, Raspberry PI, BeagleBone Black, and so on). Generally, these gadgets are interfaced with a central administration to provide the clients with the requisite details.

3.3. Communication

Heterogeneous apps work along with the IoT connectivity technologies to communicate specific cognitive resources. The IoT nodes usually operate using low power from the point of view of failure and disruptive communication links. Communication standard instances used by IoT include Bluetooth (Albazrqaoe et al., 2019), IEEE 802.11 b/g/n (Costa et al., 2019), IEEE 802.15.4 (Cao et al., 2015), Z-Wave (Qu et al., 2016), and LTE-A (Zheng et al., 2019). Many specific developments in networking are often included, such as RFID (Wang et al., 2019a), NFC (Zhao et al., 2017), and UWB (ultra-wideband) (Rahman et al., 2020) networks. RFID is the primary tool used to grasp the concept of M2M. The RFID tag is usually a simple chip that is added to items to provide identification. The reader produces a request signal for the tag and collects the mirrored signal from the object, which is passed to the database as a result. The database partners with a processing end to identify artifacts inside a (10 cm–200 m) expanse based on the reflected signals. RFID tags can be active, passive, or semi-active. The NFC agreement operates at high frequency (13.56 MHz), which allows up to 424 kbps of data transmission. The successful range is up to 10 cm where there growing to be communication between the readers and tags. The UWB connectivity is intended to assist interchanges within a limited range utilizing low energy and high bandwidth capacities which recently extended to sensors. Another networking system is IEEE 802.11 or commonly known as WiFi, which utilizes radio waves to transmit information within 100 m. WiFi helps sophisticated devices to transmit and exchange knowledge in specifically defined or ad-hoc systems without requiring a router. Bluetooth represents a networking system that is used to exchange knowledge between devices over short separations, utilizing low frequency to minimize the usage of resources. Recently, the Bluetooth special interest group (SIG) delivered Bluetooth 4.1 that gives BLE (Bluetooth Low Energy), which is faster than previous versions and supports IP connectivity to help IoT. The IEEE 802.15.4 specifies both a physical layer and MAC (medium access control) for low power wireless systems focusing on reliable and adaptable interchanges. LTE (Long--Term Evolution) is nowadays a standard cellular communication technology for fast data transfer between cell phones dependent on GSM/UMTS technologies. It can cover quick voyaging gadgets and give broadcasting and multicasting services. LTE-A (LTE Advanced) is an improved rendition of LTE including bandwidth capacity expansion which supports up to 100 MHz, uplink and downlink spatial multiplexing, expanded inclusion, higher throughput, and lower latency. Fig. 4 will show IoT communication protocols and frameworks.

3.4. Computation

Computational units (e.g., microcontrollers, microchips, SOCs,

Table 2
Relevant works and Contribution of this work.

Topics	This Work	Cerny et al. (2018)	Yang et al. (2017)	Hu et al. (2020)	Chen et al. (2017)	Aufner, (2019)	Noor et al. (2018a)	Ammar et al. (2018)	Neshenko et al. (2019)	Farris et al. (2019)	Yu et al. (2018a)	Menegheilo et al. (2019)	Yu et al. (2019a)	Lin et al. (2017)	Cho et al. (2019a)	Chaabouni et al. (2019)	Tschofenig et al. (2019)
Review of ongoing IoT security research	✓						✓				✓						
Review of intrusion detection mechanisms	✓			✓									✓			✓	
Application layer security	✓	✓															
Middleware security	✓																
Network layer security	✓																
Gateway security	✓																
Sensing layer security	✓																
Threat modeling	✓				✓	✓										✓	
Details of vulnerable IoT architecture	✓										✓						
Privacy issues in IoT framework	✓							✓									
Vulnerabilities of Internet IoT	✓								✓								✓
Vulnerable IoT applications	✓		✓														
Security threats against IoT gadgets and applications	✓											✓					
Security in location-aware IoT	✓			✓													
SDN NFV based IoT security	×									✓							
Blockchain-based security	×														✓		
Cryptography-based security	✓																
Machine Learning-based security	✓															✓	
Fog Computing-based security	✓													✓			
Edge Computing-based security	✓										✓						
Hardware-based security	×																
Internet protocol suite for secure IoT	×																✓
Client security	✓		✓				✓		✓							✓	
Authentication	✓		✓		✓								✓	✓			
Trust	✓												✓				

(*continued on next page*)

Table 2 (*continued*)

Topics	This Work	Cerny et al. (2018)	Yang et al. (2017)	Hu et al. (2020)	Chen et al. (2017)	Aufner, (2019)	Noor et al. (2018a)	Ammar et al. (2018)	Neshenko et al. (2019)	Farris et al. (2019)	Yu et al. (2018a)	Menegheilo et al. (2019)	Yu et al. (2019a)	Lin et al. (2017)	Cho et al. (2019a)	Chaabouni et al. (2019)	Tschofenig et al. (2019)
Access control	✓			✓													
Authorization	✓							✓			✓						
Detail security framework	✓												✓				
Communication and computations overheads	✓																
Challenges, Issues, and Future	✓					✓						✓					✓

Topics	This Work	Ngu et al. (2017)	Benkhelifa et al. (2018)	Carracedo et al. (2018)	Xie et al. (2019)	Borgohain et al. (2015)	Granjal et al. (2015)	Hou et al. (2019)	Jing et al. (2014)	Samaila et al. (2018)	El-Hajj et al. (2019)	Das et al. (2018)
Review of ongoing IoT security research	✓							✓		✓	✓	✓
Review of intrusion detection mechanisms	✓		✓									
Application layer security	✓										✓	
Middleware security	✓	✓										
Network layer security	✓										✓	
Gateway security	✓											
Sensing layer security	✓										✓	
Threat modeling	✓								✓	✓		✓
Details of vulnerable IoT architecture	✓									✓	✓	✓
Privacy issues in IoT framework	✓					✓	✓	✓		✓	✓	
Vulnerabilities of Internet IoT	✓			✓								
Vulnerable IoT applications	✓			✓				✓		✓	✓	
Security threats against IoT gadgets and applications	✓				✓				✓		✓	
Security in location-aware IoT	✓											
SDN NFV based IoT security	×											
Blockchain-based security	×											
Cryptography-based security	✓			✓						✓		✓
Machine Learning-based security	✓											
Fog Computing-based security	✓											
Edge Computing-based security	✓											
Hardware-based security	×									✓		
Internet protocol suite for secure IoT	×											
Client security	✓						✓					
Authentication	✓						✓			✓		✓
Trust	✓						✓			✓		✓
Access control	✓						✓			✓		✓
Authorization	✓											✓
Detail security framework	✓								✓			
Communication and computations overheads	✓									✓	✓	
Challenges, Issues, and Future	✓							✓		✓		✓

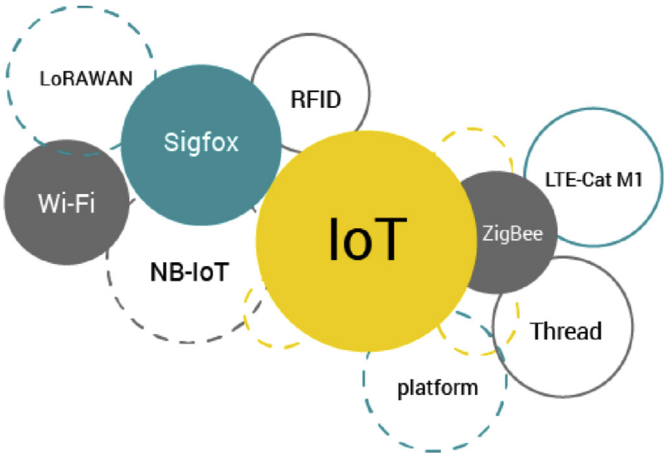

Fig. 4. IoT communication protocols and frameworks.

FPGAs), and programming programs reflect the IoT's knowledge and computational ability. For instance, Arduino, Raspberry PI, STM Series, UDOO, Intel Galileo, FriendlyARM, BeagleBone, Gadgeteer, and T-Mote Sky, numerous equipment platforms were developed to operate IoT applications. Additionally, various devices or computerized systems are used to include IoT functionality. Operating Systems are invaluable to computing platforms because they execute a gadget for the entire enactment period. There are a few Real-Time Operating Systems (RTOS) which are an appropriate candidate for RTOS-aided IoT applications to progress. The Contiki RTOS, for example, has been used widely in IoT infrastructures. Contiki has a test program named Cooja that enables the replication and imitation of IoT and WSN (Yıldırım et al., 2018) or WSAN applications by specialists and designers (Ma et al., 2018). Additionally, TinyOS (Amjad et al., 2016), Riot OS (Baccelli et al., 2018), and LiteOS (Takahashi et al., 2009) deliver lightweight IoT solutions. Besides, several Google-based automobile industry pioneers set up the OAA (Open Car Alliance) are planning to introduce new highlights to Smartphone networks to promote the Internet of Vehicles (IoV) concept's appropriation (Chang et al., 2019). Cloud Systems are just another critical IoT computing field. These systems promote smart devices for transmitting data to the web, for continuous processing of large data, and finally for end-clients to get the greatest value from the knowledge derived from the massive amount of information collected. There are tons of free, business-oriented cloud infrastructure and available sites to host IoT services.

4. Security vulnerable applications of IoT

For all IoT applications that have either been communicated or are moving towards implementation, protection is a vital issue. IoT applications are increasingly growing and reaching a greater portion of today's companies. Although service providers are enabling such IoT apps through recent networking advancements, some of these apps require even more robust protection help from the technologies they use. Various IoT implementations are discussed in this segment in which protection is an apparent and essential requirement.

Smart Cities: Smart cities require the widespread usage of growing computer and networking technology to improve individuals' overall personal satisfaction. It incorporates shrewd homes, savvy traffic management, intelligent calamity management, smart utilities, and so on. There is a push to make urban areas more astute, and governments overall are empowering their advancement through different incentives (Kolozali et al., 2019). Although the usage of smart apps is supposed to improve the residents' happiness, it is followed by a challenge to the residents' privacy. Smart card services will threaten the resident's card subtleties and purchasing behavior. Intelligent portability technologies may leak consumer locations. Several applications are utilizing which guardians can monitor their children. However, if such kinds of applications are under attack, then the privacy and security of the children can face a huge threat (Mohammad, 2019). Fig. 5 will illustrate a smart city.

The figure (Fig. 6) shows the IoT analytics for a smart city.

Smart Home: Smart home (Wang et al., 2018) application of IoT contribute to upgrading the individual way of life by making it simpler and progressively helpful to screen and operate home apparatuses and frameworks (e.g., An HVAC control system, environment monitoring frameworks, energy meters, and so on.) remotely. For instance, a smart home is capable of opening and closing the windows depending on the data gathered by monitoring the surrounding environment automatically. Savvy homes are required to have standard interaction with their internal and external condition of the environment (Kumar et al., 2017a). The internal condition of the environment may incorporate all the home apparatuses and gadgets that are Internet-associated while the outer environment comprises objects that are not in control of the smart home system, for example, smart grid elements. Fig. 7 will visualize an IoT-based smart home.

Smart Environment Monitoring: A shrewd environment observation system incorporates different IoT applications, for example, fire recognition in forests, evaluation of snow rates in high altitude regions, forestalling avalanches, early detection of quakes, evaluation of contaminants, and so on. Each of these IoT technologies applied to humans and animals residing in certain territories. Similarly, data from these IoT providers will be used by regulatory bodies dealing with such industries. For any area associated with these IoT technologies, security weakness may have significant implications. False positives and false negatives in this sense will cause appalling outcomes for these IoT services. For instance, if the program continues to wrongly identify quakes, then it would cause budgetary losses for the government and organizations at that level. When the code cannot predict the quake, it would cause the destruction of all properties and existence. Subsequently, devices to track

Fig. 5. A smart city.

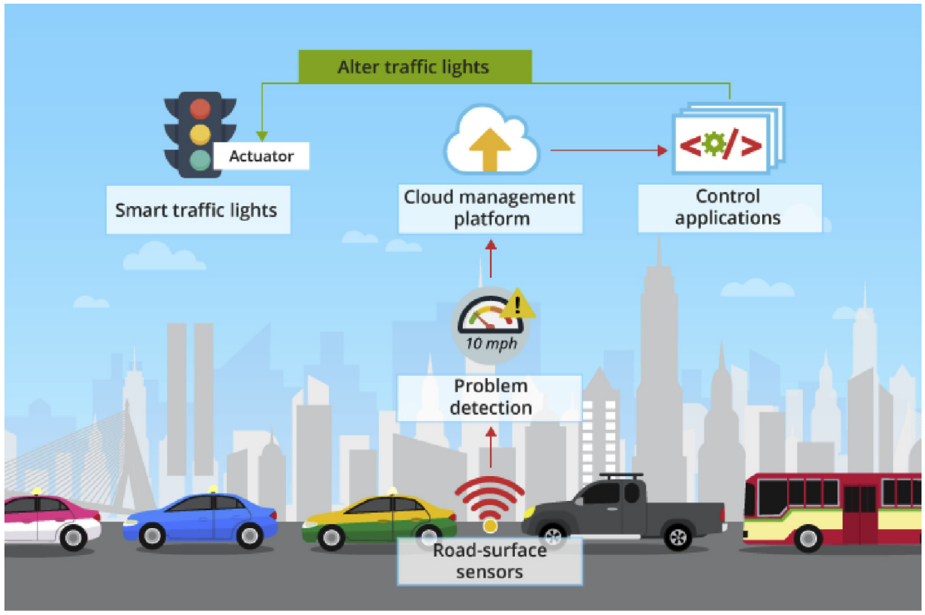

Fig. 6. IoT analytics for smart city.

the smart world must be incredibly accurate and attempts at security attacks and altering of information must be avoided (Sung et al., 2013).

Intelligent Transportation: Smart transportation frameworks represent coordination among communication and computation to screen and control the transportation system (Dey et al., 2015). The system means to accomplish unwavering quality, effectiveness, accessibility, and enhancement of the transportation infrastructure. It utilizes four primary segments, in particular: vehicle sub-system (comprises of GPS, RFID, OBU, and communication devices), station sub-system (street side hardware), monitoring, and security assurance sub-system. Also, connected vehicles are getting increasingly significant with the means to make driving progressively reliable, secure, and productive. For example, Audi turned into the main automaker with a permit for self-driving in Nevada. Google is another pioneer in this sector. Likewise, in December 2013, Volvo declared its self-driving vehicle to travel around 30 miles in occupied streets in Gothenburg, Sweden. Recently, the USDOT declared that it would graph an administrative path that would require every new vehicle to be deployed with V2V (vehicle-to-vehicle) communications frameworks in the following years (Wei et al., 2019). Fig. 8 visualizes intelligent transportation equipped with IoT.

Smart Metering and Smart Grid: Smart metering incorporates services relevant to different estimation, observation, and management. The well-known application of smart or clever metering is smart grids, where it measures and tracks electricity usage. Smart metering can also be used to counter the power theft issue (Liu et al., 2015). Different forms of shrewd or clever metering use include water, oil, and gas volumes found in tanks and reservoirs. Smart meters are often used to track and optimize the view of solar power plants by automatically changing the edge of solar panels to harvest the highest possible amount of solar energy. Many IoT apps still exist that use smart metering technologies to calculate water pressure in water transport systems or to determine liquid weight. Nonetheless, as compared with traditional meters, smart metering systems are ineffective against both physical and remote or electronic threats or assaults that can only be changed by a physical attack. A smart metering system is also designed to conduct outside traditional monitoring of energy use. Both electrical gears at home are connected with smart meters in an adaptive home area network (HAN), and the data obtained from these forms of gears may be used for device costs and load control. Deliberate interference by clients or an adversary in these communication contexts can modify the data collected, resulting in a financial loss to service organizations or clients (Ghosal et al., 2019). Fig. 9 will show the concept of a smart grid incorporating IoT.

Industrial Automation: Industrial automation or computerization (Lo Bello et al., 2019) is automating gadgets to finish production steps

Fig. 7. Smart home.

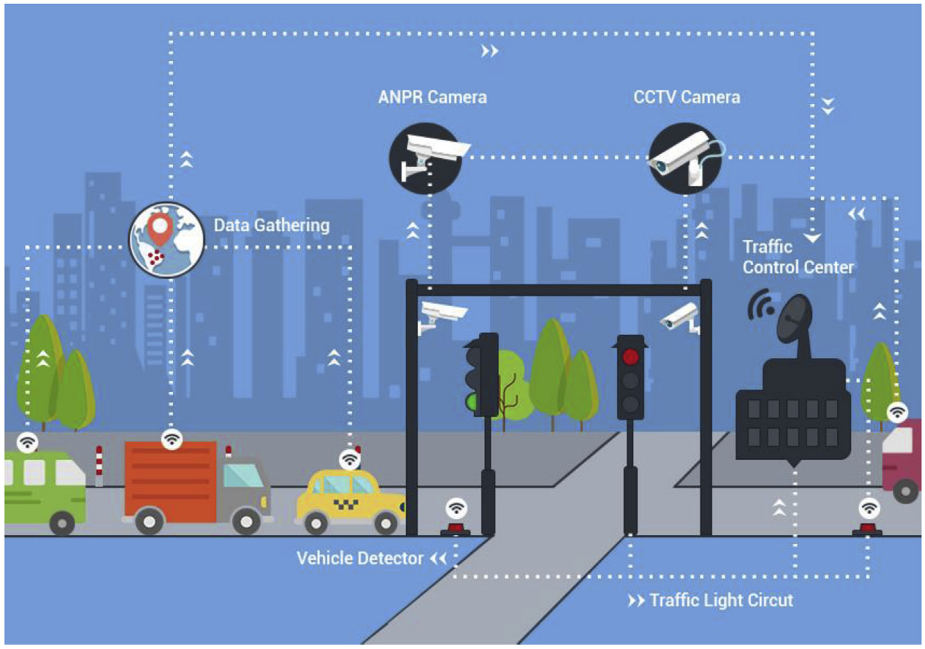

Fig. 8. Smart transportation.

with an insignificant human contribution. It permits machines to create items rapidly and more precisely depending on four components: transportation, handling, detecting, and communication. The IoT is used in industrial computerization (automation) to control and screen production machinery and their functionalities, and productivity rate via the Internet. For example, if a specific production machine experiences an unexpected issue, an IoT framework sends an emergency maintenance request promptly to the maintenance staff to deal with the issue. Besides, the IoT builds efficiency by examining production data, and different reasons for production issues. The figure (Fig. 10) will show an illustration of industrial automation.

Security and Emergencies: Security and crises are significant sectors where different IoT applications are being conveyed. It incorporates applications, for example, permitting approved individuals accessing in confined zones and so on. Another function is the identification of spillage of toxic gasses in agricultural areas or processing facilities for pharmaceutical manufacturing. In the regions surrounding atomic reactors or cellular base stations, radiation levels may often be measured, and alarms can be produced when the radiation level is high. Technology programs may be distributed to protected computers and confidential details. Similarly, authentication breaches in these systems may have various severe implications. The offenders, for example, may seek to access the restricted territories by exploiting the weaknesses in these applications. False cautions on the amount of radiation may often have

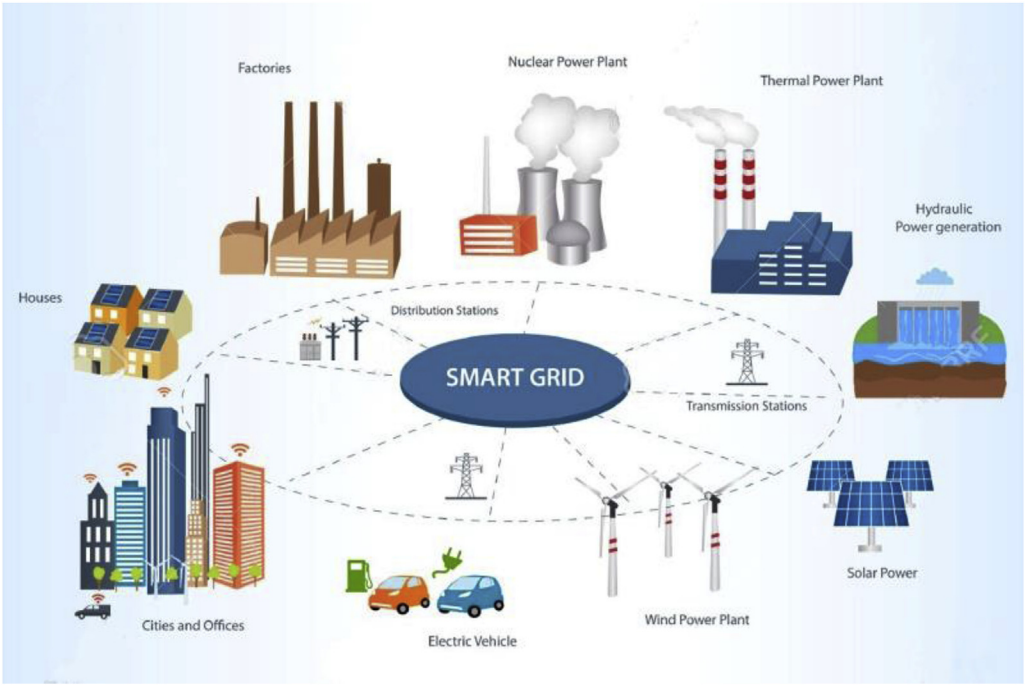

Fig. 9. Smart grid.

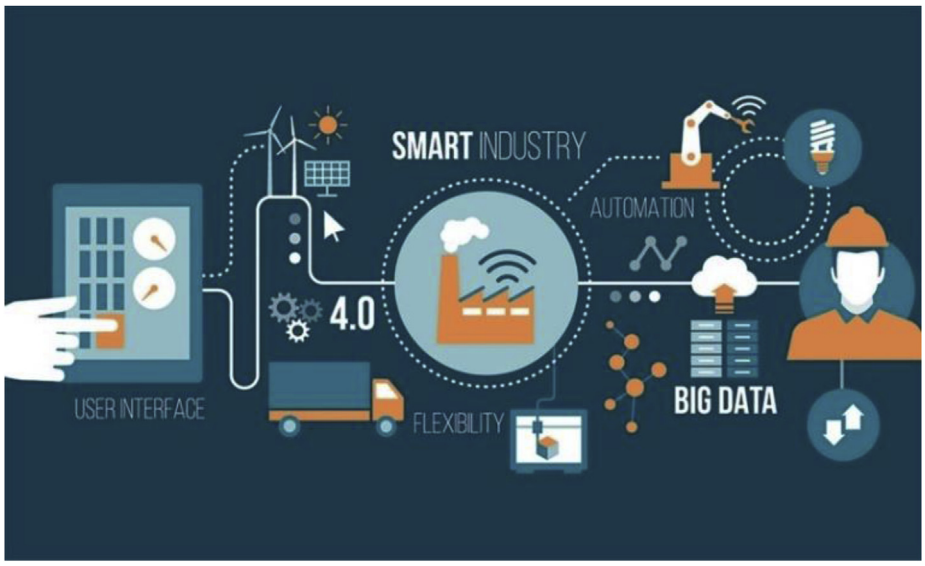

Fig. 10. Industrial automation.

immediate and long haul impacts. For starters, if unborn babies are exposed to high radiation rates, this may cause dangerous long-term illnesses.

Smart healthcare: Smart healthcare (Amin et al., 2019) or e-healthcare assumes a noteworthy job in healthcare services through attaching sensors and actuators into the patients and their medication for observation and tracking purposes. The IoT is utilized by clinical consideration to screen the physiological conditions of patients through sensors by gathering and dissecting their data and afterward sending the information remotely to processing centers to take necessary steps. For instance, Masimo Radical-7 screens the patient's status remotely and reports that to medical personnel. IBM used RFID at one of OhioHealth's medical clinics to track handwashing after observing every patient (Wang et al., 2019a; Alabdulatif et al., 2019). That activity could be utilized to avoid diseases that cause around 90,000 deaths and losing about $30 billion every year. Fig. 11 visualizes an illustration of smart healthcare or e-healthcare based on IoT.

Smart Retail: IoT services are nowadays broadly utilized in the retail sector. Specific IoT tools were developed to track the product's capability status as they travel through the development chain. IoT is often used to screen products in fulfillment centers so that restocking will preferably be feasible. Different shopping applications are likewise being created to support the clients depending on their inclinations, propensities, hypersensitivities to specific components, and so forth. Several companies, in conveying and using various IoT applications, have faced protection problems. A few of these organizations incorporate Apple, JP Morgan Chase, Home Depot, and Sony. Cyber-enemies may attempt to undermine the IoT resources relevant to the product's capability status and may attempt to provide consumers with inaccurate data regarding products to increase the selling. If protection principles are not changed in a smart retail environment, assailants can capture credit and debit card records, mobile phone numbers, email addresses, and so on from consumers that can result in financial losses to consumers and retailers (Xiao et al., 2018a). Fig. 12 shows smart retail services.

Smart Agriculture: Intelligent farming incorporates observing soil moisture, pH monitoring, controlling micro-level atmospheric conditions, irrigation system, and controlling temperature and humidity. Utilization of such advanced technologies in horticulture can assist in accomplishing higher crop productivity and can spare ranchers from financial losses. Regulation of temperature and moisture rates in the processing of different grains and vegetables may help avoid fungal infections and other microbial pollutants. Regulation of the environment will also help to improve the yield and consistency of the crops and harvests. As with harvest monitoring, IoT apps are possible to track livestock behaviors and well-being by adding sensors to the animals. If these resources are compromised, an animal burglar from the ranch may be spurred and enemies can also damage the harvest (Ayaz et al., 2019). Fig. 13 will illustrate smart farming concepts.

Fig. 11. An illustration on e-healthcare based on IoT.

Fig. 12. Smart retail.

5. IoT standards and protocols

Numerous IoT standards are proposed to encourage and streamline application software engineers and specialist roles. Various groups have been formed to develop protocols for IoT services including endeavors drove by the W3C, IETF, IEEE, and ETSI. In this work, the author characterizes the IoT protocols into two classes, to be specific: application protocols, and service revelation protocols. However, it is not mandatory that, these protocols must be packaged together to convey a given IoT application. Also, because of the idea of the IoT service, a few models may not be required to be included in a service. In the accompanying subsections, the author has introduced an outline of a few of the protocols in these classes and their core functionalities (Palattella et al., 2013; Aijaz et al., 2015; Tomić et al., 2017a).

5.1. Application protocols

Constrained Application Protocol (CoAP): Working associates of the IETF's CoRE (Constrained RESTful Environments) have built CoAP, an IoT device layer protocol. The CoAP characterizes a REST (REpresentational State Transfer) based network transfer convention or protocol on HTTP functionalities. REST is concerned with a less complicated solution to sharing details between clients and servers over HTTP. REST can be described as a cacheable communication protocol that depends on the design of a stateless client-server. It is used in casual network apps as well as in mobile phones and by utilizing HTTP post, get, put, and erase strategies it strips away vagueness. REST empowers servers and clients to uncover and devour web-based services such as the SOAP (Simple Object Access Protocol) yet in a simpler way utilizing URIs (Uniform Resource Identifiers) and HTTP get, post, put, and delete techniques. REST is not dependent on XML for message trades. Unlike Others, CoAP is built as a matter of course on UDP (not TCP) which makes it increasingly suitable for the IoT services. In turn, CoAP modifies certain HTTP functionalities to satisfy the IoT requirements, such as low power consumption and operation in error and disruptive links. Because CoAP is designed dependent on REST; the transition in REST-CoAP intermediaries between those protocols is direct (Chander et al., 2012; Garcia-Carrillo et al., 2018). The overall functionality of the CoAP protocol is demonstrated in Fig. 14.

Message Queue Telemetry Transport (MQTT): MQTT is a kind of message protocol that was designed by Andy Stanford-Clark a technologist of IBM and Arlen Nipper from Arcom (presently Eurotech) in 1999 and was institutionalized in 2013 at OASIS (Amin et al., 2019). MQTT targets interfacing embedded gadgets and systems with applications and middleware. The connection activity utilizes a routing technique (one--to-one, one-to-many, many-to-many) and empowers MQTT as an ideal protocol for the IoT and M2M. MQTT uses the publish-and-subscribe technique to ensure adaptability and simplicity of execution as portrayed in Fig. 15. Likewise, MQTT is reasonable for resource compelled gadgets that utilize untrustworthy or low bandwidth connections. MQTT is based on the TCP. It conveys messages through three degrees of QoS. Two significant determinations exist for MQTT: MQTT v3.1 and MQTT-SN (once known as MQTT-S) V1.2. The last one was characterized explicitly for sensor networks and characterizes a UDP-mapping technique of MQTT and includes broker assistance for ordering subject names. The specifications introduce three components: connection semantics, packet routing, and endpoint. MQTT comprises of three elements, message publisher, subscriber, and a broker. An intrigued gadget would enroll as a subscriber for explicit subjects with the end goal for it to be informed by the broker when publishers distribute subjects of intrigue. The publisher performs as a generator of intriguing information. Then, the publisher sends the information to the intrigued elements (endorsers) via the broker. Moreover, the broker accomplishes security by checking the approval of the publishers and the subscribers (Refaey et al., 2019; Quincozes et al., 2019). Various IoT services use the MQTT,

Fig. 13. Smart farming.

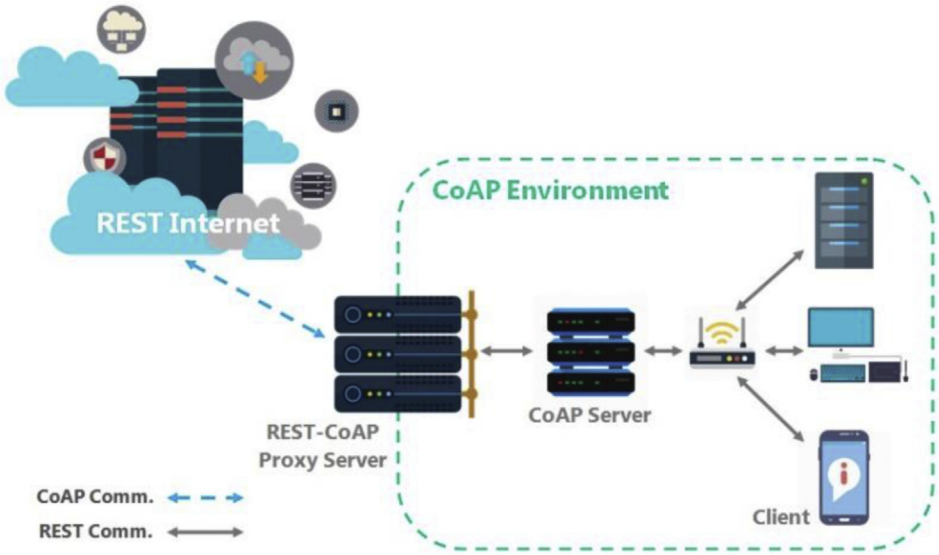

Fig. 14. CoAP protocol.

for example, health care, energy meter, and Facebook notification. Thusly, the MQTT represents a perfect messaging convention for the IoT and M2M interchanges and can provide routing to little, modest, low power, and low memory gadgets in vulnerable and low bandwidth systems.

Fig. 16 shows an analytics based MQTT protocol illustration.

Extensible Messaging and Presence Protocol (XMPP): XMPP is an IETF messaging interface used for multi-user talking, voice calls, and video communication. The Jabber developed XMPP to assist in a free, stable, and unified messaging model. XMPP helps clients to connect with each other by transmitting messages across the Internet irrespective of the application they are using. XMPP permits instant messaging applications to accomplish validation, access control, security estimation, end-to-end privacy, and compatibility with different conventions. Fig. 17 shows the architecture of the XMPP protocol. Numerous XMPP features lead it a favored protocol by most instant messaging services and important within the extent of the IoT. It runs over an assortment of Internet-based platforms in a distributed manner. XMPP is secure and takes into account the expansion of new services on top of the central protocols (Cho et al., 2019b). XMPP associates a user to a server utilizing streams of XML stanzas. An XML stanza speaks to a bit of code that is isolated into three segments: message, presence, and iq (information/-query). Message stanzas distinguish the source and destination locations,

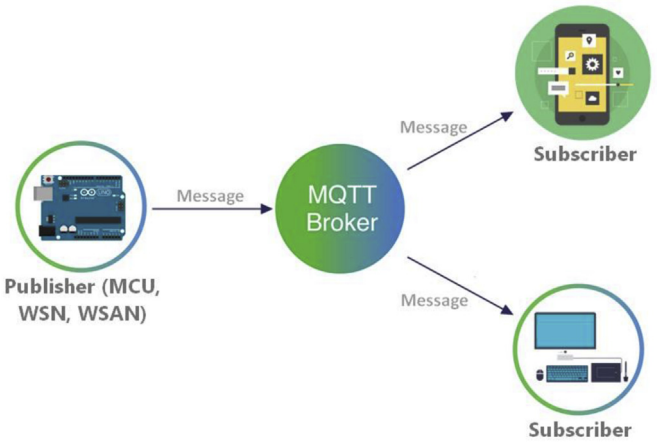

Fig. 15. Typical MQTT protocol.

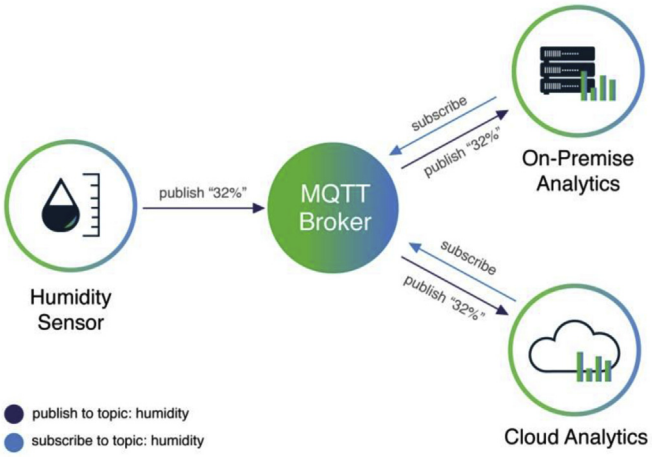

Fig. 16. Analytics based MQTT.

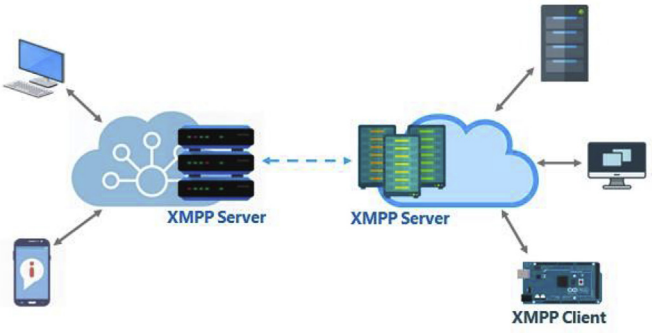

Fig. 17. Simplified architecture of XMPP.

types, and IDs of XMPP substances that use a push technique to retrieve information. The message stanza fills out the subject and body with the message title and substance. The presence stanza appears and informs clients of announcements as approved. The iq stanza establishes the sender and recipient of a letter. Throughout XMPP the content-based communication using XML introduces a high overhead method. One approach to this question is to pack XML streams using EXI as defined in

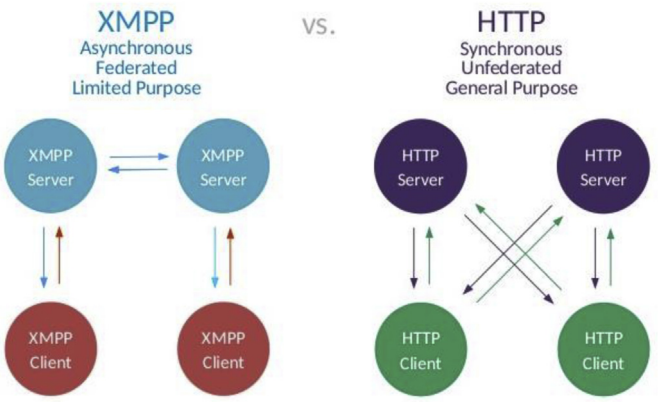

Fig. 18. XMPP vs. HTTP

Saint-Andre (2011) and Waher et al. (2013).

Fig. 18 will be more helpful for the better realization of XMPP protocol.

Advanced Message Queuing Protocol (AMQP): AMQP (Caiza et al., 2019) is an open-source application layer protocol for the IoT concentrating on message-oriented conditions. It ensures trustworthy communication utilizing message delivery assurance techniques, including at-least-once, at-most-once, and exactly-once delivery. AMQP needs a solid transport protocol such as TCP to trade messages. By characterizing a wire-level standard, AMQP can exchange messages with one another. Interchanges are taken care of by two primary components. Exchanges are responsible for ensuring communications are redirected to appropriate queues. Several pre-characterized rules rely on routing within exchanges and message queues. Data should be packed away in lines of communications and delivered to the receiver afterward. AMQP still promotes the publish-and-subscribe paradigm outside this form of end-to-end correspondence. AMQP characterizes the transport layer through a communications network. Within this row, Messaging abilities are taken care of. AMQP characterizes two kinds of communications: void messages received by the sender, and descriptions of communications available to the receiver. In Fig. 19, the arrangement of AMQP is indicated (Keophilavong et al., 2019). In this case, the header transmits the parameters like robustness, required time-to-live, first acquirer, and conveyance test. The transport layer protocols assure the necessary expansion points for the messaging layer. At this layer, data transfer is frame oriented. The structure of the AMQP outlines is delineated in Fig. 19. The initial four bytes represent the frame size. Data Offset ensures the situation of the body within the frame. The Type field demonstrates the organization and motivation of the frame.

5.2. Service revelation protocols

The high adaptability of the IoT needs a resource management framework that can enroll and find resources and services in a self-designed, proficient, and a dynamic way. The premier conventions in this area are multicast DNS (mDNS) and DNS Service Discovery (DNS-SD) that can find resources and services delivered by IoT gadgets. Even though these two conventions have been planned initially for resource-rich gadgets, studies and research are ongoing to design light versions of them for IoT services.

Multicast DNS (mDNS): For certain IoT programs a simple but necessary feature is Name Resolution protocol. mDNS is such a thing that the unicast DNS service errand will play (Walkowiak et al., 2011). mDNS is adaptable because DNS namespace is used locally without extra costs or arrangements. mDNS is a good choice for embedded gadgets, since a) there is no need for manual reconfiguration or extra gadget control organization; b) it can operate without a frame; c) it will continue to function if a malfunction occurs. mDNS inquires system names by submitting multicast IP messages to all attached nodes in the surrounding domain With this question; the client asks devices that have the name provided to respond back. When the target computer gets its name it multicasts an acknowledgment response comprising its IP addresses. All devices in the network that receive answer messages change their surrounding cache using the name and IP address allocated to them. An illustration where mDNS operation discovery is used can be seen in Kaiser et al. (2014).

DNS Service Discovery (DNS-SD): The pairing capability of necessary resources by mDNS-users is called DNS-based service discovery or disclosure (DNS-SD). Using this protocol, users will use regular DNS messages to check for several desired resources in a given program. DNS-SD as mDNS is a part of the nil configuration service for system interaction without external arrangement (Stolikj et al., 2014). DNS-SD uses mDNS to transmit packets of DNS over UDP to explicit multicast addresses. Processing Device Discovery has two primary steps: finding the hostname of the necessary facilities, for instance, printers combining IP addresses with their hostname using mDNS. Hostname exploration is critical because IP's can shift, while names don't. The Multicast Pairing mechanism provides network subtleties such as IP, port number, etc. to every specific host. Using DNS-SD, the system's case names can be held clear to the degree that trust can be increased and stability unwavering. For instance, once a few people already learn and use a specific printer, they would be encouraged to use it without difficulties from now on.

6. Layers in IoT architecture

The IoT tends to be capable of connecting multi-millions of heterogeneous gadgets over the internet. So there is a requirement for adaptable layered engineering. The constantly increasing number of models suggested has not yet unified with a reference model (Eldrandaly et al.,

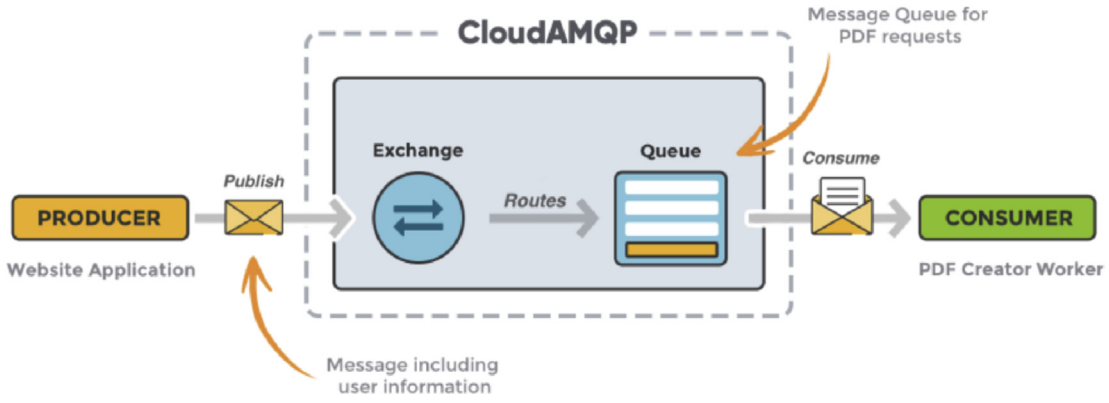

Fig. 19. AMQP protocol.

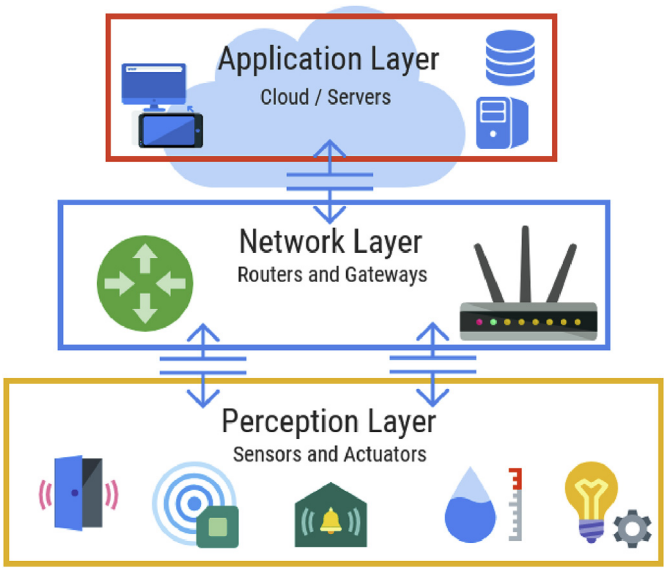

Fig. 20. 3-layer IoT architecture.

2019). Then, there are a few practices such as IoT-A (Silva et al., 2019) that seek to organize a traditional system based on analysts and market needs investigation. The fundamental paradigm is a 3-layer design (Bing, 2016; Wu et al., 2010; Kaur et al., 2017) composed of Application, Network, and Perception or Sensing Layers, from several proposed models. Recent studies have proposed several specific models that give more deliberation to the IoT architecture (Navani et al., 2017; Virat et al., 2018; Atzori et al., 2010). Fig. 20 delineates 3-layer architecture of IoT (Bing, 2016).

Fig. 21 visualizes the 7-layer architecture of IoT (Tietz, 2016).

This work has considered the most prominent and accepted 4-layer architecture (in Fig. 22).

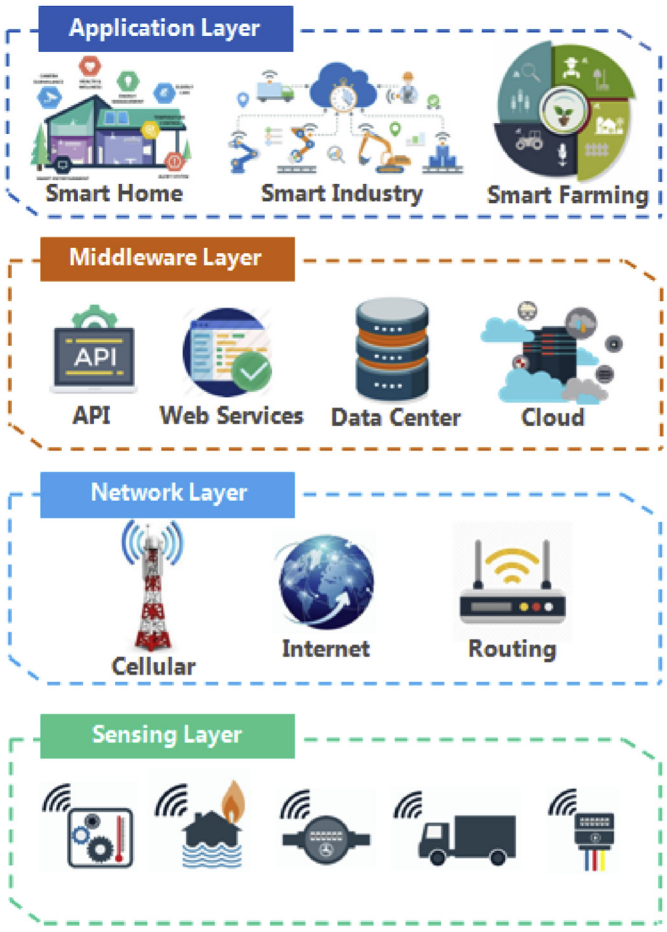

Fig. 22. IoT architecture (Typical).

6.1. *Object or sensing or perception or recognition layer*

The identification or perception layer refers to the IoT's internal sensors that require captured knowledge to be gathered and analyzed. This layer integrates sensors and actuators for performing various functionalities, such as inquiring field, temperature, strain, moisture, movement, acceleration, vibration, etc. Institutionalized plug-and-play systems should be utilized by this layer to design heterogeneous devices. The layer of perception or recognition digitizes and transfers knowledge through safe connections to the Subject Abstraction layer. At

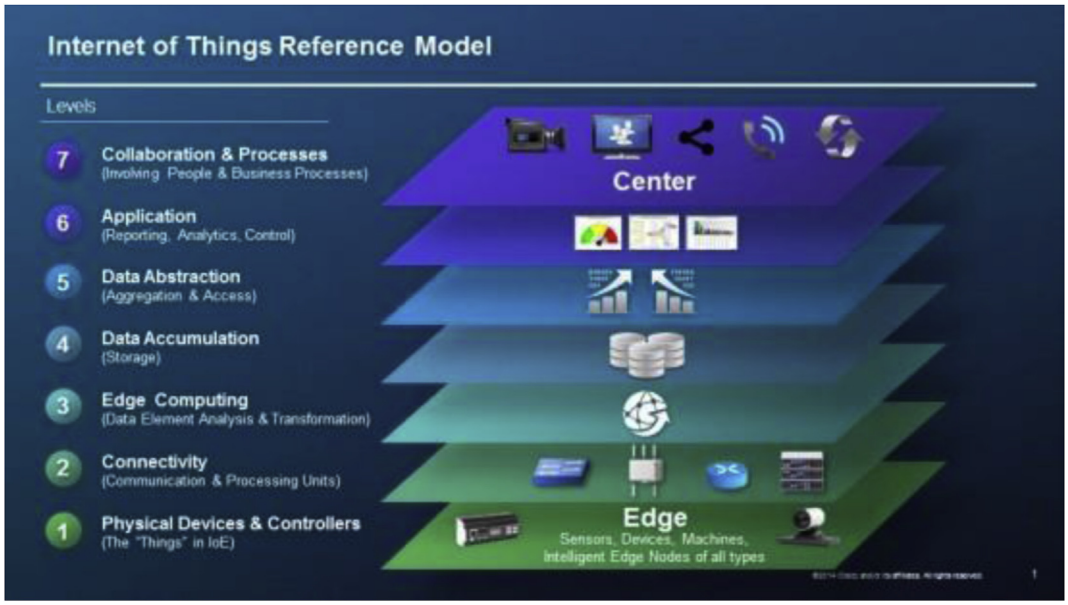

Fig. 21. 7-layer architecture.

this layer, the enormous data provided by the IoT is started (Jin et al., 2018).

6.2. Object abstraction or networking layer

Object abstraction layer transfers information generated by the perception layer through safe links to the Service Management layer. For example, data can be transferred through different technologies, such as RFID, GSM, 3G, UMTS, BLE, WiFi, ZigBee, etc. Besides, different technologies such as cloud computing and data processing are taken care of at this layer (Divarcı et al., 2018; Wang et al., 2019b).

6.3. Service Management or middleware layer

Service Orchestration or Middleware layer assist clients with necessary addresses and names. This layer empowers IoT application developers to deal with heterogeneous devices without thinking of a particular hardware platform. Additionally, this layer prepares the received information and performs necessary computation. After that conveys the necessary services over the network protocols (Joseph et al., 2017; Li et al., 2019a).

6.4. Application layer

The application or framework layer provides the types of support customers have listed. The framework layer, for example, will provide estimates of temperature and air humidity to the client who requests the detail. With the IoT, the importance of this network is that it will include top-notch, analytical applications to solve the concerns of customers. The application layer includes various vertical markets, for example, smart home, smart transportation, savvy building, industrial automation, and intelligent medical services (Tandale et al., 2017; Yassein et al., 2016).

7. Threat modeling frameworks

Modeling of threats is a procedure that recognizes, organizes, classifies, and rate threats depending on a detailed analysis of the architecture of a system. Recognizing such risks and evaluating them helps an individual to recognize the risks that present a significant danger for a company. Modeling threats helps implement a structured way to address the safety impact of enterprises. This is a simultaneous process that starts from the early stages of layered security design and continues all through the lifecycle of security (Popescul et al., 2014). Threat modeling begins with the collection of various kinds of data to produce a model appropriate for the gadget to be examined. The model for threats helps to identify a gadget or a framework's vulnerable areas that may be targeted (Torr, 2005). Modeling of threats can be used in the security designing lifecycle to ensure privacy and security by development rather than identifying it as a spare layer above components. A brief look at the versatility of these frameworks is provided in the forthcoming paragraphs.

STRIDE is the widely cited security framework. In the circumstance of the IoT, the work Seeam et al. (2019) used STRIDE as a threat model. Quantitative threat modeling was chosen mainly as a supportive addition to STRIDE, representing the innovation in the area of frameworks for threat modeling. STRIDE is a Microsoft-developed and optimized program for Security Development Lifecycle (SDL). STRIDE utilizes data-flow schemes that are created as a component of the SDL. These schemes are utilized for mappings to detect threats.

The term STRIDE stands for:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

CORAS is another framework frequently cited in research. E.g., in the sense of embedded networks (Vasilevskaya et al., 2016), this concept is introduced. This also refers to work on the health of connectivity between IoT gadgets and smartphones (Bhuyan et al., 2018). During software designing, CORAS operates through iterative processes between developers and analysts. CORAS differs from other existing frameworks, as it focuses on the concept that developers are distinct persons. The system or gadget under examination is illustrated by UML graphs, and CORAS graphs are developed in posterior steps. Different types of diagrams are used for this approach: UML graph, UML cooperation graph, and UML activity graph are such diagrams. The CORAS solution to multiple programs is more robust because it does not necessarily imply that particular risks are delegated to certain systems or their elements.

LINDDUN was selected by developers for its special attention to privacy. In the previous frameworks, security risks are mostly discussed, but privacy is emphasized in this framework compared to the other frameworks. The system was described as inappropriately relevant in a paper that sought to establish a theoretical data security structure for IoT (Perera et al., 2016). In the circumstance of the smart grid, however, LINDDUN was applied (Neureiter et al., 2013).

LINDDUN is classified as a framework for modeling privacy threats in software-oriented systems. LINDDUN is also a mapping scheme that presents potential threats by the data-flow graph, similar to STRIDE.

It classifies privacy threats with forthcoming terms:

- Linkability
- Identifiability
- Non-repudiation
- Detectability
- Disclosure of the information
- Unawareness
- Non-compliance

These are the most common frameworks used for modeling threats in IoT infrastructures.

8. Sources of the threats

Each IoT framework can be divided into four layers, as described in Section I: (1) sensing layer; (2) network layer; (3) middleware layer; and (4) network layer. Any of these layers in an IoT framework uses different technologies that carry with them many issues and threats to security. For these four levels, this segment addresses specific security vulnerabilities in IoT applications. Fig. 23 shows the possible cyber threats on these layers.

8.1. Security issues at sensing layer

Physical IoT sensors and actuators are primarily operated by the detecting or perception layer. Sensors feel the real magic that is occurring around them (Tukur et al., 2019). Actuators, then again, play out a specific activity on the physical condition, depending on the detected information. There are different sorts of sensors for detecting or collecting various sorts of information, e.g., camera sensors, ultrasonic sensors, fire and smoke identification sensors, temperature sensors, and so on. The physical state can be measured using visual, mechanical, thermal, or chemical sensors. Different advancements are used in various IoT applications such as GPS, WSANs, WSNs, RSNs, RFID, so on (Tomić et al., 2017b).

Significant security issues that can be emerged at the sensing layer are described below:

Node Capturing: IoT facilities provide, for example, a few low-power hubs, sensors, and actuators. These forms of IoT nodes are exposed by automated enemies (adversaries) to different styles of assaults. The

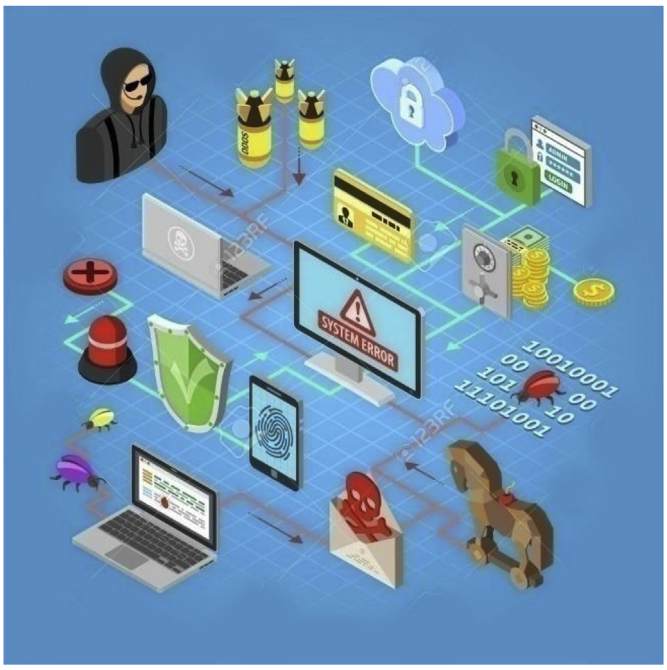

Fig. 23. Cyber assaults.

aggressors can attempt to use a pernicious or harmful node to catch or supplant the node in the IoT system. The new node will appear as a piece of the framework, however, is constrained by the cyber-aggressor. This may prompt trading off the security of the total IoT system (Lin et al., 2013).

Malicious Code Injection Attack: This form of attack involves the intruder inserting any malignant code into the node's memory. The software of IoT nodes is typically changed on the breeze, and this allows the assailants a path to infuse malicious code. Using these codes, cyber-criminals can compel nodes to conduct certain unintended activities or even attempt to access the IoT network as a whole (Ayeni et al., 2018).

False Data Injection Attack: The aggressor can use it when the node is caught to infuse false information into the IoT context. This will trigger false outcomes and can induce IoT program failure. Likewise, the cyber-assailant can use this strategy to perform a DDoS attack.

Side-Channel Attacks (SCA): Without direct assaults on nodes, numerous side-channel assaults can cause confidential information to spill out. Processor's micro-architecture, radio communication technologies, and their utilization of electricity reveal confidential details to cyber-attackers. Side-channel assaults might be founded on power utilization, laser-based assaults, and electromagnetic assaults. Modern microchips come with numerous countermeasures to avoid such assaults whilst the cryptographic modules are being modified.

Eavesdropping and Interference: IoT applications frequently comprise nodes conveyed in open environments (Aliyu et al., 2018). Therefore, such IoT nodes are exposed to cyber-attackers. During various stages such as data transmission or validation, the cyber-aggressors can eavesdrop and capture information.

Sleep Deprivation Attacks: Throughout these assaults, the cyber-attackers try to deplete the low-powered IoT machine batteries. This triggers a denial of service owing to a dead battery from the IoT System nodes. This would be possible by running endless loops in edge gadgets using malignant programming or wrongly extending the edge gadgets' power utilization.

Booting Attacks: During the boot process, edge gadgets are extremely susceptible to different assaults. This is because in that case the built-in protection technologies are not allowed. Cyber-attackers can leverage this vulnerability and try to assault the gadgets when rebooted. As edge gadgets are typically low-power gadgets and move through cycles of sleep-wake, the booting of such gadgets, therefore, needs to be safe.

8.2. Security issues at network layer

The primary role of the networking layer is the transfer to the computer or processing device of the data obtained from the detection (sensing) node. The substantial threats faced by the network layer are as follows.

Phishing Site Attack: Phishing assaults typically apply to assaults where an insignificant exertion placed by the cyber-aggressor may depend on a few IoT gadgets. At least a majority of the devices would become a survivor of the attack, the aggressors assume. When a client accesses websites on the internet, there is a risk of visiting phishing pages. The whole IoT network used by the company is susceptible to threats when the client's identity and authentication are compromised. The networking layer is fairly vulnerable to phishing attacks (Chiew et al., 2018).

Access Attack: This kind of assault is called advanced persistent threat (APT). This is a kind of attack where the IoT infrastructure is breached by an unapproved person. The cyber-aggressor will stay undetected in the network for a long time. The aim of this kind of attack is not to damage the device, but to gather valuable details. IoT systems share critical knowledge constantly and are thus extremely susceptible to these assaults (Li and Chen, 2011).

DDoS/DoS Attack: In these assaults, the attacker is overwhelming the intended database with a large number of unnecessary requests for operation. This weakens the goal application and consequently disturbs credible client supports. When the attacker uses multiple methods to overwhelm the site, otherwise such an intrusion is classified as invasion or attack by DDoS (Distributed-DoS). These forms of attacks are not specific to IoT implementations, but due to the complexity and multi-faceted existence of IoT networks, the IoT's network layer is susceptible to these assaults. Numerous IoT devices are not unambiguously built-in IoT infrastructure and therefore are easy interfaces for assailants to deploy DDoS assaults on the targeted servers. The assault on the Mirai botnet mentioned earlier is such an attack (Huang et al., 2020; Yin et al., 2018).

Data Transit Attacks: IoT systems do a large amount of storage and sharing of information. Data is critical and therefore the primary focus of cyber-assailants is continuous. Information that is maintained on the normal database or cloud storage is endangered by security; furthermore, information that moves from one end to another is more susceptible to digital threats. There are tons of exchanges of knowledge between actuators, sensors, servers, and so on in IoT services. In these activities, distinctive networking systems are used and IoT networks are vulnerable to data breaches in this way.

Routing Attacks: In such assaults, malignant nodes are shared in an IoT network through the exchanging of knowledge attempting to block the routing pathways. Sinkhole attacks are a specific form of routing interference in which an attacker helps and drives traffic through a fake shortest route in nodes. Another intrusion is a worm-hole attack and may become a significant security issue because, for example, sinkhole assaults are combined with other threats. A warm-hole is band-out connectivity between two nodes for quick data transmission. An assailant can make a warm-hole between an undermined node and a gadget on the web and attempt to bypass the essential security protocols utilized in an IoT application (Ma et al., 2017a).

8.3. Security issues at middleware layer

The middleware functionality of IoT is to provide a deliberative layer (abstraction) between the network layer and the application layer. Middleware also has impressive scientific and computational capabilities (Borgohain et al., 2015). It ensures APIs fulfill the demands of the application interface. The middleware framework comprises permanent

data warehouses, brokers, queuing systems, artificial intelligence or computing devices, etc. Although the middleware layer helps ensure a secure and effective IoT process, there are also delicate unique cyber attacks. By contaminating the middleware such attacks will take control of the entire IoT program. Other key protection issues in this layer involve storage and cloud protection. In the middleware layer different possible threats are investigated as follows Ma et al. (2017b).

Man-in-the-Middle Attack: The MQTT utilizes the publish-and-subscribe model between subscribers and users using the MQTT broker which performs adequately as an intermediary. This help may be conveyed without the receiving end knowledge in decoupling the publishing and subscribing bodies from one another, and without any information of the receiver as well. If the cyber-assailant may gain a charge of the broker and become a guy in the center, then he or she will have full leverage of the whole correspondence without being revealed to the customers (Sun et al., 2017; Yaseen et al., 2019).

SQL Injection Attack: Middle-ware is vulnerable to another kind of assault named SQL Injection (SQLi) (Gu et al., 2020). In such assaults, cyber-assailant can install vindictive SQL proclamations in a program. The cyber-assailants will then obtain every client's private details and modify the company information that is contained in the database. In their 2018 report (Ping-Chen, 2011), OWASP (Open Web Application Protection Project) noted SQL injection as a high risk to network security.

Signature Wrapping Attack: XML signatures are often used in the middleware of web-based services (Kumar et al., 2017b). The cyber-assailant removes the signature code in a signature wrapping cyber-assault and can perform operations or modify eavesdropped messages by leveraging weaknesses in SOAP (Simple Object Access Protocol) (Jensen et al., 2011).

Cloud Malware Injection: The aggressor may get power, infuse a malevolent code in the software, or infuse a virtual machine into the software. The aggressor professes to be serious assistance by attempting to render an instance of a computer system or a network with malignant assistance. This enables cyber-assailant to view the target's service requests and to collect confidential details that can be changed by the case.

Flooding Attack in Cloud: This assault functions almost similar to the cloud DoS attack, and affects the QoS. Where cloud services are exhausted, the aggressors constantly submit multiple requests for support. By extending the load on cloud servers such assaults will impact cloud frameworks.

Replay attack: The nature of the assault is to ruin the uniformity of two communicating entities, intercept data packets, and forward them to the designated destinations without alteration. If a cryptographic algorithm produces a key (private) with restricted randomness during the process of signature generation, the key might be leaked by the attacker and this limitation could be exploited to launch a replay attack. Singh et al. (2012) have analyzed cryptographic replay attacks and corresponding mitigation mechanisms.

Impersonation Attack: An intrusion by impersonator is an assault in which the attacker may conceive the identity of authorized entities in a scheme or protocol. The objective of a dynamic authentication protocol is to identify or authenticate a person to neglect the likelihood that any other party 'C' distinct from 'A', performing as 'A', can lead the party 'B' to accept the malicious one ('C') as 'A'. Yu et al. (2019b) have proposed a lightweight authentication scheme against impersonation attack for cloud computing aware IoT environment. Aghili et al. (2017) have presented a lightweight authentication protocol to secure RFID systems of an IoT infrastructure.

Privileged Insider Attack: Privileged insider assaults are directed by malevolent users having authorized (i.e. insider) system access. Unquestionably, malicious insiders generate a threat to information technology infrastructure, including operational technology and IoT systems that are relatively vulnerable, merely because of not having the fundamental defense mechanisms of IT. There are often concerns at issue where insider attacks frequently end in data-stealing and financial damage. Moreover, an insider attack targeting operation technology and IoT networks may trigger power grids to be shut down, water sources to be contaminated and the infrastructure of a nation to be ruined. Khan et al. (2020) have proposed an insider attack detection scheme for IoT infrastructure based on big data analytics.

8.4. Security issues at gateways

Gateway is a large layer that plays a major role in linking various computers, users, and cloud services. Gateways also help in supplying IoT applications with hardware and software solutions. Gateways are used to encrypt and decode IoT data, and to convert communication protocols between different layers (Huynh et al., 2019). IoT networks today are heterogeneous, with loads of gateways in between like LoRaWAN, ZigBee, Z-Wave, and TCP/IP stacks. Any of the IoT gateway's Privacy issues are listed below.

Secure Onboarding: It is important to maintain encryption keys at the stage where another device or sensor is inserted into an IoT environment. Gateways serve as an interface portal between the latest devices and the administrations and all keys are transferred via the gateways. The gateways are also vulnerable to man-in-the-middle attacks and tests to snatch the encryption keys, particularly during onboarding.

Extra Interfaces: Limiting the assault surface is a significant procedure that should be remembered while implementing IoT gadgets (Stanciu et al., 2017). An IoT gateway maker will be reviewing only the basic applications and conventions. So stay free from loophole authentication or data theft, a portion of the facilities and functionalities will be restricted for end-clients.

End-to-End Encryption: Genuine end-to-end protection of the application layer is needed to guarantee the data privacy (Sabir et al., 2018). The service does not require any other attacker than the service's stated receiver to decode the encrypted messages. Given the fact that ZigBee and Z-Wave conventions assist with encryption, this is not end-to-end encryption, provided that the gateways are expected to decipher and re-encode the messages to read the data from one convention to another. Such decryption at the portal leads sensitive knowledge to security breakdowns.

Firmware updates: Many IoT devices are required to utilize money, and therefore they do not have a UI or the opportunity to access and update the software updates. Gateways are typically used for uploading and updating the software updates. The current and new firmware versions should be registered, and the authenticity of the signatures for stable firmware updates should be checked.

8.5. Security issues at application layer

The platform layer handles and provides client services. IoT features include shrewd (smart) houses, smart communities, smart meters, smart grids, and so on. For starters, this layer has specific security concerns that vary from other levels, such as identity stealing and privacy problems. Security problems are often specific to various applications in the layer specified. Numerous IoT implementations often have a sub-layer between the networking layer and the device layer, commonly referred to as the device service layer or the application layer. The layer supports numerous company administrators and helps in the distribution and measurement of smart capital. Down below are called major protection problems faced by the network layer.

Data Thefts: IoT services have to manage a lot of private information. The information in travel is significantly more vulnerable to cyber-assaults than information at rest, and in IoT services, enormous information exchange happens. If such apps are defenseless to identity security attacks, the clients may refuse to enroll their private details on IoT apps. Any of the approaches and conventions used to protect IoT applications against knowledge breaches are data protection, separation, device and network authentication, security monitoring, and so on (Canovas Sanchez et al., 2018).

Access Control Attacks: Access control is a kind of permission

program that only allows legitimate customers or procedures to access the information or account. Access management attack in IoT systems is a very important attack as if security is compromised and then the whole IoT infrastructure is vulnerable to cyber assaults (Tan, 2018).

Service Interruption Attacks: Those cyber-attacks are close to illegal intrusion or DDoS assaults, too. IoT systems have been exposed to multiple instances of these assaults. These attacks deny credible clients the usage of the IoT resources by misleading the servers or too busy a device to respond (Feng et al., 2020).

Malicious Code Injection Attacks: Cyber-assailants usually look with the easiest method they may use to hack into a network or program. If the system is prone to malignant material due to insufficient code tests, so this will be the key passage point chosen by a cyber-assailant. Cyber-assailants typically use cross-site scripting (XSS) to infuse any harmful material into a website. An effective cross-site scripting attack can result in an IoT account being caught and can corrupt the IoT network.

Sniffing Attacks: The cyber-assailants can use sniffers to track the IoT infrastructure's network traffic. It will enable assailants to access confidential consumer details if inadequate protection measures are implemented to avoid it (Anu et al., 2017).

Reprogram Attacks: If the software architecture isn't secured, the assailants can attempt to reprogram the IoT devices remotely.

9. Security and privacy-preserving techniques for IoT

9.1. Cryptographic techniques for location-based security

Standard Cryptography for IoT Device Location Information Privacy: Assume that a gadget (e.g., a reference point node or a client's gadget) be acquainted with its location (e.g., has a GNSS chip), which it and the system trust to be right during necessity, and the gadget needs to impart this data to some other gadgets (e.g., standard hubs or cloud server) over the system (i.e., the Internet) in a safe way. In this case, location data can be dealt with similarly as some other basic snippet of data, and standard cryptographic procedures can be utilized for secure communication (Shouqi et al., 2019). Different gadgets can confide in the accuracy of the location data only if they can check their credibility and trustworthiness. The previous implies that the location data was truly transited by the gadget professed to be the source and not by a malicious group professing to be the right source (mocking). The last implies that the data has not changed in transit. The previous infers the last mentioned, however, not a vice versa. The legitimacy and trustworthiness of location data can be guaranteed with standard cryptographic strategies. Preparing a checksum by utilizing (cryptographic) hash algorithm (e.g., SHA-256 (Quist-Aphetsi et al., 2019)) ensures integrity, yet without additional procedures just against data transmission errors (i.e., no security). If the groups have a mutual secret key, they can utilize cryptographic message validation to guarantee both integrity and validity (see, e.g., HMAC (Ma et al., 2017c)). Digital signature schemes dependent on public-key cryptography (e.g., DSA (Li et al., 2019b)) permit a check of legitimacy and integrity without shared secrets. Also, digital signatures ensure non-denial that prevents a transmitter from later challenging sending messages. This might be a significant element additionally with regards to location data since it guarantees that a gadget that has professed to be at a particular location can't later decline this claim. The above plans ensure just validness and integrity of location, yet the location data itself is, as a matter of course, moved as plain text and is accessible to anybody monitoring the traffic in the system. The least complex type of protection of location data (i.e., security regarding intruders) can be obtained by guaranteeing the privacy of area data moved in the system. Secrecy can be accomplished by encrypting the location data with standard cryptographic procedures. Encryption can be implemented either with secret-key cryptography, which necessitates that the imparting groups have a shared secret-key or with public-key cryptography, where the key utilized for encrypting is a public-key but the decryption can only be performed utilizing a secret-key. Usually, a blend of these is utilized so the participating groups trade a secret-key utilizing public-key cryptography (e.g., with Diffie-Hellman protocol (Chen et al., 2016)) and the real encryption is performed with increasingly effective secret-key cryptography (e.g., with AES (Tsai et al., 2018)) by utilizing this key. Public key cryptography gives a method for key dispersion but frequently requires a PKI (Public-Key Infrastructure) to guarantee that public keys belong to specific substances. With a mix of privacy, integrity and authenticity authenticated encryption can be accomplished by verifying (with the above plans), the encrypted location data or legitimately by utilizing a cryptographic model for validated encryption (e.g., AES-GCM (Jankowski et al., 2011)). Nonetheless, even simpler encryption may provide integrity and authenticity since it can be difficult to produce a ciphertext that decodes into an important location. Assistance for cryptographic systems is included in protocol suites, for example, IPSec, SSL (for example, OpenSSL (Liu et al., 2019b)), and SSH. The figure beneath shows a cryptography approach incorporating digital certificates (Fig. 24).

Secure Lightweight Cryptography for IoT: Although cryptography techniques can be utilized for securing location data in IoT as examined in the previous section, but resources are usually limited for IoT gadgets making cryptography difficult to execute effectively and safely. Lightweight cryptography tends to algorithms and executions that are intended to offer security with minimum implementation prerequisites (small circuitry, low power utilization, low memory, and so on). These incorporate codes running on microcontroller as well as devoted integrated circuits. In the last couple of years, a vast of research has been performed in lightweight cryptography. In secret-key cryptography, this incorporates a few lightweight stream ciphers (e.g., Trivium, Grain, and so

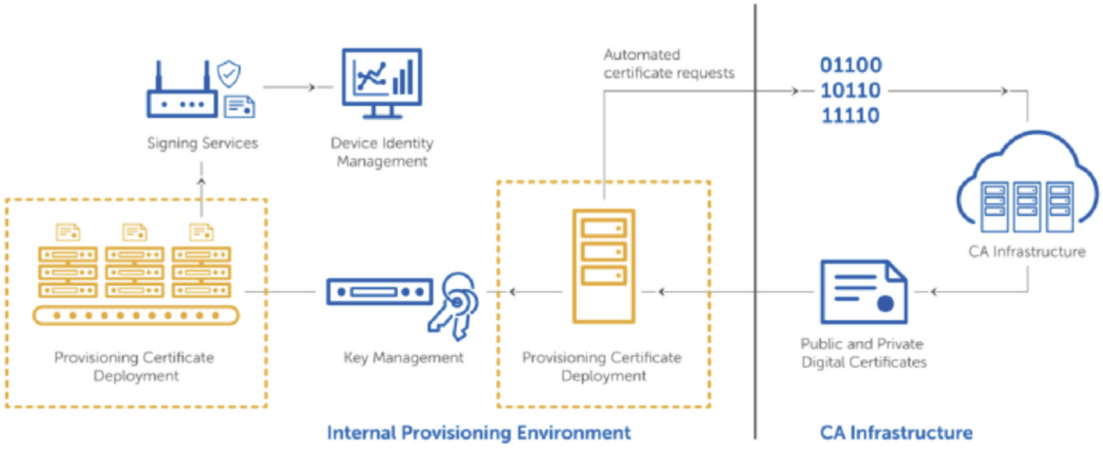

Fig. 24. Cryptography using the digital certificate.

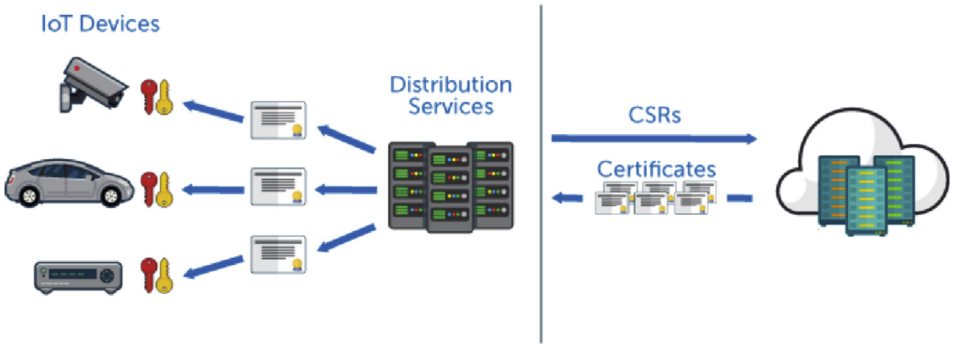

Fig. 25. Cryptography technique for IoT applications.

on.) and block ciphers (e.g., PRESENT, SPECK, KTANTAN, and so forth.) combined with different lightweight secret-key primitives (e.g., (Chen et al., 2019a)). In the case of public-key cryptography, the work has concentrated predominately on the elliptic-curve-cryptography (Almajed et al., 2019) and its lightweight executions (e.g., (He et al., 2015)) as a result of its small key sizes and generally low computational complexity. The consequences of research on lightweight cryptography can be utilized additionally for privacy-preserving localization in IoT (and for assuring a generalized security of IoT). The principal threats against well-structured cryptographic algorithms (including the previous one) are relevant to weak deployments and utilize data spillage through inadvertent channels called side-channels, which are designed by various characteristics of cryptographic gadgets (Wang et al., 2019c). To prevent these spillages, cryptography must be actualized with special consideration so that they incorporate securities against implementation attacks. Since gadgets in IoT communicate over the Internet, remote assaults over the system are a danger and every single cryptographic execution ought to have protection against them. Specifically, all cryptographic programming and equipment must be time-constant to ensure security against timing assaults (De et al., 2019), which uncover secret keys from execution time if it relies upon the presumptions of the secrets. Additionally, assaults that need physical access to a gadget performing cryptographic computations (for example, power consumption analysis, electromagnetic radiation analysis, and so on.) can cause risk. Acquiring secret keys from a gadget by physical assault permits acting as the gadget later on (for example, performing mocking assaults). However, physical assaults are commonly not a risk to the privacy of the location because having physical access already infers information on the location of a gadget. However, assaults during impermanent access to a gadget may permit recuperating its past or future locations. Fig. 25 shows a simplified digital certificate-based cryptography technique for IoT applications.

The work Pranata et al. (2012) presented a light PKI (Public Key Infrastructure) that is to be implemented in IoT usage cases, while traditional PKI is regarded as heavy in communication and computation expenses. To ensure the protection of data during transmission, the authors of Zhao et al. (2013) presented an efficient transmission scheme. The conceptual framework used a customizable data encapsulation technique to reduce overhead for computation and connectivity.

9.2. *IoT security using fog computing*

Fog Computing Architecture: The key errand of fog computing is to deal locally with the knowledge created by IoT gadgets for better administration, and therefore requires an architecture consisting of different layers. It consists of two different application architectures and those are architecture for Fog-Device and architecture for Fog-Cloud-Device (Baccarelli et al., 2019). The previous one consists of gadgets and a layer of fog and the second one consists of gadgets, a fog, and a layer of cloud server/s. A layered architecture is constructed according to their storage and computational capacities. Contact between various levels is achieved using wired (for example, fiber optics, Ethernet) or wireless networking (for example, WiFi, Bluetooth, so on). Through Fog-Device design, the fog nodes deliver a client different forms of assistance without cloud service support. Nonetheless, in Fog-Cloud-Device architecture, the fog layer takes simple decisions, while the more complicated operations are carried out on the cloud (Hernandez et al., 2017). The architecture of the fog-cloud-device framework is shown in Fig. 26. The writers of paper (Chiu et al., 2019) hypothetically and theoretically considered the fog computing architecture when comparing the fog computing model view with the usual cloud

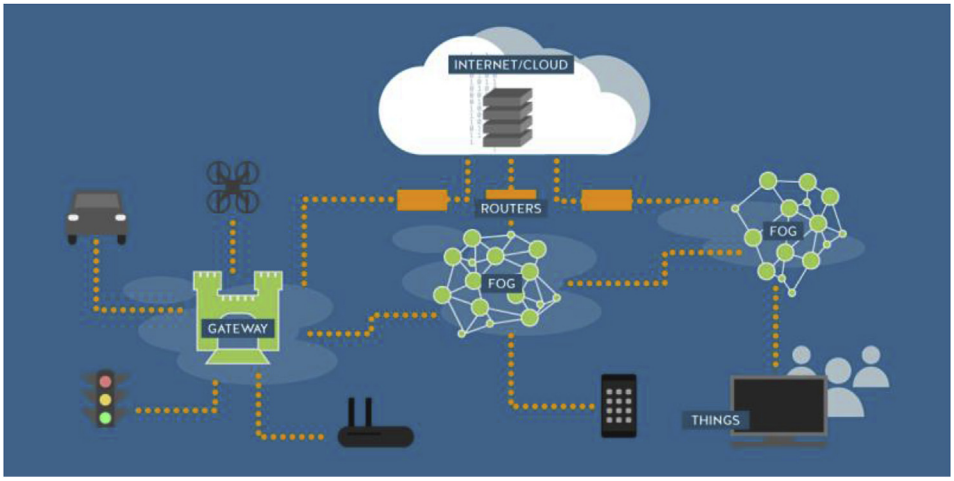

Fig. 26. Fog computing architecture.

computing framework based on service latency and power consumption. Fog computing diminishes server and network edge application flow by 90 percent and a client's usual reaction time by 20 percent while the system is contrasted with web-only. Authors in Yi et al. (2015) also addressed in depth the concept and principle of fog computing, comparing it with other related concepts, such as mobile edge computing (MEC) and other specific technologies, such as MCC. Moreover, the authors also provided several tools such as virtual reality (AR), visual monitoring, large data analysis, and fog software caching.

9.2.1. Features of Fog Computing against IoT Security Threats

About the assaults mentioned in the previous portion, the structure of fog computing is able to overcome certain privacy issues analyzed below.

Man-in-the-middle attack: Fog serves as a protection layer between a device and an IoT or cloud system. Both dangers involved with assaults on IoT systems tend to go through the fog layer in general, so this layer will identify so mitigate irregular activities until they are transferred to the network.

Data transit attacks: Information analysis and handling were vastly enhanced as contrasted with IoT gadgets, as done on stable fog nodes. If it is processed on the fog nodes in comparison to keeping the details in the application hardware, knowledge would be best assured. Fog nodes often help to render knowledge to the client increasingly available.

Eavesdropping: Using fog processing nodes, connectivity only takes place between the device and the fog node, instead of spreading the data across the whole network. The chances of a cyber-attack trying to eavesdrop diminish significantly as the traffic on the network is reduced.

Resource-constraint issues: A significant portion of IoT gadgets are resource-constrained, and the cyber-assailants use this reality throughout the assault. They seek to hurt the edge gadgets and use them as poor links to get into the picture. Fog nodes can support the devices on the edge and can hold them secure from these assaults. A nearby fog node may conduct the more complicated safety functions which are necessary for security.

9.2.2. Security Threats and Prevention Mechanisms in Fog Layer

While the fog layer offers specific functionality for IoT applications, new vulnerabilities are created by the knowledge and computation operation conducted in this layer. In this way, it is important to consider these safety goals of fog computing before implementing fog-based IoT services. In this segment (Puthal et al., 2019) different features presented by fog computing, privacy problems encountered, and potential strategies for beating them are discussed.

Real-Time Services: Fog computing will; typically provide a real-time operation in the IoT frameworks by conducting various computations near the edges of data generation.

Intrusion detection: The infringement of the policy and malevolent tests on fog nodes and IoT hardware would not be detected because there is no valid intrusion detection technique. The assaults probably won't impact the entire framework of fog computing, yet the cyber-assailants can control the nearby services. Fog nodes may recognize assaults based on city infrastructure by teaming up with their neighboring hubs. The application attack can be differentiated by tracking system behavior and client software frameworks (An et al., 2019).

Identity authentication: The method of providing and accessing real-time resources such as fog nodes, service suppliers, and clients has various aspects connected with it. Believing all of the drugs listed are a burdensome task, so it creates protection issues for IoT programs so knowledge regarding customers. Service functionality should be provided only to authorized and trustworthy clients; otherwise, cyber assailants attack the server and access services and privacy of the customer. The identity authentication systems are needed to keep attackers away from unlawfully accessing resources. Some successful identity authentication methods were implemented to provide a reliable service (Chandrasekhar et al., 2015).

Transient Storage: With the help of transient storage, clients may store and handle their data momentarily on fog nodes. Another way, however, it helps to efficiently handle data on local servers, creating new difficulties and protection concerns, particularly for protecting data privacy.

Identifying and protecting sensitive data: Data contained in IoT gadgets may involve social gatherings, behaviors of individuals, patterns of traffic, weather, etc. A portion of the information may be close to sensitive while a few of the information might be made open (public). Moreover, for various clients, similar information has diverse security requirements. That is why identifying and securing the critical details from a large amount of data is important.

Sharing Data Securely: To ensure adequate protection, encryption is expected over the data transmitted to the fog servers. When it's authenticated, no one other than its proprietor can peruse the knowledge. This raises the information-sharing issue. To counter this issue, several cryptographic approaches have been implemented in, for example, key-aggregate encryption, attribute-sharing, intermediate re-encryption.

Data Dissemination: Due to safety concerns, the details cannot be transferred to the fog repository without encryption. Because of this transition of encrypted knowledge to the fog server, various required functions, such as networking, browsing, and conglomeration, are given away.

Searching data securely: Information needs to be authenticated before it is moved. However, clicking on the ciphertext is complicated for proprietors much as many people do when it is authenticated. In Liu et al. (2016), search-capable encryption and its protection rates are defined for retrieving the data from the encrypted information (Naveed et al., 2014). provides a special symmetrical search algorithm.

Data aggregation: Fog servers may require aggregating the information in specific cases to prevent information spillage and minimize communication overhead. It is essential to create secure aggregation algorithms to prevent information robberies. Different homomorphic encryption algorithms, for example, BGN (Wei, 2015) and Paillier (Rong-Bing et al., 2019), conceived to achieve efficient aggregation of information.

Decentralized Computation: The system will evaluate the details collected on the fog servers and optimize it for better performance. In any case, such computations have a few risks related to them. For instance, cyber-assailants can take control of the analyzed results and expose the information as well.

Server-aided computation: Operations which cannot be carried out by IoT gadgets themselves are performed with the aid of fog servers. However, if the fog repositories that obtained information from IoT services are still compromised, this will cause leakage of confidential details to cyber-assailants. Server-based computing is such a technique that focuses on ensuring stable computing.

Verifiable computation: Clients depend on the fog servers for processing their results. A defensive function is required to validate the effects of the computation from the fog servers. The authors also implemented some multi-client frameworks in Papamanthou et al. (2013) that can assist with verifiable computation.

9.3. IoT security using machine learning

In recent years, the idea of machine learning has taken a major interest in the recent few years. Many sectors use ML for their enhancement, and it is also used for IoT protection. ML has proved to be an excellent strategy for protecting IoT devices against cyber-attacks by offering an effective means of coping with assaults as opposed to other traditional strategies. The protection strategies that machine learning provides to resolve such threats are listed below.

DoS Attack: DoS assaults are a major problem on IoT devices. One way to deal with these assaults is to use a norm based on Multi-Layer Perceptron which secures IoT infrastructure against DoS assaults (Fatayer et al., 2019). The article Li et al.(2018) built an algorithm for particle swarm streamlining and backpropagation to prepare a system that enhances the reliability of wireless IoT networks. ML-based

strategies are extremely helpful in extending the precision of deductions and through the reliability of IoT hardware susceptible to DoS assaults.

Eavesdropping: During information transmission, cyber-criminals can eavesdrop on messages. For starters, Q-learning aided the offloading system (Zhang et al., 2019) or non-parametric Bayesian strategies (Pan et al., 2015) can be used to deploy security against these assaults. Techniques such as Q-learning and Dyna-Q are methods of machine learning, and can also be used to protect gadgets from eavesdropping. The application of such methods is implemented in Xiao et al. (2016) by way of experiments and reinforcement learning.

Spoofing: The use of Dyna-Q (Hwang et al., 2013), Q-learning, SVM (Hu et al., 2019), DNN model (Yu et al., 2018b), Frank-Wolfe distributed (dFW) (Xiao et al., 2018b), and incremental aggregated gradient (IAG) (Xiao et al., 2018) strategies to discourage spoofing assaults. Such techniques not only improve the precision of identification and detection, but also tend to decrease the average error and false alarm rate.

Privacy Leakage: For example, the variety of person records, health-related details, venue, or photographs places the safety of consumers at risk. Logical calculations that safeguard security should be used to prevent spillage of safety. Another approach developed to build trustworthy IoT resources is a resource fidelity detection algorithm that is built based on the rest of the Chinese theorem.

Digital Fingerprinting: The automated fingerprinting method is growing as a prevalent bio-metric identification technique because of its minimal commitment, precision, acceptability, and high-security (Darlow et al., 2017). Apart from the benefits of computerized fingerprinting, there are many obstacles to utilizing this method successfully in IoT, such as special fingerprint identification, image enhancement, detection and fitting of features, etc. Different ML-aided algorithms were developed to ensure sophisticated strategies for overcoming these challenges (Baldini et al., 2017).

SVM is a linear and non-linear classification simulation system, text categorization, PCA (Principal Component Analysis), voice recognition, and regression testing. It extends the distance between the limit of an option and the sequence of preparation. The article Meraoumia et al. (2015) has dealt in depth with the usage of SVM in optical fingerprinting. Furthermore, reviewers compared it with other modern ones. A part vector is generated based on the specific fingerprint's pixel estimation and is applied to train the SVM algorithm. Various patterns are examined behind the fingerprint, and the matching of a particular fingerprint is then achieved based on pattern recognition.

The popularly used algorithm in ML is ANN. This provides other advantages, including proactive thinking, fault detection, and imagination. In Abiodun et al. (2019) a program was developed to use ANN for precise identification of fingerprints. The advanced estimates of different features in the fingerprint, including information, ridge-starting, ridge--finishing, and bifurcation are used as input into the neural network to train ANN's algorithm. The fingerprint authentication procedures are carried out similarly to the previous experiential values contained in the database.

IoT's key need is to protect all of the systems and gadgets connected with the program. The role of machine learning is to use and train algorithms to identify irregularities in IoT devices or to recognize any unauthorized behavior that happens in the IoT environment to avoid security breaches and problems such as data loss. Moreover, extended research contributions are required to keep up the development of IoT.

9.4. IoT security using edge computing

Edge computing is also another extension of cloud infrastructure and is commonly utilized by different organizations. Net, cloud, and edge are not identical except that they are separate types of IoT systems. The basic difference between cloud computing, fog computing, and edge computing is where information and computational resources are found. The cloud is distributed on a wider scale to handle the huge amount of knowledge, which is situated at a strong detachment from its customers (Qi et al., 2019). Edge computing is seen as a possible way to solve the issues faced by cloud computing when an edge device is installed between the application and the cloud or fog. On the edge node, outside of the cloud, certain computing and calculation operations are performed. Edge computing architecture comprises edge gadgets, cloud servers, and fog servers or nodes as appeared in Fig. 27.

The computing and processing power in an edge-computing system is given at the edge itself. The gadgets in an application will shape a network among them and can collaborate to interpret the knowledge among themselves (De Donno et al., 2019). Therefore, one ton of knowledge can be saved from moving beyond the device, either to cloud or fog, and this technique will improve the IoT application's protection. Additionally, edge computing helps ensure low connectivity costs by growing the need for all knowledge to be transmitted to the cloud (Chen et al., 2019b).

9.4.1. Edge computing to secure IoT

The useful solutions increasing edge computing ensures to resolve such threats to security are listed below.

Data Breaches: Usually the data is analyzed and stored inside the gadget or in the local network in an edge computing environment. No data is transmitted from the data generator to the data processing system within this structure. It also avoids data transfer, therefore eliminates data manipulation which intrusion attacks. But there is a transfer of data from a gadget to a fog layer in a fog computing system and cyber-criminals may manipulate this change (Zhou et al., 2019b).

Data Compliance Issues: Specific nations have strict regulatory laws to prohibit the transfer of knowledge outside their borders, such as the unique legislation of the European Union named the Universal Data Protection Act. Using edge computing (processing), various organizations will retain their confidential details within their limits and maintain compliance with data sovereignty legislation (Hagan et al., 2019).

Safety Issues: As the application of cyber-physical systems progresses, protection and privacy are seen as important concerns. Even if answers are marginally deferral, this can cause physical protection concerns. For instance, if a vehicle's embedded sensors expect an incident, then the airbags have to be activated automatically. If the sensing device relies on all the data being sent to the cloud server and has to wait for the cloud server answer to do some operation, therefore there could be a pause in avoiding serious injury or even death. Surveillance cameras may also be implemented utilizing edge computing to track and evaluate disturbances, and the brief and suspicious data can be sent to data centers to obtain quicker reaction times.

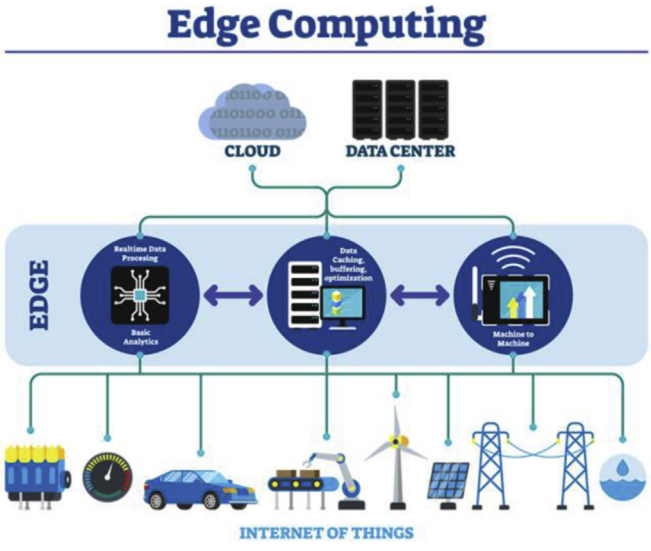

Fig. 27. Edge computing.

Bandwidth Issues: IoT systems produce vast quantities of data. Some of such results are coarse. The migration of all such data directly to the cloud often needs a higher bandwidth rate, in addition to the security risks during data flow. By utilizing edge computing, a lot of data cleaning and aggregation should be available at the bottom, and only the brief data should be sent to the cloud whenever necessary (Abbas et al., 2018).

9.4.2. Challenges in edge layer

Edge gadgets contain cameras, RFID devices, actuators, and built-in devices. The edge layer of an IoT system is particularly susceptible to assaults. If the edge layer protection is compromised, then the whole architecture may be vulnerable at that level. MQTT and CoAP are the two commonly recognized edge-layer conventions. Both of these protocols allow no automatic usage of any compliance regulation. Given the fact that there is an option to have a flexible encryption layer as TLS for MQTT and DTLS for CoAP, but it may require more storage and encoding overhead. Issues specific to edge hardware include battery-depleting assaults and assaults like blackouts. Edge devices are usually a resource necessity, and the battery power is the most critical resource they rely upon. The easiest solution to targeting the edge gadgets is to deplete an edge gadget's battery in any way. The method of achieving a balance between storage and data processing is of great significance for the cloud. Holding excess knowledge on the edge will also cause edge gadgets overpowering, which can impact the whole program.

10. Open issues, challenges, and future research

Some safety and efficiency problems need to be reconsidered through the usage of cryptography, fog computing, edge computing, and ML for IoT security. Each segment looks at a few of those things.

Asymmetric protocols are dependent on crude public keys and are not scalable, which is already been observed, and thus must be supported up with solid validation mechanisms, to guarantee the protected exchange of keys. The more adaptable certificate-based techniques should be streamlined, principally because, with IEEE128-byte 802.15.4 data packets, PKI authentications are unreasonably enormous for being utilized with IoT applications. Future researches on this topic may investigate techniques to develop compressed certificates that are best suitable for IoT applications and associated gadgets (Khalid et al., 2019).

Saied et al. (2014) propose a lightweight approach to the key generation of security protocols to make them appropriate for IoT gadgets. The proposed scheme assists constrained gadgets with comparatively less communication and computational overhead. The authors have argued that restricted gadgets can save around 35% energy by utilizing this mechanism. Further research is required to extend the efficiency.

Noura et al. (2019) have proposed a lightweight cryptographic authentication scheme for IoT-based communication. However, new features may be employed to increase the accuracy level while maintaining an acceptable overhead.

Zeadly et al. (2019) performed a review on cryptography-based IoT security. Most importantly they have prescribed some important research directions which might be helpful for future research. Their work has prescribed to perform further research on lightweight symmetric cryptography algorithms and elliptic curve cryptography (ECC) based on the public key to enhance their efficiency.

Because fog computing is an assistive extension of cloud storage, some of the problems, for example, would appear to be security and safety. Therefore, these privacy and security issues regarding fog computing needed to be addressed before actualizing fog-aided IoT applications. A portion of these problems and research concerns relating to privacy and protection in IoT environments and the arrangements offered by fog computing are addressed in Ni et al. (2018).

There are several current ML algorithms. Therefore, selecting a suitable algorithm that is rational for the task is important. Choosing an offbase algorithm will produce a trash yield, resulting in a lack of energy, adequacy, and accuracy. In comparison, selecting an unacceptable collection of data would cause the feedback of trash generating inaccurate outcomes. Such variables, as well as variety in selecting results, are the best outcome of an ML structure. If the data is not clustered and organized then the exactness of the forecast would be smaller. The historical records can often include various uncertain characteristics, inconsistencies, incomplete values, and insignificant details. IoT systems produce vast volumes of data, and cleaning and pre-processing the data correctly is a tricky errand. Different features such as linear regression, multivariate regression, trait development, redundancy expelling, and packing (compressing) data are needed to protect IoT apps and services viable using ML.

The main considerations are in terms of edge computing, infrastructure, and consumer protection. Private details of a customer may be spilled and misused if cyber assaults are revealed to a company which is applied with IoT gadgets. For instance, the presence or non-appearance of a person at home may be discovered simply by tracking the data regarding power or water usage. As the data is processed at the resource edge (e.g., home), however, any of the protocols such as securing WLAN will be communicated to the customer. In fact, details at the edge will be entirely owned by the user, and he or she will be in charge of which knowledge to transmit.

Lesson Learned: The sub-section will provide an overview of the lessons which have learned from the whole work. These are described below.

- Critical comparative analysis of the current researches on IoT security.
- A detailed overview of IoT infrastructure including core elements, architectures, applications.
- Introduced several threat modeling approaches.
- Elaborated layer by layer security threats and vulnerabilities.
- Described preventing mechanisms to eliminate threats.
- Security features on IoT gadgets can cause extra overhead on the network. This is a vital issue that must be addressed carefully.
- More and more researches on lightweight cryptographic algorithms should be performed.
- Machine learning is a hot topic of the current time. Researchers should perform thorough research aiming at the integration of ML in IoT security.
- Edge computing and analytics might be very much supportive of IoT security. Because if edge computing is utilized in IoT, the edge gadgets will perform the necessary computation and analysis and the data will remain much secure as they do not have to traverse a wide area network.

Some of the future research directions in this field are:

The edge gadgets in the IoT are most capital intensive gadgets and are susceptible to assaults. Work into intrusion reveals that although it requires relatively little time to ensure the safest protection for edge nodes, they are often susceptible to several noxious (malicious) assaults.

In the IoT system, the gateways between various layers should be secured. Gateways offer the cyber-assailants a clear passage point into the IoT system. End-to-end encryption will be a viable approach to protect the data transiting via the gateways, rather than simple encryption methods for specific protocols. The data can only be decrypted at the intended target, and not at the protocol transfer gateways.

Data sharing between fogs is one of the sectors in which more work is required. If due to considerable load the fog layer is unable to handle the queries, the message is submitted to the air. In this case, the sharing of resources among neighboring fog layers could be implemented to prevent undesirable requests.

The fog layer can be rendered even more shrewd using different strategies dependent on ML and AI. The fog layer will include the ability to decide the time during which the data should be retained in the fog and when the data should be disposed of or transferred to the cloud during extended storage. Increasingly efficient and robust consensus

processes can be targeted at achieving agreement between the fog nodes alongside avoiding unrestricted usage of computing resources. The new algorithms for consensus are resource hungry and less efficient.

Data processing is desperately required for the successful organization of IoT systems in real-time and in the vicinity of the IoT node. Specific ML-based algorithms could be intended to process the data inside the node itself to reduce wasteful data transfer. This will help improve the service's protection by stopping vulnerable data flow.

The looming acknowledgment of versatile quantum computers has prompted dynamic research in Post-Quantum Cryptography. The challenge is more diligently for implanted IoT gadgets, because of their unavoidable dissemination and their constraint resources. Among different classes of quantum cryptography plans, Lattice-dependent Cryptography is rising as a feasible technology; almost 50% of the 'survivors' of the second round of the NIST's PQC rivalry is lattice-dependent (Li et al., 2020).

11. Conclusion

The analyst has implemented growing protection issues and risks at specific levels of an IoT program in this review or survey. The research dealt with problems related to different levels of IoT infrastructure. The research also explored the existing and emerging strategies toward threats to IoT protection, including encryption, fog, edge computing, and ML. Specific issues and concerns resulting from the construction of the approach itself have already been addressed. Additionally, there has been talking of the cutting edge of IoT security with a fraction of upcoming work to improve IoT protection strength. This survey is intended to fill in for upcoming IoT applications as a significant asset to boost protection. Also, this work might be assistive to researchers and scholars currently working on the relevant fields.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abbas, N., et al., Feb. 2018. Mobile edge computing: a survey. IEEE Internet Things J. 5 (1), 450–465.

Abiodun, O.I., et al., 2019. Comprehensive review of artificial neural network applications to pattern recognition. IEEE Access 7, 158820–158846.

Aghili, S.F., et al., September 2017. DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT. Springer - The Journal of Supercomputing 54, 509–525.

Ahmad, S., et al., 2019. Enhancing fast TCP's performance using single TCP connection for parallel traffic flows to prevent head-of-line blocking. IEEE Access 7, 148152–148-162.

Aijaz, A., et al., April 2015. Cognitive machine-to-machine communications for internet-of-things: a protocol stack perspective. IEEE Internet of Things Journal 2 (2), 103–112.

Al-Ani, A.K., et al., 2020. Match-prevention technique against denial-of-service attack on address detection processes in IPv6 link-local network. IEEE Access 8, 27122–27138.

Al-Kaseem, B.R., et al., April 2019. End-to-End delay enhancement in 6LoWPAN testbed using programmable network concept. IEEE Internet of Things Journal 6 (2), 3070–3086.

Alabdulatif, A., et al., 2019. Secure edge of things for smart healthcare surveillance framework. IEEE Access 7, 31010–31021.

Albazrqaoe, W., et al., February 2019. A practical Bluetooth traffic sniffing system: design, implementation, and countermeasures. IEEE/ACM Trans. Netw. 27 (1), 71–84.

Aliyu, F., et al., 2018. A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing, vol. 141. Elsevier - Procedia Computer Science, pp. 24–31.

Almajed, H.N., et al., 2019. SE-enc: a secure and efficient encoding scheme using elliptic curve cryptography. IEEE Access 7, 175865–175878.

Amin, S.U., et al., 2019. Cognitive smart healthcare for pathology detection and monitoring. IEEE Access 7, 10745–10753.

Amjad, M., et al., May 2016. TinyOS-new trends, comparative views, and supported sensing applications: a review. IEEE Sensor. J. 16 (9), 2865–2889.

Ammar, M., et al., February 2018. Internet of Things: A Survey on the Security of IoT Frameworks, vol. 38. Elsevier – Journal of Information Security and Applications, pp. 8–27.

Ande, R., et al., March 2020. Internet of Things: Evolution and Technologies from a Security Perspective, vol. 54. Elsevier – Sustainable Cities and Society.

An, X., et al., 2019. Node state monitoring scheme in fog radio access networks for intrusion detection. IEEE Access 7, 21879–21888.

Anu, P., et al., 2017. A survey on sniffing attacks on computer networks. In: 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, pp. 1–5.

Atzori, L., et al., October 2010. The internet of things: a survey. Comput. Network. 54 (15), 2787–2805.

Aufner, P., June 2019. The IoT Security Gap: a Look Down into the Valley between Threat Models and Their Implementation, vol. 19. Springer – International Journal of Information Security, pp. 3–14.

Ayaz, M., et al., January 2018. Wireless sensor's civil applications, prototypes and future integration possibilities: a review. IEEE Sensor. J. 18 (1), 4–30.

Ayaz, M., et al., 2019. Internet-of-Things (IoT)-Based smart agriculture: toward making the fields talk. IEEE Access 7, 129551–129583.

Ayeni, B.K., et al., August 2018. Detecting cross-site scripting in web applications using fuzzy inference system. Hindawi - Journal of Computer Networks and Communications 2018, 1–10.

Baccarelli, E., et al., 2019. EcoMobiFog–design and dynamic optimization of a 5G mobile-fog-cloud multi-tier ecosystem for the real-time distributed execution of stream applications. in IEEE Access 7, 55565–55608.

Baccelli, E., et al., Dec. 2018. RIOT: an open source operating system for low-end embedded devices in the IoT. IEEE Internet of Things Journal 5 (6), 4428–4440.

Baldini, G., et al., Thirdquarter 2017. A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components. IEEE Communications Surveys & Tutorials 19 (3), 1761–1789.

Benkhelifa, E., et al., Fourthquarter 2018. A critical review of practices and challenges in intrusion detection systems for IoT: towards universal and resilient systems. IEEE Communications Surveys & Tutorials 20 (4), 2671–2701.

Bhuyan, M.H., et al., December 2018. Analyzing the communication security between smartphones and IoT based on CORAS. Proceedings of International Conference on Network and System Security 251–265.

Bing, Fu, 2016. The research of IOT of agriculture based on three layers architecture. In: 2016 2nd International Conference on Cloud Computing and Internet of Things (CCIOT), Dalian, pp. 162–165.

Borgohain, T., et al., 2015. Survey of Security and Privacy Issues of Internet of Things.

Caiza, G., et al., 2019. Industrial shop-floor integration based on AMQP protocol in an IoT environment. In: 2019 IEEE Fourth Ecuador Technical Chapters Meeting (ETCM). Ecuador, Guayaquil, pp. 1–6.

Canovas Sanchez, J.L., et al., 2018. Towards privacy preserving data provenance for the Internet of Things. In: 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, pp. 41–46.

Cao, X., et al., October 2015. An analytical MAC model for IEEE 802.15.4 enabled wireless networks with periodic traffic. IEEE Trans. Wireless Commun. 14 (10), 5261–5273.

Carracedo, J.M., et al., 2018. Cryptography for security in IoT. In: 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, Valencia, pp. 23–30.

Cerny, T., et al., June 2018. Survey of authentication and authorization for the internet of things. Hindawi – Security and Communication Networks 2018.

Chaabouni, N., et al., Thirdquarter 2019. Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials 21 (3), 2671–2701.

Chander, R.P.V., et al., 2012. A REST based design for Web of Things in smart environments. In: 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, Solan, pp. 337–342.

Chandrasekhar, S., et al., November 2015. Efficient and scalable query authentication for cloud-based storage systems with multiple data sources. IEEE Trans. Services Comput. 10 (4), 520–533.

Chang, W., et al., 2019. DeepCrash: a deep learning-based internet of vehicles system for head-on and single-vehicle accident detection with emergency notification. IEEE Access 7, 148163–148175.

Chen, R., et al., April 2016. Dual-server public-key encryption with keyword search for secure cloud storage. IEEE Trans. Inf. Forensics Secur. 11 (4), 789–798.

Chen, L., et al., 2017. Robustness, security and privacy in location-based services for future IoT: a survey. IEEE Access 5, 8956–8977.

Chen, Y., et al., Dec. 2019a. A new reversible data hiding in encrypted image based on multi-secret sharing and lightweight cryptographic algorithms. IEEE Trans. Inf. Forensics Secur. 14 (12), 3332–3343.

Chen, S., et al., 2019b. Internet of things based smart grids supported by intelligent edge computing. IEEE Access 7, 74089–74102.

Chiew, K.L., et al., September 2018. A Survey of Phishing Attacks: Their Types, Vectors and Technical Approaches, vol. 106. Elsevier - Expert Systems with Applications, pp. 1–20.

Chiu, T., et al., 1 . Latency-driven fog cooperation approach in fog radio access networks. IEEE Transactions on Services Computing 12 (5), 698–711.

Cho, S., et al., 2019a. Survey on the application of Blockchain to IoT. In: 2019 International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand, pp. 1–2.

Cho, C., et al., 2019b. Building on the distributed energy resources IoT based IEC 61850 XMPP for TPC. In: 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS), Taipei, Taiwan, pp. 61–66.

Costa, R., et al., June 2019. Handling real-time communication in infrastructured IEEE 802.11 wireless networks: the RT-WiFi approach. J. Commun. Network. 21 (3), 319–334.

Da Rocha, P.A.S., et al., 2019. An embedded system-based snap constrained trajectory planning. IEEE Access 7, 125188–125204.
Darlow, L.N., et al., 2017. Fingerprint minutiae extraction using deep learning. In: 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, pp. 22–30.
Das, A.K., et al., December 2018. Taxonomy and analysis of security protocols for Internet of Things. Elsevier - Future Generation Computer Systems 89, 110–125.
De Donno, M., et al., 2019. Foundations and evolution of modern computing paradigms: cloud, IoT, edge, and fog. IEEE Access 7, 150936–150948.
De, P., et al., May 2019. Path-balanced logic design to realize block ciphers resistant to power and timing attacks. IEEE Trans. Very Large Scale Integr. Syst. 27 (5), 1080–1092.
Dey, K.C., et al., June 2015. Potential of intelligent transportation systems in mitigating adverse weather impacts on road mobility: a review. IEEE Trans. Intell. Transport. Syst. 16 (3), 1107–1119.
Divarcı, S., et al., 2018. Secure gateway for network layer safety in IoT systems. In: 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, pp. 1–4.
El-Hajj, M., et al., March 2019. A survey of internet of things (IoT) authentication schemes. MDPI – Sensors 19 (5).
Eldrandaly, K.A., et al., 2019. Internet of spatial things: a new reference model with insight analysis. IEEE Access 7, 19653–19669.
Farris, I., et al., Firstquarter 2019. A survey on emerging SDN and NFV security mechanisms for IoT systems. IEEE Communications Surveys & Tutorials 21 (1), 812–837.
Fatayer, T.S., et al., 2019. IoT secure communication using ANN classification algorithms. In: 2019 International Conference on Promising Electronic Technologies (ICPET), Gaza City, Palestine, pp. 142–146.
Feng, Z., et al., May 2020. Secure cooperative event-triggered control of linear multiagent systems under DoS attacks. IEEE Trans. Contr. Syst. Technol. 28 (3), 741–752.
Garcia-Carrillo, D., et al., October 2018. Multihop bootstrapping with EAP through CoAP intermediaries for IoT. IEEE Internet of Things Journal 5 (5), 4003–4017.
Ghosal, A., et al., Thirdquarter 2019. Key management systems for smart grid advanced metering infrastructure: a survey. IEEE Communications Surveys & Tutorials 21 (3), 2831–2848.
Granjal, J., et al., 2015. Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials 17 (3), 1294–1312.
Gu, H., et al., March 2020. DIAVA: a traffic-based framework for detection of SQL injection attacks and vulnerability analysis of leaked data. IEEE Trans. Reliab. 69 (1), 188–202.
Hagan, M., et al., 2019. Enhancing security and privacy of next-generation edge computing technologies. In: 2019 17th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, pp. 1–5.
Hamamreh, J.M., et al., Secondquarter 2019. Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey. IEEE Communications Surveys & Tutorials 21 (2), 1773–1828.
He, D., et al., February 2015. An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE Internet of Things Journal 2 (1), 72–83.
Hernandez, L., et al., 2017. Implementing an edge-fog-cloud architecture for stream data management. In: 2017 IEEE Fog World Congress (FWC), Santa Clara, CA, pp. 1–6.
Hou, J., et al., January 2019. A Survey on the Internet of Things Security from the Data Perspective, vol. 148. Elsevier - Computer Networks, pp. 295–306.
Huang, K., et al., 2020. A low-cost distributed denial-of-service attack architecture. IEEE Access 8, 42111–42119.
Hu, J., et al., 2019. Network security situation prediction based on MR-SVM. IEEE Access 7, 130937–130945.
Hu, R., et al., March 2020. A Survey on Data Provenance in IoT, vol. 23. Springer – World Wide Web, pp. 1441–1463.
Huynh, C.N., et al., 2019. Controlling web traffic and preventing DoS/DDoS attacks in networks with the proxy gateway security solution built on open hardware. In: 2019 International Conference on System Science and Engineering (ICSSE), Dong Hoi, Vietnam, pp. 239–244.
Hwang, K., et al., 2013. Model-based indirect learning method based on dyna-Q architecture. In: 2013 IEEE International Conference on Systems, Man, and Cybernetics, Manchester, pp. 2540–2544.
Imran, M., et al., March 2019. Enabling Technologies for Social Internet of Things, vol. 92. Elsevier – Future Generation Computer Systems, pp. 715–717.
Jankowski, K., et al., Jan. 2011. Packed AES-GCM algorithm suitable for AES/PCLMULQDQ instructions. IEEE Trans. Comput. 60 (1), 135–138.
Jensen, M., et al., 2011. On the effectiveness of XML Schema validation for countering XML Signature Wrapping attacks. In: 2011 1st International Workshop on Securing Services on the Cloud (IWSSC), Milan, pp. 7–13.
Jin, Y., et al., 2018. Content centric cross-layer scheduling for industrial IoT applications using 6TiSCH. IEEE Access 6, 234–244.
Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D., 2014. Security of the internet of things: perspectives and challenges. Springer - Wireless Networks 20 (8), 2481–2501.
Joseph, T., et al., 2017. IoT middleware for smart city: (An integrated and centrally managed IoT middleware for smart city). In: 2017 IEEE Region 10 Symposium (TENSYMP), Cochin, pp. 1–5.
Kaiser, D., et al., 2014. Efficient privacy preserving multicast DNS service discovery. In: 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst (HPCC,CSS,ICESS), Paris, pp. 1229–1236.
Kaur, N., et al., June 2017. An energy-efficient architecture for the internet of things (IoT). IEEE Systems Journal 11 (2), 796–805.
Keophilavong, T., et al., 2019. Data transmission in machine to machine communication protocols for internet of things application: a review. In: 2019 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, pp. 899–904.
Khalid, A., et al., 2019. Lattice-based cryptography for IoT in A quantum world: are we ready?. In: 2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI), Otranto, Italy, pp. 194–199.
Khan, A.Y., et al., 2020. Malicious insider attack detection in IoTs using data analytics. in IEEE Access 8, 11743–11753.
Kolozali, Ş., et al., April 2019. Observing the pulse of a city: a smart city framework for real-time discovery, federation, and aggregation of data streams. IEEE Internet of Things Journal 6 (2), 2651–2668.
Kumar, P., et al., April 2017a. Anonymous secure framework in connected smart home environments. IEEE Trans. Inf. Forensics Secur. 12 (4), 968–979.
Kumar, J., et al., 2017b. XML wrapping attack mitigation using positional token. In: 2017 International Conference on Public Key Infrastructure and its Applications (PKIA), Bangalore, pp. 36–42.
Kumar, S., et al., December 2019. Internet of Things Is a Revolutionary Approach for Future Technology Enhancement: a Review, vol. 6. Springer – Journal of Big Data.
Li, C., Chen, C., 2011. A multi-stage control method application in the fight against phishing attacks. In: Proc. 26th Comput. Secur. Acad. Commun. Across Country, p. 145.
Li, S., et al., 2018. An improved information security risk assessments method for cyber-physical-social computing and networking. IEEE Access 6, 10311–10319.
Li, J., et al., 2019a. A remote monitoring and diagnosis method based on four-layer IoT frame perception. IEEE Access 7, 144324–144338.
Li, L., et al., Nov. 2019b. An energy-efficient privacy preserving security-oriented DSA with low latency. IEEE Trans. Veh. Technol. 68 (11), 11283–11294.
Li, Z., et al., May 2020. Breaking the hardness assumption and IND-CPA security of HQC submitted to NIST PQC project. IET Inf. Secur. 14 (3), 313–320.
Lin, C., et al., June 2013. Enhancing the Attacking Efficiency of the Node Capture Attack in WSN: a Matrix Approach, vol. 66. Springer - The Journal of Supercomputing, pp. 989–1007.
Lin, J., et al., October 2017. A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things Journal 4 (5), 1125–1142.
Liu, X., et al., Sept. 2015. A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure. IEEE Transactions on Smart Grid 6 (5), 2435–2443.
Liu, J., et al., 2016. Searchable encryption scheme on the cloud via fully homomorphic encryption. In: 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, pp. 108–111.
Liu, X., et al., November 2019a. Overview of spintronic sensors with internet of things for smart living. IEEE Trans. Magn. 55 (11), 1–22.
Liu, X., et al., 2019b. A blockchain-based medical data sharing and protection scheme. IEEE Access 7, 118943–118953.
Lo Bello, L., et al., June 2019. A perspective on IEEE time-sensitive networking for industrial communication and automation systems. Proc. IEEE 107 (6), 1094–1120.
Lu, X., et al., 2019. Secure internet of things (IoT)-Based smart-world critical infrastructures: survey, case study and research opportunity. IEEE Access 7, 79523–79544.
Ma, G., et al., 2017a. A security routing protocol for internet of things based on RPL. In: 2017 International Conference on Networking and Network Applications (NaNA), Kathmandu, pp. 209–213.
Ma, G., et al., 2017b. A security routing protocol for internet of things based on RPL. In: 2017 International Conference on Networking and Network Applications (NaNA), Kathmandu, pp. 209–213.
Ma, J., et al., 2017c. A new countermeasure against side channel attack for HMAC-SM3 hardware. In: 2017 IEEE 12th International Conference on ASIC (ASICON), Guiyang, pp. 327–330.
Ma, J., et al., 2018. An efficient retransmission scheme for reliable end-to-end wireless communication over WSANs. in IEEE Access 6, 49838–49849.
Mehta, R., et al., 2018. Internet of Things: Vision, Applications and Challenges, vol. 2018. Elsevier – Procedia Computer Science, pp. 1263–1269.
Menegheilo, F., et al., October 2019. IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal 6 (5), 8182–8201.
Meng, Z., et al., April 2019. RFID-based object-centric data management framework for smart manufacturing application. IEEE Internet of Things Journal 6 (2), 2706–2716.
Meraoumia, A., et al., 2015. Finger-Knuckle-Print identification based on histogram of oriented gradients and SVM classifier. In: 2015 First International Conference on New Technologies of Information and Communication (NTIC), Mila, pp. 1–6.
Mohammad, N., 2019. A multi-tiered defense model for the security analysis of critical facilities in smart cities. IEEE Access 7, 152585–152598.
Navani, D., et al., 2017. The internet of things (IoT): a study of architectural elements. In: 2017 13th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Jaipur, pp. 473–478.
Naveed, M., et al., May 2014. Dynamic searchable encryption via blind storage. In: Proc. IEEE Symp. Secur. Privacy, pp. 639–654.
Neshenko, N., et al., Thirdquarter 2019. Demystifying IoT security: an exhaustive survey on vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials 21 (3), 2702–2733.
Neureiter, C., et al., 2013. Towards a framework for engineering smart-grid-specific privacy requirements. In: IECON 2013-39th Annual Conference of the IEEE Industrial Electronics Society, Vienna, pp. 4803–4808.

Ngu, A.H., et al., February 2017. IoT middleware: a survey on issues and enabling technologies. IEEE Internet of Things Journal 4 (1), 1–20.
Ni, J., et al., Firstquarter 2018. Securing fog computing for internet of things applications: challenges and solutions. IEEE Communications Surveys & Tutorials 20 (1), 601–628.
Noor, M.M., et al., December 2018a. Current Research on Internet of Things (IoT) Security: A Survey, vol. 148. Elsevier – Computer Networks, pp. 283–294.
Noor, M.M., et al., December 2018b. Current Research on Internet of Things (IoT) Security: A Survey, vol. 148. Elsevier – Computer Networks, pp. 283–294.
Noura, H.N., et al., 2019. Secure and lightweight mutual multi-factor Authentication for IoT communication systems. In: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), Honolulu, HI, USA, pp. 1–7.
Palattella, M.R., et al., Thirdquarter 2013. Standardized protocol stack for the internet of (important) things. IEEE Communications Surveys & Tutorials 15 (3), 1389–1406.
Pan, Z., et al., 2015. Building and testing network security situational awareness model based on Bayesian method. In: Third International Conference on Cyberspace Technology (CCT 2015), Beijing, pp. 1–4.
Papamanthou, C., et al., 2013. Signatures of correct computation. In: Proc. Theory Cryptogr. Conf. Springer, pp. 222–242.
Pathan, A.K., et al., March 2019. Internet of Things for Smart Living. Springer –Wireless Networks.
Perera, C., et al., November 2016. Privacy-by-Design framework for assessing internet of things applications and platforms. Proceedings of the 6th International Conference on the Internet of Things 83–92.
Ping-Chen, X., 2011. SQL Injection Attack and Guard Technical Research, vol. 15. Elsevier - Procedia Engineering, pp. 4131–4135.
Popescul, D., et al., 2014. Internet of things–some ethical issues. The USV Annals of Economics and Public Administration 13 (2), 208–214, 18.
Pranata, I., et al., December 2012. Securing and governing access in ad-hoc networks of internet of things. In: Proceedings of the IASTED International Conference on Engineering and Applied Science, Colombo, Sri Lanka, pp. 84–90.
Puthal, D., et al., May 2019. Fog computing security challenges and future directions [energy and security]. IEEE Consumer Electronics Magazine 8 (3), 92–96.
Qi, Q., et al., 2019. A smart manufacturing service system based on edge computing, fog computing, and cloud computing. IEEE Access 7, 86769–86777.
Qu, L., et al., October 2016. Performance enhancement of ground radiation antenna for Z-wave applications using tunable metal loads. Electron. Lett. 52 (22), 1827–1828.
Quincozes, S., et al., September 2019. MQTT protocol: fundamentals, tools and future directions. IEEE Latin America Transactions 17 (9), 1439–1448.
Quist-Aphetsi, K., et al., 2019. A hybrid data logging system using cryptographic hash blocks based on SHA-256 and MD5 for water treatment plant and distribution line. In: 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, pp. 15–18.
Rahman, M., et al., March 2020. A systematic methodology for the time-domain ringing reduction in UWB band-notched antennas. IEEE Antenn. Wireless Propag. Lett. 19 (3), 482–486.
Ray, P.P., July 2018. A survey on Internet of Things architectures. Elsevier – Journal of King Saud University-Computer and Information Sciences 30 (3), 291–319.
Refaey, A., et al., 31-10-2019. On IoT applications: a proposed SDP framework for MQTT. Electron. Lett. 55 (22), 1201–1203.
Rong-Bing, W., et al., 2019. Electronic scoring scheme based on real paillier encryption algorithms. IEEE Access 7, 128043–128053.
Sabir, M.Z., et al., 2018. Design and Implementation of an End-To-End Web Based Trusted Email System, vol. 141. Elsevier - Procedia Computer Science, pp. 231–238.
Saied, Y.B., et al., May 2014. Lightweight collaborative key establishment scheme for the Internet of Things. Elsevier – Computer Networks 64, 273–295.
Saint-Andre, P., 2011. Extensible Messaging and Presence Protocol (XMPP): Core. Internet Eng. Task Force (IETF), Fremont, CA, USA, Request for Comments: 6120.
Samaila, M.G., et al., May 2018. Challenges of securing Internet of Things devices: a survey. Wiley – Security and Privacy 1 (2).
Seeam, A., et al., 2019. Threat modeling and security issues for the internet of things. In: 2019 Conference on Next Generation Computing Applications (NextComp), Mauritius, pp. 1–8.
Shouqi, C., et al., 2019. An improved anonymous authentication protocol for location-based service. IEEE Access 7, 114203–114212.
Silva, J.D.C., et al., 2019. M4DN.IoT-A networks and devices management platform for internet of things. IEEE Access 7, 53305–53313.
Silvera-Tawil, D., et al., March 2020. Emerging Technologies for Precision Health: an Insight into Sensing Technologies for Health and Wellbeing, vol. 15. Elsevier – Smart Health.
Singh, A.K., et al., January 2012. Analysis of cryptographically replay attacks and its mitigation mechanism. In: Proceedings of the International Conference on Information Systems Design and Intelligent Applications 2012 (INDIA 2012), Visakhapatnam, India, pp. 787–794.
Skoberne, N., et al., April 2014. IPv4 address sharing mechanism classification and tradeoff analysis. IEEE/ACM Trans. Netw. 22 (2), 391–404.
Stanciu, A., et al., May 2017. Securing the IoT gateway based on the hardware implementation of a multi pattern search algorithm. In: Proc. Int. Conf. Optim. Elect. Electron. Equip. (OPTIM) Int. Aegean Conf. Elect. Mach. Power Electron. (ACEMP), pp. 1001–1006.
Stolikj, M., et al., 2014. Proxy support for service discovery using mDNS/DNS-SD in low power networks. In: Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, Sydney, NSW, pp. 1–6.
Sun, D., et al., September 2017. Man-in-the-middle Attacks on Secure Simple Pairing in Bluetooth Standard V5.0 and its Countermeasure, vol. 22. Springer - Personal and Ubiquitous Computing, pp. 55–67.
Sung, W., et al., November 2013. Intelligent environment monitoring system based on innovative integration technology via programmable system on chip platform and ZigBee network. IET Commun. 7 (16), 1789–1801.
Takahashi, M., et al., 2009. Demo abstract: design and implementation of a web service for liteos-based sensor networks. In: 2009 International Conference on Information Processing in Sensor Networks, San Francisco, CA, pp. 407–408.
Tan, S., 2018. Comment on "secure data access control with ciphertext update and computation outsourcing in fog computing for internet of things. IEEE Access 6, 22464–22465.
Tandale, U., et al., 2017. An empirical study of application layer protocols for IoT. In: 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, pp. 2447–2451.
Thakore, R., et al., 2019. Blockchain – based IoT: a survey. Elsevier – Procedia Computer Science 155, 704–709.
The Hacker News. Dark Nexus: a new emerging IoT botnet malware spotted in the wild [Online]. Available: https://thehackernews.com/2020/04/darnexus-iot-ddos-botnet.html?m=1. (Accessed April 2020).
Tietz, L.H.B., 2016. Development of an Architecture for a Tele-Medicine-Based Longterm Monitoring System.
Tomić, I., et al., December 2017a. A survey of potential security issues in existing wireless sensor network protocols. IEEE Internet of Things Journal 4 (6), 1910–1923.
Tomić, I., et al., December 2017b. A survey of potential security issues in existing wireless sensor network protocols. IEEE Internet of Things Journal 4 (6), 1910–1923.
Torr, P., 2005. Demystifying the threat modeling process. IEEE Security & Privacy 3 (5), 66–70.
Tsai, K., et al., 2018. AES-128 based secure low power communication for LoRaWAN IoT environments. IEEE Access 6, 45325–45334.
Tschofenig, H., et al., Sept.-Oct. 2019. Cyberphysical security for the masses: a survey of the internet protocol for internet of things security. IEEE Security & Privacy 17 (5), 47–57.
Tukur, Y.M., et al., 2019. Ethereum blockchain-based solution to insider threats on perception layer of IoT systems. In: 2019 IEEE Global Conference on Internet of Things (GCIoT), Dubai. United Arab Emirates, pp. 1–6.
Vasilevskaya, M., et al., 2016. Model-based security risk analysis for networked embedded systems. Lect. Notes Comput. Sci. 8985, 381.
Virat, M.S., et al., 2018. Security and privacy challenges in internet of things. In: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, pp. 454–460.
Waher, P., et al., 2013. Efficient XML Interchange (EXI) Format. Std. XEP-0322.
Walkowiak, K., et al., 2011. Shared backup path protection for anycast and unicast flows using the node-link notation. In: 2011 IEEE International Conference on Communications (ICC), Kyoto, pp. 1–6.
Wang, P., Chen, X., Ye, F., Sun, Z., 2018. A smart automated signature extraction scheme for mobile phone number in human-centered smart home systems. IEEE Access 6, 30483–30490.
Wang, X., et al., December 2019a. On remote temperature sensing using commercial UHF RFID tags. IEEE Internet of Things Journal 6 (6), 10715–10727.
Wang, D., et al., 2019b. Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city. IEEE Access 7, 54508–54521.
Wang, J., et al., August 2019c. Dynamic scalable elliptic curve cryptographic scheme and its application to in-vehicle security. IEEE Internet of Things Journal 6 (4), 5892–5901.
Wei, Z., 2015. A BGN-type multiuser homomorphic encryption scheme. In: 2015 International Conference on Intelligent Networking and Collaborative Systems, Taipei, pp. 268–271.
Wei, S., et al., February 2019. An integrated longitudinal and lateral vehicle following control system with radar and vehicle-to-vehicle communication. IEEE Trans. Veh. Technol. 68 (2), 1116–1127.
Wu, M., et al., 2010. Research on the architecture of internet of things. in Proc. 3rd ICACTE V5-484–V5-487.
Xiao, L., Wan, X., Lu, X., Zhang, Y., Wu, D., Sep. 2018. ``IoT security techniques based on machine learning: how do IoT devices use AI to enhance security?'. IEEE Signal Process. Mag. 35 (5), 41–49.
Xiao, L., et al., Dec. 2016. PHY-layer spoofing detection with reinforcement learning in wireless networks. IEEE Trans. Veh. Technol. 65 (12), 10037–10047.
Xiao, G., et al., March 2018a. Printed UHF RFID reader antennas for potential retail applications. IEEE Journal of Radio Frequency Identification 2 (1), 31–37.
Xiao, L., et al., March 2018b. PHY-layer authentication with multiple landmarks with reduced overhead. IEEE Trans. Wireless Commun. 17 (3), 1676–1687.
Xie, H., et al., April 2019. Data collection for security measurement in wireless sensor networks: a survey. IEEE Internet of Things Journal 6 (2), 2205–2224.
Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H., Oct. 2017. A survey on security and privacy issues in Internet-of-Things. IEEE Internet Things J. 4 (5), 1250–1258.
Yaseen, M., et al., October 2019. MARC: A Novel Framework for Detecting MITM Attacks in eHealthcare BLE Systems, vol. 43. Springer - Journal of Medical Systems.
Yassein, M.B., et al., 2016. Application layer protocols for the Internet of Things: a survey. In: 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, pp. 1–4.
Yi, S., et al., 2015. A survey of fog computing: concepts, applications and issues. Proc. Workshop Mobile Big Data 37–42.
Yin, D., et al., 2018. A DDoS attack detection and mitigation with software-defined internet of things framework. IEEE Access 6, 24694–24705.
Yu, W., et al., 2018a. A survey on the edge computing for the Internet of Things. IEEE Access 6, 6900–6919.

Yu, H., et al., October 2018b. Spoofing detection in automatic speaker verification systems using DNN classifiers and dynamic acoustic features. IEEE Transactions on Neural Networks and Learning Systems 29 (10), 4633–4644.
Yu, J., et al., 2019a. Analysis of IoT platform security: a survey. In: 2019 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea (South), pp. 1–5.
Yu, S., et al., August 2019b. A secure lightweight three-factor Authentication scheme for IoT in cloud computing environment. MDPI – Sensors 19 (16).
Yıldırım, G., et al., 2018. Simplified agent-based resource sharing approach for WSN-WSN interaction in IoT/CPS projects. IEEE Access 6, 78077–78091.
Zeadly, S., et al., June 2019. Cryptographic technologies and protocol standards for internet of things. Elsevier – Internet of Things. https://doi.org/10.1016/j.iot.2019.10.0.075.
Zhang, K., et al., October 2019. Deep learning empowered task offloading for mobile edge computing in urban informatics. IEEE Internet of Things Journal 6 (5), 7635–7647.
Zhao, Y.L., et al., 2013. Research on data security technology in internet of things. Appl. Mech. Mater. 433–435.
Zhao, A., et al., 2017. Dual-resonance NFC antenna system based on chip antenna. IEEE Antenn. Wireless Propag. Lett. 16, 2856–2860.
Zheng, C., et al., May 2019. A quasi-perfect resource allocation scheme for optimizing the performance of cell-edge users in FFR-aided LTE-A multicell networks. IEEE Commun. Lett. 23 (5), 918–921.
Zhou, W., et al., April 2019a. The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal 6 (2), 1606–1616.
Zhou, P., et al., March 2019b. Differentially-private and trustworthy online social multimedia big data retrieval in edge computing. IEEE Trans. Multimed. 21 (3), 539–554.

Mobasshir Mahbub is currently engaged in Post-Graduation (MSc Engineering) in Electrical and Electronic Engineering under the Department of Electrical and Electronic Engineering at Ahsanullah University of Science and Technology, Dhaka, Bangladesh. He graduated (September, 2018) in Electronic and Telecommunication Engineering under the Department of Electronics and Communications Engineering at East West University, Dhaka, Bangladesh with an outstanding academic performance (Merit Scholarship and Dean's List Award). His fields of interest are Circuit Design & Analysis, Embedded Electronics, IoT, IoT Security, Intelligent IoT-Enabled Gadgets, Robotics, Microcontroller Interfacing, Wireless Communications, PCB Designing, etc. He served as a Project Engineer, in Transport Network Rollout Department under the Technology Division of Robi Axiata Ltd., a renowned telecom operator of Bangladesh. He has two book chapter publications with Springer, eight research paper publications in reputed international journals and four conference publications in reputed international conferences. He served as organizer and instructor in several workshops on IoT and Embedded System. He has been serving as a reviewer for reputed journals like Springer, IEEE, Wiley, and Emerald and served as reviewer for several international conferences. He is currently engaged in research on the above mentioned topics.