DOI 10.12694/scpe.v20i3.1544
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 20, Number 3, pp. 457–484. http://www.scpe.org © 2019 SCPE

ASSESSING THE SERVICES, SECURITY THREATS, CHALLENGES AND SOLUTIONS IN THE INTERNET OF THINGS

SYED RAMEEM ZAHRA AND MOHAMMAD AHSAN CHISHTI[*]

Abstract. The purpose of this paper is to chalk out the criticality of the most important pillar of the Internet of Things (IoT), i.e., Security and Privacy (S&P). IoT has seen its journey from implausible and impossible to sustainable and tenable. Its rate of expansion into various grounds from agriculture to sports; personal health to intelligent traffic detection; waste management to smart homes is astonishing, dramatic, and unforeseen. With such vast adaptability and functionality, its security remains the biggest concern because, in contrast to the traditional networks, IoT faces huge vulnerabilities, some of which are inherent and others explicit. The existing security solutions cannot be implemented in IoT because of its unique characteristics. Therefore, there is a dire need to develop novel security procedures befitting IoT. This paper spots the features that are peculiar to IoT and concurrently analyzes the security threats, and challenges they pose. This work also provides a glimpse of the major IoT implementations with their particular security requirements and challenges. Moreover, this paper critically evaluates the proposed countermeasures to security attacks on different features and why they cannot be used in IoT environments. Also, it is found that most of the security solutions used in IoT devices are inspired by Wireless Sensor Networks (WSN, but the striking differences among the two make them inadequate in IoT. The security requirements and challenges peculiar to various IoT services are also identified. To assist the researchers in remaining up-to-date, we for the first time have thoroughly expressed some of the most famous and practical attacks faced across the world in the recent past, how much damage they caused, how many financial losses were faced, etc.

Key words: Internet of Things, Security, Privacy, Vulnerabilities, Wireless Sensor Networks.

AMS subject classifications. 68M14, 68M10

1. Introduction. Internet of Things (IoT) pilots the automation in an ample number of realms ranging from management of items with trivial importance like thermostats to the management of life-saving medical implants. The application spectrum of IoT runs from monitoring the dampness in crops, to auditing the flow of items through a production line, to remotely observing the patients with interminable illnesses and overseeing their restorative devices. It is to say that the potential application areas of IoT are innumerable and diverse, percolating into all the spheres of individual lives as well as into the enterprises and society as a whole. The European Research Cluster on the Internet of Things (IERC) identifies primal applications of IoT that span numerous domains and describe them as Smart City, Smart Health, Smart Buildings, Smart Transport, and Smart Industry.

As IoT maneuvers past a catchphrase and begins to offer solutions to such a wide range of multi-faceted problems, a clear understanding of 3 of its vital pillars has been achieved [1] a) the foundation of contextual awareness is laid by the blend of sensors and actuators which make the interaction with the environment as well as the transformation of stimulus to data and vice versa possible b) the devices used in IoT are highly constrained in terms of power, bandwidth, processing abilities, memory, and size. Hence in the missions where less latency, consideration to less bandwidth usage and real-time analytics is needed, local edge computing and fog computing become essential c) data exchange between the IoT devices and the local aggregators or cloud happens through low power communication links.

Left out from this picture, and not completely acknowledged yet, is the fourth pillar of IoT: Security and Privacy (S&P). Given that all the vital elements of IoT- people, processes and things work together just to create more data and to extract profitable and relevant information from that data, then how the S&P is dealt with will decide the destiny of IoT i.e. whether there will be a second round of rapid expansion and escalation of IoT or an extreme downfall and debacle.

Recent breaks in S&P are changing the way businesses view this matter because even the tiny IoT devices that have restricted functionality pose serious dangers to the entire security system of the network when their security is compromised. This is because by connecting everything to the internet, IoT creates a huge attack surface for the rogue players and weak points could easily be targeted and compromised to set off an attack and steal sensitive data. Therefore our approach of looking at IoT should be changed, making S&P a vital

[*] Department of Computer Science Engineering, National Institute of Technology Srinagar, India. (rameemzahra@gmail.com).

requirement at the design phase itself. Also, the major research conducted in the direction of S&P of IoT mainly tries to adapt the security solutions aimed at Wireless Sensor Networks (WSN) and internet to IoT [2]. However, on contemplating the inherent features of IoT and its differences from WSN, we come across a glaring reality which says that IoT challenges take another dimension which is a long way from being anything but difficult to defeat with customary solutions. In essence, the contribution of this paper includes:

1. Identification of basic features of IoT and how they constitute the internal security vulnerabilities of IoT devices.
2. Primal applications of IoT are studied from their security point of view.
3. An exhaustive study of various papers and projects proposed in the realm of IoT applications and security.
4. Examination of various attacks targeting the vulnerabilities of IoT devices and causing huge financial losses.
5. The critical analysis of existing threats and challenges about the identified features.

The rest of the paper is organized as follows: Section 2 gives a background about the intrinsic IoT features which are fundamental to any IoT application. Section 3, describes how IoT is different from WSN. In Section 4, we discuss in detail 5 important IoT application use cases that are identified by IERC. It also sketches out the security challenges and requirements of the described IoT applications. The major threats, challenges and the proposed solutions posed in the entire IoT environment by the intrinsic IoT features are discussed in Section 5. It also describes the problems that exist with the given solutions. Section 6 describes a simple security mechanism for Smart Transport with an experimental evaluation. Finally Section 7 concludes the paper.

2. Inherent IoT Features. Less storage capacity, small battery back-up, and limited compute ability mark the identity of IoT devices. As such, constrained is one of the inherent features of these devices. Apart from being constrained, the uniqueness of IoT devices is marked by features like Interdependence, Heterogeneity, Constrained, Pervasiveness, Unattended, Affinity, and Mobility [3]. These features also represent the critical inherent vulnerabilities of IoT devices and are briefly explained below:

1. **Interdependence:** The root cause of security risk in the IoT environment is dependence. With the evolutionary increase in the number of IoT devices, the communication among the devices become complex since they no longer communicate only by explicit pinging but implicitly as well by using services like IFTTT (If this, then that).

   In IFTTT, the company offers a software platform that connects the devices, applications, and services belonging to diverse developers to each other to initiate one or more automation involving those devices, applications, and services. For example, the automation happens like, if one makes a phone call on his/her android phone, then a call log will be added to Google Spreadsheet, if smoke is seen, then turn lights to red color, If I am out of home, and sight hound detects a person, turn lights to red color, If a thermometer senses the room temperature to be higher than the threshold and the smart plug detects that the AC to be switched off, then the windows would automatically open [3]. This feature is called interdependence or implicit dependence of the IoT devices.
2. **Heterogeneity:** The different kind of protocols used among the devices, range of interfaces and firmware employed, their varying storage capacities, the various access control mechanisms employed and the different authentication and communication protocols that are utilized make heterogeneity an important feature of IoT devices.

   This heterogeneity in the hardware, software, and process requirements is justified by the diverse functions of IoT devices. The protocols employed in IoT can range from being completely free to consortia-driven standards such as ZigBee or WirelessHART, to completely proprietary. Another reason for this heterogeneity is the wide variety of applications covered by IoT that require the different number of devices to operate; different communication ranges for their devices, different latencies and reliabilities, varied network coverage, and traffic loads [4]. Also, the applications might require utilizing diverse energy sources and having distinctive prerequisites on energy proficiency and lifetime [4].
3. **Constrained:** The IoT devices are designed to meet different requirements and as such, are diverse. For example, the implantable medical sensor devices have to be small in size as well as lightweight, implying that their computing abilities and storage capacities will be little. Similarly, the devices

meant for defense purposes have to remain deployed in war zones, implying that their batteries cannot be changed now and then and that their power consumption has to be less [2,3]. The same limitation applies to devices installed in the agricultural and industrial fields. Also, the devices utilized in the genre of robot control systems and automotive vehicle systems need to work under strict deadlines and hence are constrained by time. In essence, it can be said that constrained is one of the basic features of IoT.

4. **Pervasive:** It is estimated by Cisco that by 2020, every person would be surrounded by an average of 6.58 devices [2], which makes a humongous approximation of 50 billion IoT devices by 2020. As IoT devices would soon be seen everywhere, human beings would find themselves dependent on these devices just like air and water [3]. The feature of IoT to exist everywhere is referred to as Pervasiveness. Moreover, due to their rapid proliferation, the amount of data that IoT devices produce, send, and use go to the astronomical figures. Let us take the example of a supermarket where every item is Radio Frequency Identification (RFID) tagged. The raw RFID data format stands like EPC, Location and Time where EPC is the unique identification that is read by the RFID reader; location marks the place where the reader is positioned, and time represents the time when the reading was performed. To save any raw RFID record, 18 bytes of storage are required. Let us suppose; there are almost 700,000 tagged items present in the supermarket, hence if the supermarket possesses readers that scan the items every second, about 12.6 GB RFID data will be produced per second which makes to a whopping 544 TB in 24 hours [5]. Hence, for managing, analyzing, and mining RFID data, effective methods must be developed.
5. **Unattended:** Implantable medical sensors, sensors installed in the battle fields, the smart meters, the devices used in agricultural and industrial areas have to perform their functions for long periods after they are installed and because of the nature of their functions, they remain unattended during these periods [3].
6. **Affinity:** As the wearable devices and smart home products become commonplace, the privacy issues creep in; IoT devices not only collect the information such as pulse, blood pressure, etc. but also tend to record the environmental conditions like the places you have visited, the temperature of the room, etc. The sensors deployed on the roads to measure the levels of noise can record the conversation of 2 individuals and thus pose a threat to their privacy. Similarly, when people give consent to save their credentials to allow the smart TV to automatically download the content of your choice, a strong security and privacy breach can happen just by hacking onto that TV. This feature is thus named affinity since the IoT users and the devices share a close relationship with each other.
7. **Mobility:** Many IoT devices can roam from one place to another, e.g., wearable devices move as the individuals move. Similarly, the smart vehicles move from one district to another, collecting road information as they move.

   As per the International Telecommunication Union (ITU), the number of mobile users today in the world stands at a staggering figure of 7.3 billion. It is not possible to manage and support these devices using the old versions of the IP protocol. Hence newer versions like IPv6 over Low Power Personal Area Networks (6LoWPAN) were developed to support mobility and other constrained features of IoT devices [6].

3. How IoT differs from WSN. One of the major empowering technologies of IoT is the Wireless Sensor Network (WSN) [7]. The sensors used in WSN are curbed resource wise [8] as are the end nodes in IoT. Moreover, similar challenges to the design of a security system exist between WSN and IoT. Nonetheless, security issues in WSN are less challenging as compared to those of IoT [9], and thus, the security solutions applicable to WSN do not fit IoT. This is well explained by the exclusive differences in the targeted applications of the two and their distinctive characteristics as pointed out in Table 3.1.

- Primarily, the most famous and targeted applications of WSNs include the ones requiring data collection, e.g., surveillance [15] and environmental monitoring [16]. In these systems, the WSN sensors collect data and transmit it using the multi-hop routing protocols [10] to the WSN sinks. This communication is unidirectional; the reverse direction is used only to manage the sensors by sending them the control messages, i.e., the control messages only provide instructions for the sensors and do not control or

Table 3.1
Comparison of WSN and IoT Features.

Features	**WSN**	**IoT**
Impact on the physical world [9]	Insignificant just monitor the surroundings	Significant impact
Heterogeneity [9]	Made up of homogeneous devices	Communications as well as devices are heterogeneous
Communication [10]	Unidirectional	Bidirectional
Privacy Expectations[11]	Less	Very high
Scalability [11]	Large scale	Extremely large
Interdependence	Not present among applications	Applications highly interdependent
Mobility [11]	Node is said to be mobile only when it moves inside a sensor network	It is said to be mobile not only when it moves within the network but also when it moves between various service providers at the network layer
Things identification [12]	Not required as the main focus of WSN is the correlative acquisition of data	Unique identification is a must for establishing communication
Internet connection [11]	Not necessary, usually connected via a wireless connection medium	A mandatory feature.
Constraints [13]	energy	Computational, storage, and energy.
Closeness to the owner	The devices used in WSN do not share a close bond with the owner	A very close relationship with the owner is created
The Protocol used at physical/ perception layer for communication [14]	Wireless Fidelity (Wi-Fi)	6LoWPAN
The Protocol used at the network layer for communication [14]	Transmission Control Protocol (TCP)	Datagram Transport Layer Security (DTLS)
The Protocol used at application layer for communication [14]	HyperText Transfer Protocol (HTTP)	Constrained Application Protocol (CoAP)

modify the associated physical world; thereby WSN doesnt have a significant impact on it [9]. On the other hand, there is a strong coupling between the cyber world and the physical world in the IoT systems. As a result, IoT puts a considerably noteworthy impact on the physical world, and hence, it is necessary that the security of the physical system be considered as part of the security design.

- The sensors in WSNs, as well as the end nodes in IoT, are constrained of resources; while WSN sensors usually face constraints only in terms of the energy availabilities [13], the IoT devices suffer from a plethora of such constraints (memory, energy, computability, etc). As such, the device centric security mechanisms (software patches or anti-viruses) cannot be expected to be used in IoT. For example, the storage space required for a mere antivirus exceeds the total RAM of a normal IoT device, e.g., Common touch antivirus demand 128 MB RAM whereas most IoT devices own a single-threaded microcontroller (8051,MSP430, ATMEL series) that has got less than 2 MB RAM.
  This makes the security of IoT end devices more challenging. Since they cannot support encryption algorithms, frequency hopping communication [17], anti-viruses, etc. lightweight encryption is employed for IoT devices.
- The sensors in WSN are mostly homogenous [9], but there is a huge factor of heterogeneity involved in IoT as the devices vary in the type of protocols they use, architecture, size, functions, operating systems, etc. This makes it tricky to build a generic security solution for these heterogeneous IoT devices.
- Representing one of the peer-peer ad-hoc networks, WSNs are generally designed for one particular application and each WSN remains detached, and works independently of other WSNs [15]. On the other hand, the essence of IoT is that it interconnects multiple domain-specific autonomous systems, including WSNs.
- The scalability of IoT is huge, hence to maintain the key management system is difficult. The heterogeneity of devices makes the process even more complex in IoT. The most famous key management scheme used in WSN is the random key distribution [18, 19]. The scheme has enough scalability to support WSN but not good enough to support IoT scalability.

- Moreover, it utilizes a centralized key pool which lacks in IoT, thereby making it extremely difficult to apply random key distribution in IoT. Another famous key distribution mechanism is the polynomial based key pre-distribution [20, 21] but it cannot be applied in IoT because it demands heavy computational overhead and a lot of memory as well. Therefore, new key distribution mechanisms are needed to be built for IoT.
- Finally, the data collected by WSN applications is less human-related as compared to the data collected by IoT applications. Therefore, on analysis of the data transmitted by the IoT devices, personal information of people can be deduced, making privacy a huge concern.

Hence, we can conclude that the Security and Privacy issues and requirements in IoT are much higher than those of WSNs and thus the security solutions meant for WSNs cannot be adapted in the environment of IoT.

4. IoT applications with their security requirements and challenges. In this section, we illustrate five important IoT applications identified by IERC and highlight the services, particular security requirements, and challenges of each application. This section brings into highlight the vast services offered by IoT but also hints towards the major security and privacy hurdle that comes along with this comfort and ease.

4.1. Smart City. While there remains a conflict on any single definition of a smart city [22, 23], its common contemporary understanding brings us to the following Smart City features: Smart Energy, Smart Mobility, Smart Healthcare, Smart Economy, Smart Homes, Smart Information Communication and Technology (ICT), Smart Infrastructure, Smart Citizen and Smart Governance. The central motivation for the building of smart cities is to raise the quality of living of its citizens. In simplest terms, the smart city can be described as a city planning approach that banks significantly on Information and Communication Technology (ICT) to monitor and subsequently integrate and optimize the conditions and usage of citys lifelines like roads, bridges, tunnels, railway lines, seaports, airports, electricity, water, communication , etc. and an approach that effectively plans their management.

By keeping an eye on all the major systems, better decisions could be expected from the colossal streams of enormous data. For example, when home appliances like refrigerators, and washing machines are controlled by IoT, better energy management is obtained. Also, when the trees, plants, air, and the environment get monitored in a non-obstructive manner, optimal quality work environment could be expected. Cities keep on attracting new people, and by 2030, the UN assesses that more than 60 percent of the worldwide populace is assumed to live in huge cities [24]. With almost 38 million individuals, Tokyo stands at the pinnacle of most crowded cities of the world taken after by Delhi, Shanghai, Mexico City, Sao Paulo, and Mumbai. The results and difficulties for such huge increment in populace on the city assets and administrations are more than self-evident. The only feasible solution is to stand up to this issue by creating strategies to lessen the asset utilization of the city in a savvy and clever way. Figure 4.1 illustrates some of the most important smart city services, along with the challenges that require addressing.

4.1.1. Security requirements and challenges. The security requirements claimed by the smart city are shown in figure 4.2 while the major challenges include:

1. Extreme Heterogeneity: In the form of huge number of different sensors deployed in the city which are brought together in a single smart city eco-system [2]. Developing a generic security procedure here is challenging.
2. Scalability: Since there is a multitude of available devices, attack surface is also huge.

Therefore, it is exposed to all the threats & challenges posed by these features, which are described in detail in section 5.

4.2. Smart Health. Today a significant rise in the proportions of aging populace is witnessed. As such, IoT Health monitoring Systems (HMS) have been developed to provide a feasible contrasting option for dealing with healthcare instead of traditional approaches. The intent of HMS is to provide cheap remote healthcare to people who need it, thus maintaining their independence as well as avoiding hectic and skyrocketing costly interactions with healthcare institutions. Apart from HMS, other services [25] of smart health include:

- Activity of Daily Living (ADL): Grooming activities like brushing teeth, face washing, making hair, eating, dressing, sleeping, toileting, etc.

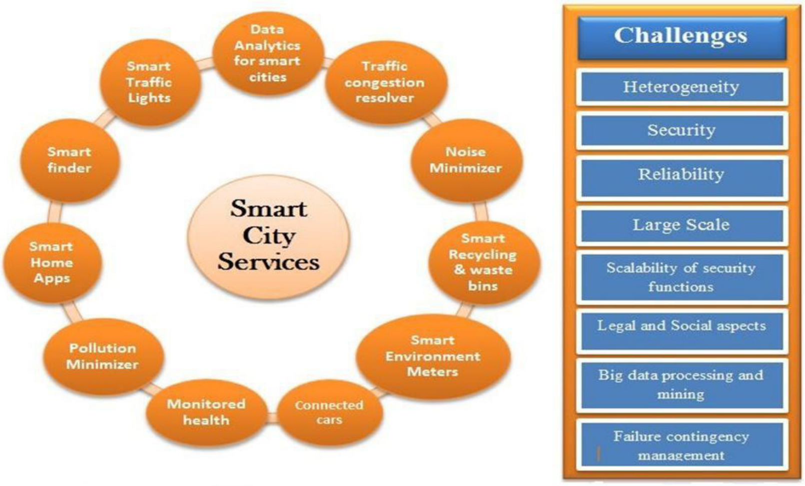


FIG. 4.1. *Smart City services and challenges.*

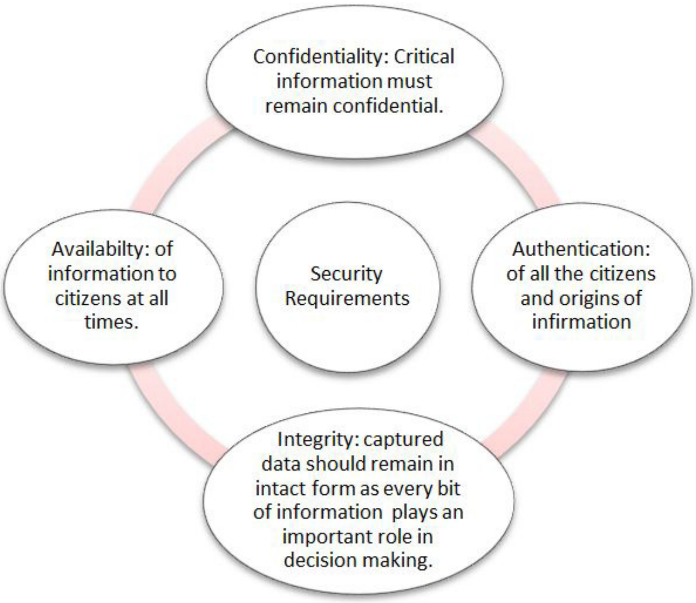

Confidentiality: Critical information must remain confidential.
Availabilty: of information to citizens at all times.
Security Requirements
Authentication: of all the citizens and origins of infirmation
Integrity: captured data should remain in intact form as every bit of information plays an important role in decision making.

FIG. 4.2. *Smart City security requirements*

- Instrumental Activity of Daily Living (IADL): preparation of meals, laundry, use of medicines, housekeeping, shopping and etc.
- Ambulatory Activity of Daily Living (AADL): Static activities like lying, standing and sitting, dynamic activities like walking, running, jogging, bike riding and etc., transitional activities like standing to sitting, sitting to standing, standing to walking, etc.
- Monitoring of mental functions (MF): Memory, judgment, understanding, sense of direction, etc.
- Physiological activities: monitoring of heart brain and muscle working.
- Social Activities of Daily Living (SADL): get together with family and friends, making phone calls, video calls, etc.

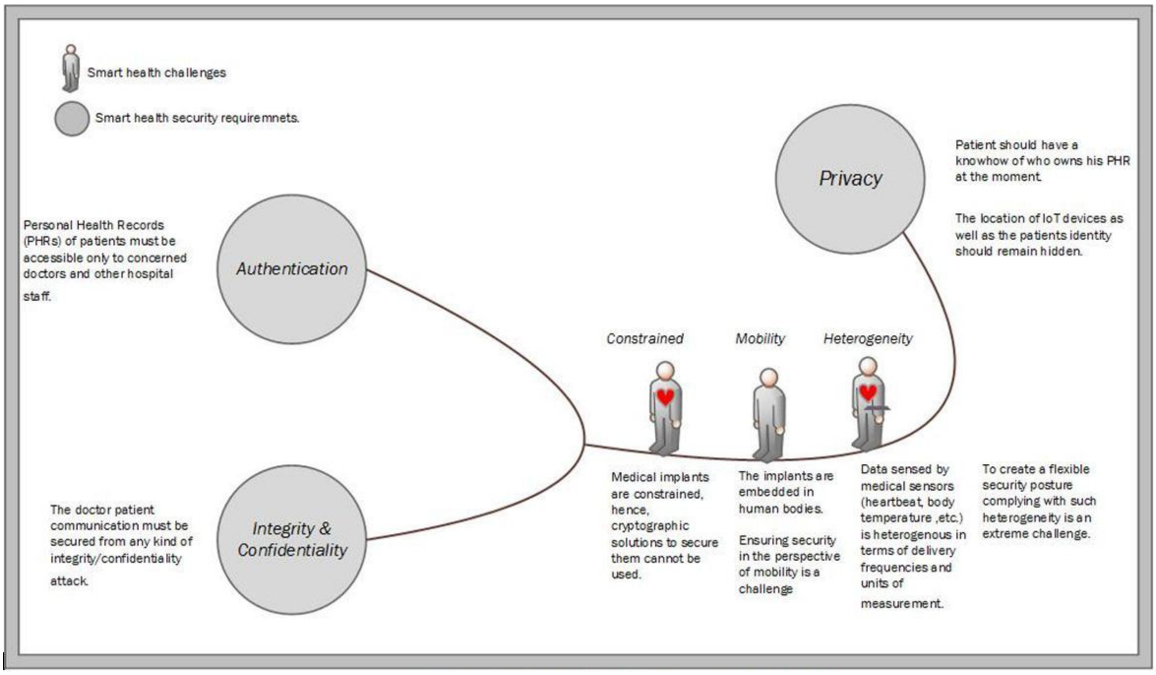

Smart health challenges
Smart health security requiremnets.
Personal Health Records (PHRs) of patients must be accessible only to concerned doctors and other hospital staff.
Authentication
Privacy
Patient should have a knowhow of who owns his PHR at the moment.
The location of IoT devices as well as the patients identity should remain hidden.
Constrained
Mobility
Heterogeneity
The doctor patient communication must be secured from any kind of integrity/confidentiality attack.
Integrity & Confidentiality
Medical implants are constrained, hence, cryptographic solutions to secure them cannot be used.
The implants are embedded in human bodies.
Ensuring security in the perspective of mobility is a challenge
Data sensed by medical sensors (heartbeat, body temperature ,etc.) is heterogenous in terms of delivery frequencies and units of measurement.
To create a flexible security posture complying with such heterogeneity is an extreme challenge.

Fig. 4.3. *Security requirements and challenges of smart health.*

As per the United Nations Population Fund (UNFPA) [26] there would be more than 2 billion people all around the world who will be aged more than 60 by the year 2050. Also, World Health Organization (WHO) says that by 2035, the world would be 12.9 million short of healthcare personnel [27]. Age itself becomes a significant criterion of risk for developing chronic diseases like dementia, alziemers, diabetes, cardiac problems, osteoarthritis, etc. [25]. Also, the aged people may face an elevated danger of falling and sustaining hip fractures [28]. However, there are not enough resources available to deal with this type of sensitive care [29, 30]. As such, it is very important to have smart healthcare development. Nonetheless, smart health environment provides benefits; it also suffers from various challenges.

4.2.1. Security requirements and challenges. Given the medical implants usually remain unattended for long durations, the S&P requirements and challenges [31] in the light of IoT intrinsic features are summarized below in figure 4.3. The holistic impact of these challenges would be visualized in the next section when the threats/challenges raised by each of the feature are studied in detail.

4.3. Smart Building. One of the major building blocks of a smart city, a Smart Building is the one in which all the service systems are controlled automatically and are integrated with each other, working co-operatively in order to optimize the utilization of resources and boost the savings of vested money and operating costs, flexibility and performance [32, 33].

With the advancements in the technology, smart buildings were induced with the ability to self-learn, change, and adjust their performance as per the requirements of the environment, organization or an individual [34]. The vision of connecting various things to the internet is brought into practice with the use of various applications that offer remote monitoring and control of these devices. But regardless of the presence of smart buildings and smart technologies for quite some time now, their prevalence is not widespread and hence, their potential is not fully tapped. This is because there are still a lot of hurdles that exist in the way to the exact realization of smart buildings.

4.3.1. Security requirements and challenges. The vital security requirements of smart buildings / smart homes (SH) are sketched out diagrammatically in figure 4.4 while the critical security challenges include:

1. Heterogeneity: Bringing different technologies together can give rise to new security threats [35].

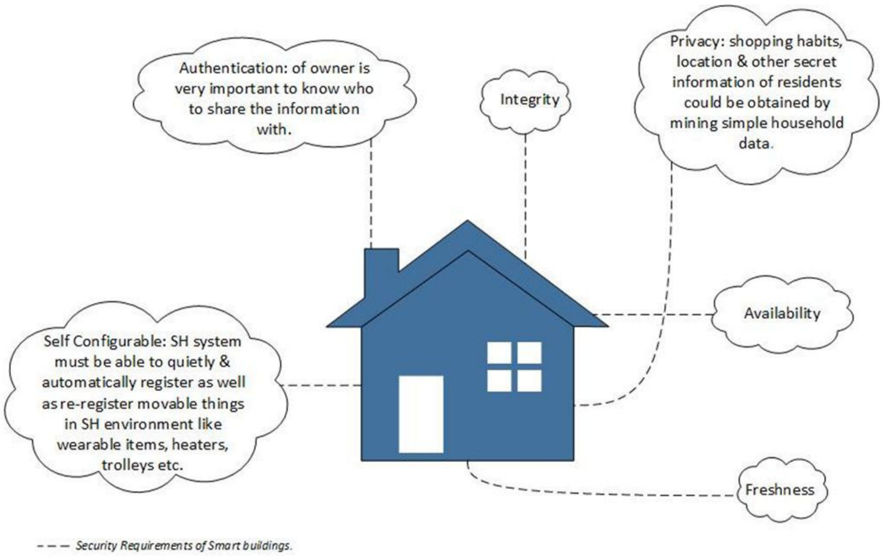

Authentication: of owner is very important to know who to share the information with.
Integrity
Privacy: shopping habits, location & other secret information of residents could be obtained by mining simple household data.
Availability
Self Configurable: SH system must be able to quietly & automatically register as well as re-register movable things in SH environment like wearable items, heaters, trolleys etc.
Freshness
--- Security Requirements of Smart buildings.

Fig. 4.4. *Vital security requirements of smart buildings*

2. Context Awareness: If a thing moves to a new location or its environment/context changes, the SH system must be able to both detect as well as react to it. Making of such an adaptable security solution is challenging.
3. Usability: The easy to use and easy to learn feature must be there in the SH system. Designing a simplistic security posture is challenging.
4. Internet Theft: Stealing private photos from clouds, video content from IP connected house cameras.

4.4. Smart Transport. The development of Intelligent Transport System (ITS) has paved the way to the creation of smart cars, smart bicycles, smart buses and trains [36] by equipping them with various types of sensors and actuators that include radars, cameras, Global Positioning System (GPS), Event Data Recorders (EDRs), omni-directional antennas, Electronic License Plates, Electronic Chassis Numbers, etc. [36].

With huge number of these autonomous and highly sophisticated vehicles hitting the roads, researchers are considering ways to smarten and tidy up the roads on which they travel. Smart cars on smart roads would offer advantages like notifying drivers about the empty parking slots via their mobile phones, inform cars about the road conditions, weather conditions, traffic awareness services, wildlife movement patterns, etc. The way to getting it going is an IoT system that incorporates sensors (wired/wireless) installed in the roadway and on existing traffic lights.

The vehicles are loaded with On-board Units (OBU) that communicate with other vehicles using Vehicle to Vehicle (V2V) communication and with Road Side Units (RSU) that are installed on the sides of the roads using Vehicle to Infrastructure (V2I) communication [36]. The applications in the transport industry incorporate the utilization of smart things to screen and report different parameters starting from pressure in tires to the distance from other vehicles. Radio Frequency Identification (RFID) has been utilized to aid in streamlining vehicle generation, amplify co-ordination among vehicles, upgrade quality control, and enhance client services [37].

The use of Dedicated Short Range Communication (DSRC) will conceivably help in avoiding interference with other devices as well as in accomplishing higher bit rates. V2V and V2I communications will essentially progress ITS applications, like vehicle safety applications and traffic management services, and will be completely integrated into the smart transport infrastructure [37]. Smart transport offers a lot of services to ensure efficiency and safety of travel but at the same time suffer from a lot of issues. Figure 4.5 explains the various aspects of smart transport.

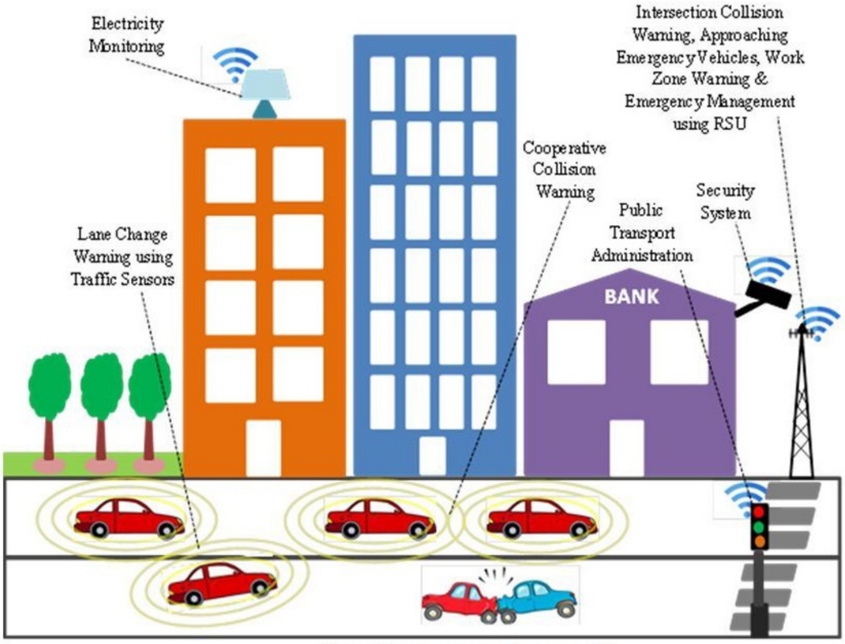

Electricity Monitoring
Intersection Collision Warning, Approaching Emergency Vehicles, Work Zone Warning & Emergency Management using RSU
Cooperative Collision Warning
Security System
Public Transport Administration
Lane Change Warning using Traffic Sensors
BANK

Fig. 4.5. *Smart transport services in a smart city*

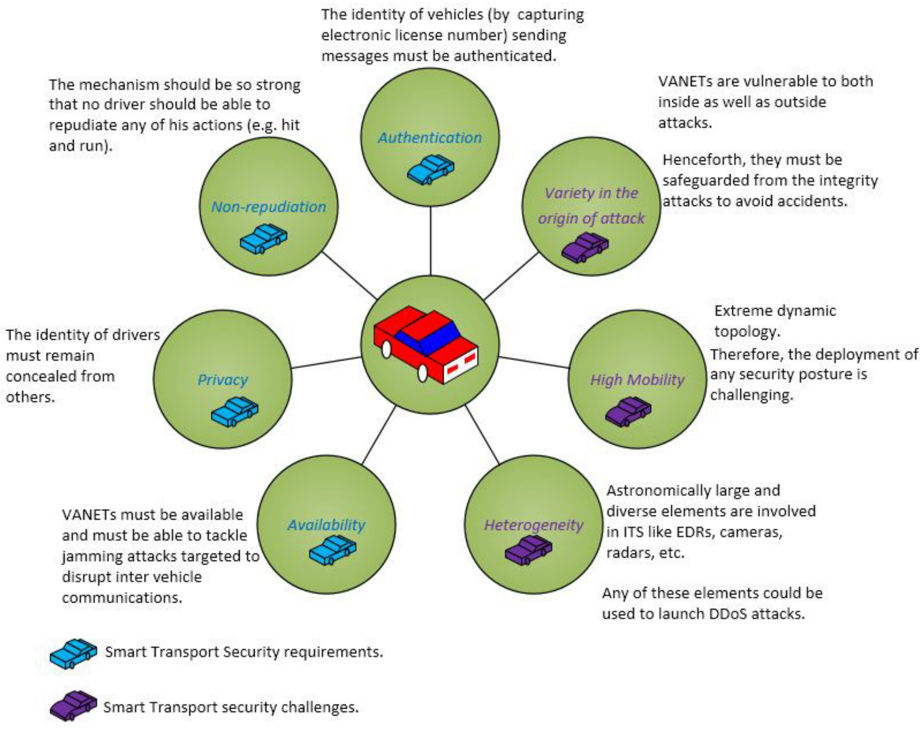
4.4.1. Security requirements and challenges. As already stated above, to achieve various smart transport services, V2V and V2I communications are used, but to secure these communications, several security requirements need to be studied comprehensively [38]. Figure 4.6 summarizes the various security requirements and challenges that are faced in the realm of ITS.

4.5. Smart Industry. The manufacturing industry will soon witness a revolution as their mode of production will shift from digital to intelligent [39]. This is attributed to the fast improvement of electric and electronic innovations, the manufacturing technology and information technology [40]. To become the best players in the smart industry development, a lot of industrialized nations are profoundly giving careful attention to the clever manufacturing technology [41]. For example, China Manufacturing Plan [42], Industry 4.0 Strategy [43], Europe 2020 Strategy [44], USA Reindustrialization and Manufacturing reflow Strategy [45]. Some of the most important services of smart industry include water monitoring, transport assessment, manufacturing, retail, electricity monitoring, gas and oil monitoring, worker safety services and location services.

Although an impressive growth is witnessed in enhancing the flexibility, quality, and efficiency of the manufacturing systems, a huge risk in this race to achieve the smartness is that of security which is viewed as being an optional concern instead of a basic part of the procedure of development and deployment.

4.5.1. Security requirements and challenges. The industry systems are one of the most targeted victims of attackers [46]. The security requirements and challenges particular to smart Industry are highlighted in figure 4.7 and explained below:

1. Confidentiality: Industry data should be known only to its owners and must be hidden from others. Espionage attacks are a commonplace in Industrial IoT (IIoT) as other companies want to know what their contemporaries are up to. Hence, data, code, and system configurations must be secured.
2. Integrity: To prevent accidents in the industrial units, it is very important that the integrity of exchanged data must be maintained.
3. Availability of the system: Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks could be easily launched, but the industry manufacturing systems must always remain in the operational state.
4. Authentication: It is necessary that every part that is involved in the manufacturing process is authen-



The identity of vehicles (by capturing electronic license number) sending messages must be authenticated.

The mechanism should be so strong that no driver should be able to repudiate any of his actions (e.g. hit and run).

VANETs are vulnerable to both inside as well as outside attacks.

Henceforth, they must be safeguarded from the integrity attacks to avoid accidents.

The identity of drivers must remain concealed from others.

Extreme dynamic topology.
Therefore, the deployment of any security posture is challenging.

VANETs must be available and must be able to tackle jamming attacks targeted to disrupt inter vehicle communications.

Astronomically large and diverse elements are involved in ITS like EDRs, cameras, radars, etc.

Any of these elements could be used to launch DDoS attacks.

Smart Transport Security requirements.

Smart Transport security challenges.

Fig. 4.6. *Smart transport security requirements and challenges*

ticated.

5. Lack of standardization: No standard protocol exists among the industry systems in general and SCADA systems in particular. In fact, there are almost 150-200 open standards.
6. Cyber-physical attacks: Trojans, viruses, worms, Dos, DDOS user-compromise, and root compromise attacks could be launched easily. Dos attacks compromise the sensors and stop them from sending any data. Such attacks could be launched by either disrupting the communication channel or the routing protocol
7. Scalability: As the number of industry units increase, the probability of attack also increases because the attack space increases.

Next section illustrates how the security requirements and challenges actually creep into the various implementations of IoT. The very features of the devices used in these applications make them insecure.

5. Practical illustrations of Security and Privacy breaches in view of IoT Features. In this section, the most important as well as famous attacks, threats and challenges are studied in the light of IoT features, i.e., the threats they cause, and the challenges that exist because of their impact. All these features are exhibited by the devices used in the implementations discussed in section 4. Some of the existing solutions from literature are discussed and their critical analysis is presented in this section.

5.1. Threats, Challenges and Solutions in Interdependence (Implicit Dependence).

1. **Threats caused by Implicit Dependence:** There are potentially three inherent security issues linked to the use of IFTTT [47]. a) No consideration to security-related context of IoT end devices b) causing ambiguity by assuming that different applications/services work independently and c) vulnerabilities that arise because of the incomplete specifications provided by the user because of their incompetence to understand the cross-device relationships and their effects. Henceforth, even if the attackers actual target has a strong defense mechanism, it can be compromised because of this feature.

   E.g., in case of smart buildings/homes, both the smoke detector and sight hound could be active at the

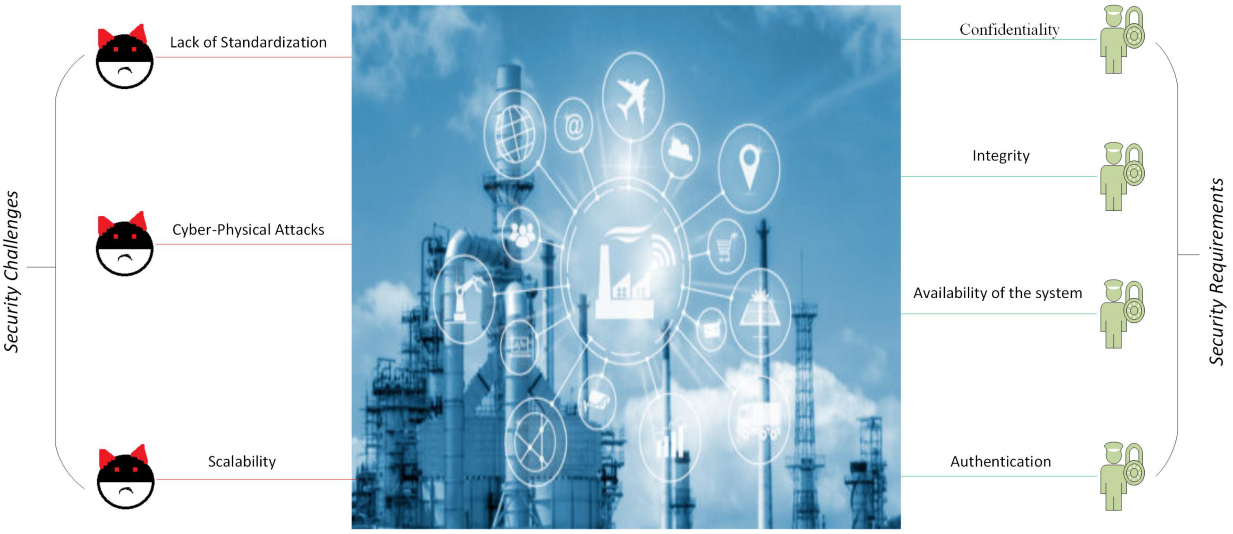


Fig. 4.7. *Smart industry security requirements and challenges*

same time creating ambiguity for people to decipher whether the lights turned red because of smoke or because of an intruder. Also, in case of the opening window scenario discussed in section 2(a) the hacker neither requires to handle the automatic window control nor the thermometer. S/he just needs to compromise the smart plug connected to the public network and make it switch off the AC. The temperature of the room will automatically increase, and consequently, the windows would open - a dangerous physical security breach [3]. Also, different interdependencies and contexts demand different levels of S&P.

In the case of smart transport, the dependence of vehicles on the information coming from RSUs could become dangerous. If an RSU is hacked for instance and there is a blind corner. A car is speeding in the wrong direction. Now, instead of asking the vehicle coming from the other side to slow down/stop, the hacked RSU tells it to go as it pleases as there are no cars on the other side. The result will be a fatal collision.

2. **Challenges:** The researchers usually try to protect single devices rather than creating a clear defensive boundary for them. This results in an adverse effect on the security aspect of IoT. It is, however, difficult to define a defensive boundary for them because of their interdependence, which makes it difficult to set a clear set of permission rules for these devices.
   ObjectivesTo study the anomalous behavior of cross-device interdependence in IoT.
   Device new security policies for differentiating normal behavior from anomalous.

3. **Solutions** The traditional security approaches like anti viruses, software patches would be inefficient in the IoT world because of the implicit dependencies shared by them. Table 5.1 depicts the various IoT solutions given in diverse fields to deal with issues caused by the interdependence feature of IoT. From the problems, it is concluded that more practical and effective solutions are the need of the hour.

5.2. Threats, Challenges and Solutions in Heterogeneity.

1. **Threats:** IoT security report, 2015 [50] indicates that >90% of IoT devices have hard-coded key vulnerabilities, 94% have web security vulnerabilities in their web interfaces implying that they can be easily attacked by the hackers. Moreover, the protocols used in IoT do not have tough security procedures implying the protocol vulnerabilities could be exploited easily [51], and since these protocols greatly vary in their semantics, when they work together erroneously, other security threats could arise like Bad Tunnel [52]. The Bad Tunnel attack is launched by persuading the victim to open a URI using a Microsoft edge web browser or internet explorer or to open an office document. Once the victim does

Table 5.1
Critical Analysis of Solutions to Interdependence Issue

References		
Tianlong et al. [47]	**Domain Studied**	Smart Home
	Interdependence	If there is a fire alarm, open the windows. The rogue player can try to compromise the fire alarm to break into the house.
	Advantages	Provides a fresh roadmap to look at the security disaster of IoT in a new light: thinking beyond the traditional approaches of security.
	Problems with the solution	A security posture is defined for every device separately for detecting whether the device is acting normally or not. The solution becomes absolutely impractical and complex when the number of devices increases, hence not suitable for IoT.
Yunhan et al. [48]	**Domain Studied**	Samsung Smart Things platform.
	Interdependence	A strong defense mechanism might be present in a smart phone, but when the apps are installed on these phones, people tend to give various permissions to these apps; the interdependence (over-privileged problem) is then exploited by the hackers to break in and cause damage.
	Objectives	To provide a permission system based on context to alleviate the over-privileged problem in appifiedIoT environment. Fine-grained control of application behavior is achieved. Provide the user with important information such as run-time data, procedure control, and data flow of each IoT device and then allow the user to either allow/reject the action.
	Advantages	Provides contextual integrity. Is backward compatible and hence can be easily taken up by the present IoT platforms. Flaws like thefts and break-ins in permission systems like smart phones have been identified. Misbehavior by the attackers will be detected very early.
	Problems with the solution	The Final decision is made by the user. So, if he makes a wrong decision and says allow where he should have said deny, the choice is remembered by the system, and the user is not prompted the next time such an attack occurs. Hence impractical in IoT.
Luca et al.[49]	**Domain Studied**	IoT Health.
	Interdependence	If a person falls, then the relatives, nurses, and other medical staff would be informed. A fall like situation can arise when a person drops himself on a sofa or lies on a bed (tries to deal with the ambiguity problem).
	Objectives	Create an alarm system to deal with sudden ailments and falls of elderly people. Aims to provide the perfect position of individuals (indoor & outdoor), monitor their vitals and activities.
	Advantages	An Omission of costly hospital charges for the care of the elderly by the use of wearable technologies.
	Problems with the solution	Consideration to S&P is completely left out. The problems caused by the interdependence could be immensely exploited. Via a huge attack space that is available in IoT, an attacker can easily attack the wearable device and create false alarms and false notifications to take medicine in huge quantities, thereby can lead to fatal outcomes. The wearable devices can pose privacy threats as well. A person could be tracked down to his exact location, which could lead to a privacy breach, and at the same time very dangerous.

so, the attacker can camouflage like a file server or a local printer, circumvent the explorers sandbox or take the download update of windows, network traffic, and certificate revocation lists under its control and could be launched on all the versions of internet explorer and Microsoft office. Table 5.2 describes various types of web security vulnerabilities and what percent of these traditional vulnerabilities still exist in IoT.

2. **Challenges:** Because of this heterogeneity among the IoT devices, a single defense posture wont suffice in the IoT environment. Researchers need to dig out the general security mechanisms somehow.
3. **Solutions:** The solutions should offer a way to manage the variety of devices/technologies/services /environments to tackle the possible vulnerabilities of diverse IoT devices. Table 5.3 highlights some

Table 5.2
Web Security Vulnerabilities

Web Security Vulnerability	**Description and Effects**	**Vulnerability %age in IoT**
Cross Site Scripting	Malevolent scripts are infused into generally favorable and confided websites.	55.5% [50]
File Manipulation	The contents of a file are modified in a way to cause the application to start erroneous processing thereby displaying horrible results like throwing the application in an unstable state, disclosing confidential information, overwriting the file, etc. [53].	12.5% [50]
File Disclosure	The Attacker tries to hack down the entire path of the file and disclose its contents. This can be done by eating the cookies or making the web application do something that is not intended [54].	4.6% [50]
File Inclusion	Application fabricates a way to executable code utilizing an aggressor controlled variable in a way that enables the attacker to control which record/file to execute at run time.	5.7%[50]
SQL Injection	SQL statements are infused with malicious lines of code. Executed through a web page input, SQL injection can destroy a complete database.	4.9%[50]
HTTP Response Splitting	Refers to the state when an application is not able to decontaminate the input values. Leads to various other vulnerabilities like cross-site scripting.	1.4%[50]
Command Injection	If the application is vulnerable, it can be exploited to run arbitrary commands as it allows the mischievous cookies, HTTP headers, etc. to pass into the system shell, thereby giving the attacker rights that it dreamt of having. If the attacker is able to insert a single delimiter like ; that marks the end of a command, it can insert its command and get it executed [55].	10.4%[50]
Code Injection	Is different from command injection in a way that the attacker needs to insert his/her code, which is then executed by the running application. Achievable by the poor data validation approach of applications. It can lead to the loss of integrity, accountability, confidentiality, and availability [56].	1.9%[50]
Possible Flow Control	Change the order in which statements execute. Usually done by altering the program counter.	1.6%[50]
Unserialize()	Unserialize is a function that takes a single serialized parameter and transforms it into a PHP value. If the suspicious input is passed to the unserialize, it can result in object instantiation and auto loading, allowing the attacker to exploit it as he wishes [57].	1.3%[50]

of the proposed solutions, their advantages, and loopholes.

The proposed solutions become practically unsuitable for large scale analysis and have some other flaws which make them incomplete. Also, most of the research is focused on using classical Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for protecting a diverse range of devices all at the same time. However, heterogeneity of the IoT devices doesnt let it work because the attacks may vary in their character depending on the device they target.

More suitable IDS and IPS systems for IoT devices which exhibit heterogeneity need to be studied further. It is concluded that full-fledged solutions to the problem posed by heterogeneity are currently absent, and more work needs to be done in this direction.

5.3. Threats, Challenges and Solutions in Constrained.

1. **Threats:** Since IoT devices are mostly constrained by resources, storage capacity, battery back-up, and time delay, they are unable to support the necessary defense of the system as well as the network. Memory Management Unit (MMU) is absent in the lightweight IoT devices, hence the functions such as memory isolation, Address Space Layout Randomization (ASLR) and other types of memory safety procedures cant be installed on these IoT devices [3]. Also, the existing encryption and authentication algorithms are heavy weight requiring huge computing resources. If the devices start utilizing their computational and other resources on performing these heavy weight operations, then they would be left with very little energy and resources to perform their intended operations.
   As a result, an easy attack space is offered to the mischief makers for compromising these IoT devices. In fact, many IoT devices communicate with the server without checking its certificate and without any encryption only to save their resources. A man-in-the-middle attack can be launched with ease apart from the interception of communication happening between the two parties.

Table 5.3
Critical Analysis of Solutions to Heterogeneity Issue

References		
Costin et al. [58]	**Type of Heterogeneity**	Firmware of 32000 distinct devices.
	Objectives	To perform a static analysis of 32000 firmware images.
	Advantages	Found 38 formerly unknown security vulnerabilities. Found that these vulnerabilities were affecting almost 1,40,000 devices on the internet.
	Problem with the Solution	Suffers from the problems of static analysis: production of false positives because of generic analysis and false negatives because of much specific analysis packed or obfuscated code, etc. A particular programming language domain is targeted like PHP, C, etc. In reality IoT equipment can contain a mixture of programs written in various languages.
Drew et al. [59]	**Type of Heterogeneity**	Different firmware of IoT devices.
	Objectives	To provide a dynamic, complete and sound analysis of firmware programs. To find potential bugs, and security threats.
	Advantages	Symbolic execution of firmware programs to investigate their security. Exposed 20 memory safety bugs and one peripheral misuse bug.
	Problem with the Solution	The Complete analysis can be unmanageable in many firmware programs. The techniques employed: state pruning and memory smudging are not enough. Imprecision factors exist among the sources: disparity in the execution of firmware (natively or symbolic execution), false positives and false negatives can arise when the proposed system executes states that are actually never reached in reality.
Zaddach et al. [60]	**Type of Heterogeneity**	Different firmware of IoT devices
	Objectives	To perform an elaborate dynamic study of firmware in embedded systems. To evaluate the performance on three real-world security scenarios: vulnerability discovery, hardcoded backdoor detection, and reverse engineering.
	Advantages	Performs dynamic analysis of firmware by giving direct memory access to the real device employing an emulator. Firmware relying on absolutely amorphous peripherals could be studied.
	Problem with the Solution	Unable to imitate all real device actions, it makes use of emulators. The need to have an emulator device for any device that is under test puts a heavy fiscal burden. Incurs serious hurdles for large scale analysis.
Daming et al. [61]	**Type of Heterogeneity**	Variety of device firmware.
	Objectives	To assess FIRMADYNE across a huge dataset of 23,035 firmware images for exposing security vulnerabilities. Aimed at the Linux operating system.
	Advantages	Enable large scale and dynamic firmware analysis. No emulator required. If the vulnerability is detected, results regarding the necessary actions to be taken are provided. Automatic vulnerability verification is performed.
	Problem with the Solution	Works only on the LINUX based systems.
Virginia et al. [62]	**Type of Heterogeneity**	Different Access Control (AC) mechanisms.
	Objectives	To replace the Access Control List (ACL) based AC mechanisms by role-based AC mechanism for the reason that former AC procedures are hard to administer when the count of devices and resources increase.
	Advantages	Adds a median layer that functions in assigning privileges to roles and roles to subjects. In this way, the rights do not descend directly to the subjects but come through roles. The effort to manage AC lists is drastically reduced.
	Problem with the Solution	It requires a hurricane effort when the numbers of roles or resources grow. Impractical when a lot of domains are covered by AC systems.
OASIS [63]	**Type of Heterogeneity**	Different access control mechanisms
	Objectives	Specifies policies of Attribute based Access Control (ABAC). To support varied data types, name types, path expressions, and objectives for attributes (String, integer, internet-based name, etc.) Provides a system of modularization to accord with complicated policies.
	Advantages	Uses attributes of the subject like its location, age, position as well as its environment and resource properties to define access policies thereby eventually cutting on the cost of complex rules, the number of rules and rule changes. Slashes the processing and data availability needs.

	Problem with the Solution	Complex to manage. Increased probability of having defect because of heavy expressiveness of ABAC. Needs a persistent description of subject attributes both within a particular domain as well as across multiple domains. It is not always possible to have a well-defined environment, resource, and attribute description of subjects in the IoT domain.
Sergio et al.[64]	**Type of Heterogeneity**	Different access control mechanisms.
	Objectives	To develop an AC system that supports scaling and changing environment needs of the IoT.
	Advantages	An easy to use, scalable, feasible, and legible AC mechanism is developed.
	Problem with the Solution	There is delegation support in which a subject can award another subject with access rights, and provide it the right to grant further subjects. If one subject gets compromised or is corrupt, malicious subjects get the access rights and the entire systems come under a heavy security threat. X.509 certificates are used. Their management and encryption needs complicate the process and make it complex. The RSA encryption scheme is utilized hence impractical for IoT devices that are constrained of both space and processing capabilities.
Ki-Wook et al. [65]	**Type of Heterogeneity**	Different authentication and key management procedures.
	Objectives	Aims to provide a new Authentication and Key Management (AKM) mechanism for constrained IoT devices based on IEEE 802.11 key management and IEEE 802.1X authentication procedures.
	Advantages	No need for pre-configured security information between the IoT service domain and access network domain. Reduces the burden of constrained IoT devices for performing AKM by offloading the process to a strong agent. Computation and network cost reduced. Less memory usage.
	Problem with the Solution	Mutual authentication is performed only once. Only session keys are exchanged later between the stations and Access points (AP). This can be dangerous in the situation when an authentication users device gets hacked or becomes corrupt.

2. **Challenges:** Designing of lightweight security solutions for constrained devices is a challenge.
3. **Solutions and opportunities:**
   - The author in [66] proposed a lightweight software fault isolation procedure on tiny embedded processors. The disadvantage of [66] however is that the performance overhead for the devices needing multiple address checking searches is huge and hence is not applicable for IoT devices expecting performance in real time.
   - The author in [67] presents a complete, trusted computing functionality on low-cost embedded systems. However, its implementation requires the changes to be made in the existing hardware of the Microcontroller unit, so it cant be used directly on existing devices. Hence, novel lightweight algorithms need to be designed.
   - New lightweight encryption algorithms are presented in [68-70], and modification in the existing cryptographic algorithm is presented in [71]. Yet, achieving the security of the same level by the lightweight algorithms is different and prone to new security issues.
   - The Cloud computing comes to rescue [72] for dealing with the above problems as it allows centralized, shared, and scalable computing resources to be used on demand by any individual or organization. The amalgam of IoT and cloud can give strong processing power, huge storage capacity, and resource allocation in a scalable manner and on the fly deployment of applications with insignificant cost [73]. But, regardless of the advantages offered by this mix of IoT and cloud, it cannot be said that the cloud is the panacea of all the IoT issues. Firstly, the resources are centralized, implying the presence of a huge distance between the IoT devices and the cloud resulting in latency and jitter [74].

     Also, the physical distance gives rise to the inability of the cloud to access the local context based information like, the state of a local network, mobility pattern of the user, location information of a user, etc. Besides, because of this communication delay, real-time time-constrained applications cannot be accessed by the end users. Hence, there must be a new technological posture to extend the IoT to support time-constrained, location-aware, and mobility supported applications.

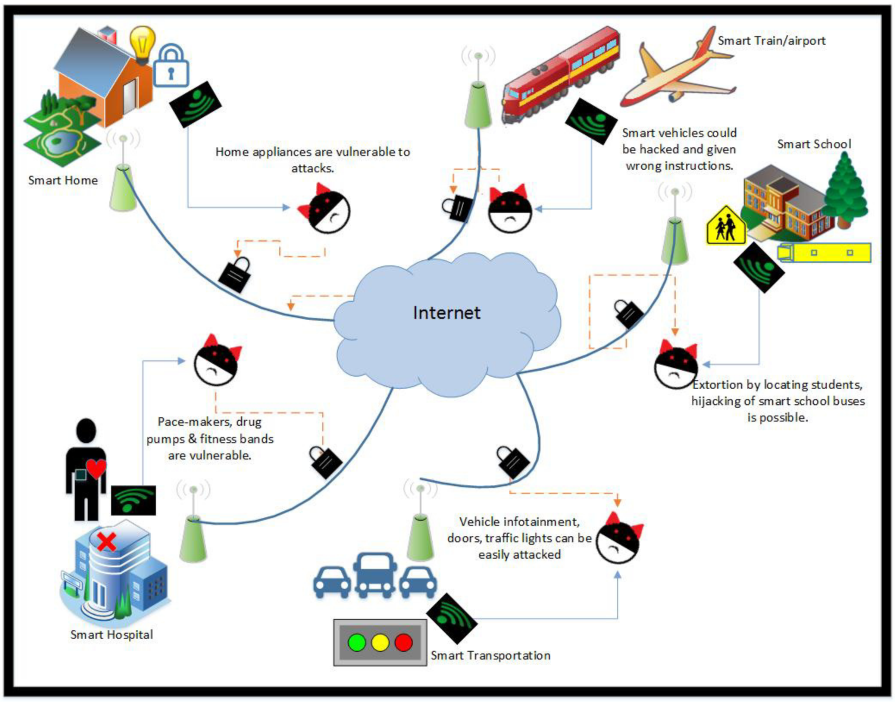

Smart Home
Home appliances are vulnerable to attacks.
Smart Train/airport
Smart vehicles could be hacked and given wrong instructions.
Smart School
Internet
Extortion by locating students, hijacking of smart school buses is possible.
Pace-makers, drug pumps & fitness bands are vulnerable.
Vehicle infotainment, doors, traffic lights can be easily attacked
Smart Hospital
Smart Transportation

Fig. 5.1. *Examples of IoT botnets*

- The fog computing paradigm offers a way to cover up the gap among IoT devices and remote data centers by offering a distributed computing environment pushing the cloud to the edge devices of the network and thus provide benefits like efficient networking, easy data access, better computation, reduced delay, storage, supporting heterogeneity, scalability, geo-distribution, locality, etc. [75]. However, fog computing suffers from the disadvantage of limited processing and storage capabilities.

5.4. Threats, Challenges and Solutions in Pervasiveness.

1. **Threats:** The MIRAI botnet of the year 2017 involved more than a million IoT devices where the attack traffic surpassed 1 Tbps. The botnet compromises the less secure IoT devices to achieve its goal of DDOS attack rather than computers. It was found by [2] that to launch huge scale DDOS attacks, IoT devices were employed. DDoS-for-hire services have lowered the barriers of entry for criminals to carry out these attacks, in terms of both technical ability and cost [76].
   As IoT penetrates into all the walks of life, i.e., industrial, agricultural, medical, etc. the IoT botnet target would no longer remain the website only, but will shift toward important national infrastructures, thereby causing grave dangers as shown in figure 5.1. Table 5.4 lists some of the botnet attacks that were launched in the recent past utilizing the multitude of available IoT devices. Also, the insecure configuration of these devices is a considerable threat to deal with.
2. **Challenges:** Since proper defense mechanisms are absent among the IoT devices, even the installation of an anti-virus is a hard task for them. Therefore, it is tough to detect and prevent IoT botnet in the early stages and thus a challenge.
   With the prediction of 50 billion devices by 2010, in addition to the scalability issues, the achievement of improvisation and optimization of IoT services on the internet would both remain a necessity as well as a hurricane challenge in front of the IoT professionals [91]. Moreover, in addition to the specific focus that cloud and fog computing paradigms would demand to increase the network efficiency and capacity, resource management will continue to remain a challenge.
3. **Solutions and opportunities:** The author in [92] distinguishes the legitimate user from the attacker

Table 5.4
Recent botnet attacks compromising IoT pervasiveness

Botnet Attacks		
Mirai botnet	**Launch date**	First seen on September 19, 2016, while the massive attack was launched against Dyn on Oct 12, 2016.[77]
	Description	Took advantage of over 600,000 less secure devices like web cameras, routers, baby monitors, etc. to launch a massive Distributed Denial of Service (DDOS) attack with attack traffic of 1 Tbps- largest on public record till Oct 2016. [77, 78]. Scanned huge blocks of the internet to find open telnet ports to hack into the devices using brute force methods of trying default username/password combinations which are seldom changed.
	Attack purpose	Launched by a Rutgers undergraduate student named Paras Jha, Mirai was one amongst the series of botnet attacks launched by him and his friends to make a profit out of DDOS attacks [78].
	Affected companies/ countries	Largest European hosting Provider Company named OVH. Dyn: A company providing Domain Name Services (DNS). Mirai launched on it brought down websites like Pinterest, Twitter, Reddit, Spotify, Github, affected Paypal, New York Times, BBC, etc. Krebs on security: independent journalists website who specializes in cybercrime.
	Monetary loss and other effects	$110 million in potential revenue was lost [79]. 8% of Dyn customer base chose to change their DNS provider after the incident [80]. HTTP flood and various other network-level attacks could be launched by Mirai botnet. Once the device gets infected by Mirai, it tends to remove any other malware on that device to claim the gadgets authority.
Reaper botnet or IoTroop	**Launch date**	On October 19, 2017, an Israeli security firm named Checkpoint announced about this new IoT botnet [81].
	Description	Built on top of the Mirai code with one significant difference, i.e., while Mirai used simple brute force method, reaper made a step ahead in the complexity of these attacks [82]. Utilizes actual software hacking techniques to find security flaws in the code of vulnerable devices to compromise them, i.e., while Mirai was looking for open doors to break in, reaper breaks open the locks on those doors [82]. It covers nine different known security vulnerabilities [83], e.g., by exploiting the CVE-2017-8225 vulnerability; the reaper gets access to devices .ini files where the important credentials are stored. This vulnerability is found in insecure cameras. Also, it spreads the infection to other devices like a worm. When the vulnerability is targeted, the device can be taken under the botnets control without raising any alarm.
	Attack purpose	AS per Arbor, the reaper is intended for use as a stressor service essentially catering the intra-China DDOS-for-hire market [84].
	Affected companies/ countries	Targets vendors like LinkSys, Ubiquity, Synology, Netgear, GoAhead, Avtech, D-Link, Mikrotik, and Vacron, among others [83]. So far, IoTroop/reaper has infected over 2 million devices across more than 1 million organizations.
	Monetary loss and other effects	Built on Lua engine and mixed with further Lua scripts (the embedded programming language that allows running of scripts), reaper code can be easily modified and updated to launch more attacks with more options [83]. When combined with some basic machine learning and AI techniques, future version of this malware would have the capacity to recognize basically any device it is confronted with, look for a related vulnerability in it and after that select a proper exploit for it and even have the capacity to build up a custom exploit [83]. With the emergence and entry of technologies like Swarm Intelligence into botnet configuration, Hivenets in which numerous compromised devices team up to work like one intelligent unit will be made [83].
Hajime botnet	**Launch date**	Identified by Rapidity networks in October 2016[85]. The infections have primarily traveled from Vietnam (greater than 20%), Taiwan (approximately 13%) and Brazil (almost 9%). So far, no high profile attacks have been launched by Hajime botnet [86].
	Description	Hajime is an IoT malware whose most important feature is that it blocks other botnets and has amassed an army of 300,000 compromised devices. [85]. It is hard to impede the Hajime operation because of its peer to peer and hidden botnet operation rather than a centralized one. Hajime has no attack code but only a propagation module. Currently in the benign state. Like Mirai, it brute forces its way into open telnet ports on various devices to compromise them.
	Attack purpose	While the botnet is ballooning up in size, its real purpose remains unknown [85].

		Table 5.4 (contd.)
	Affected companies/ countries	MikroTik [87].
	Monetary loss and other effects	The compromised devices could be used to launch different types of attacks on various websites ranging from DDOS to executing SQL injection exploits. The worm is currently in a no harm state but can block access to 23,7547,5555 and 5358 ports that serve as common entry ports for botnets like Mirai. In April 2018, Hajime was found to extensively scan 8291 ports in the bid to find devices running vulnerable MikroTik router OS and was even trying the Chimay Red HTTP exploit [86]. If it gets through this operation, it will install a new copy of itself on the victim node.
Ransomware Attacks RDOS (Ransom DDOS,e.g., WannaCry	**Launch date**	May 2017.
	Description	In any RDOS attack, the attackers communicate something specific to the owners threatening about the DDOS assaults on their organizational operations or contamination of the operational frameworks with Ransomware except if a particular ransom is paid by a specific due date. The ransom usually ranges from 5-200 bitcoins [88]. The threat messages are often escorted by brief attacks to let the victim organization have a glance at the attackers power [88]. Almost 86 countries faced ransomware attacks from April-June 2017[89]. One RDOS attack in China lasted for more than 11 days, and almost 47.42% of RDOS attacks were targeted towards China [88].
	Attack purpose	Motivated by financial gains, attackers here use the trick of extortion for making money.
	Affected companies/ countries	Countries: China(47.42%), South Korea, USA, Hong Kong, UK, Russia, Italy, Netherland, Canada, France [88]. Companies: Al Jazeera, Le Monde, Figaro, Bitfinex (Largest Bitcoin exchange).
	Monetary loss and other effects	Global financial losses from WannaCry reached $4 billion. Companies lose their customer base.
Persirai	**Launch date**	Discovered by Trend Micro in early April 2017 [89].
	Description	A security threat exploiting the vulnerabilities in computers through TCP port 81 and which has compromised almost 120,000 IP based cameras so far. IP cameras become the easiest targets for attacks because they use the universal plug and play protocol (UPnP), which allows them to open up a port and work like a server [89]. Once compromised, the attacker directs the camera to download malicious shell scripts from various sites. After that, Persirai attacks itself, deletes the installation files to hide its presence and runs only in the memory. The compromised camera on receiving the commands from the server automatically attacks other cameras utilizing zero-day vulnerability [89].
	Attack purpose	After gaining control of the cameras, the criminal can launch a DDOS attack on other computers using the User Datagram Protocol (UDP) floods. The attacker will provide the ports IP address where it wants to launch the DDOS attack and therefore can target any IP in the world.
	Affected companies/ countries	Out of 120,000 IP cameras that are compromised, 30% are from China, 3% from Italy, 3% from UK, 8% from USA [90]. 64.85% of cameras in Japan have been identified to be infected with a backdoor.
	Monetary loss and other effects	The Worst feature of Persirai is that the computers from which the command and control for running the malicious bots is executed use the country code of Iran ,i.e., IR. However, this doesnt indicate that the attacker is Iranian [90]. Organizations dont know that their cameras are utilized to launch the DDOS attacks.

based on the type of request that they send. According to [92] a legitimate user may send a request at low frequency and a proper content while as an attacker may send requests at high frequencies and with the same repeating content in all the packets. Yet, the assumption is really basic as the attacker may not always send the requests containing the same old content but may most probably simulate users requests with proper and different contents.

Besides, the IDS that are employed in IoT are actually meant for the traditional networks and hence dont work well in the constrained IoT environment. There is a dire need to develop IoT specific IDSs that are designed keeping in view the heterogeneity and the constrained nature of the IoT environment.

5.5. Threats, Challenges and Solutions in Unattended.

1. **Threats and challenges:** It is considerably impossible to monitor the state of these devices via an external interface given the condition in which they are deployed. Also, the functions that these

Table 5.5
Challenges posed because of the mobility of IoT devices

Challenge	Description	Cause	Effect
Increased mobility Signalling Cost [6]	Signalling cost refers to the cost incurred in managing the Tsunami of signalling traffic generated by the billions of mobile devices which operate today [96].	The devices may be sending the signalling data on a periodic basis. When that data is multiplied by the no. of mobile devices, the Signalling traffic reaches staggering heights [96].	Inefficient usage of resources. Extra stress is put on the network. Diminished Quality of Service (QoS) [96].
Packet Loss [6]	Refers to the loss of the packet before it reaches the destination. It can be calculated by using the formula: Packet loss= No. of packets lost/ total number of packets [97].	Network congestion. Weak radio signals. Corrupted Hardware. Cyber-attacks, e.g., Black hole attack and other DDOS attacks [97].	Decreased QoS Less Throughput Increased Delay because of the time spent in the retransmission of packets [97].
Handover Latency [6]	When a node changes its point of attachment from one network to another, it is called handover. The time spent in doing so is called the handover latency. The handover latency can be calculated by using the formula: Handover Latency = The last packet received from the previous point of attachment/first packet received from the current point of attachment[98].	Channel Detection. Authentication. Process movement. Duplicate Address Detection (DAD). Registration Association. Channel Scanning [98].	While the handover is being performed, additional delay in performing the mechanism can occur. Active connection to the network is disrupted because of these handoffs [98].
Greater End-End Delay [6]	The time spent from the point the packet was put on the channel by the source to the time it reaches the destination is called the end-to-end delay. A Very crucial issue for the applications requiring fast response [99,100].	Congestion in the network. Cyber-attacks.	Less QOS. Fatal consequences in case of hard real time systems.
Inefficient Energy Consumption [6]	Lessening the consumption of energy in constrained IoT devices is one of the critical challenges faced by the IoT community. [101]	Devices already have less energy. If their energy is spent on sending signalling messages periodically and in retransmitting the packets, the constrained devices would be left with very little energy to perform their intended jobs efficiently.	Device shuts down and doesnt perform the function it is expected to do.

unattended devices perform are crucial and tempting the potential attackers to attack them. An attacker can re-program a camera, for instance, to send the recorded data to it as well in addition to the actual server.

2. **Solutions and opportunities:**
   - The author in [93] designed a system called Trust Shadow to make sure that a trusted environment is made available for the devices to execute their security-critical applications. However, it is based on ARM TrustZone technology using ARM-Cortex-A processors and hence doesnt support small IoT devices that employ lightweight processors.
   - Also, author in [94] proposes a mechanism for remote attestation of devices, however, it involves far greater delay affecting the normal execution of devices.

5.6. Threats, Challenges and Solutions in Affinity.

1. **Threats:** This feature poses a lot of security threats e.g. [95] indicates how an attacker can infer with confidence if the smart home is currently occupied just by mining the CO2 and smoke sensor data.

Table 5.6
Various Mobility Management Protocols

Mobile IPv4 [103]	**Description**	Allows the node to adjust its point of attachment as per its need without having to alter its IP address. Foreign agents are required, i.e., an external agent that performs the mobility function on a nodes behalf in a foreign network.		
	Packet Reordering	No	**Mobility Scope & Management Class**	Global & Host-Based.
	Mobility Issue addressed	None [6]		
	Other problems with the protocol	Suffers from the fragility problem, i.e., it gets broken when the node has a single home agent (an entity that performs mobility and forwarding functions on behalf of a node in the network to which the node attaches itself in the) beginning and doesnt solve any mobility issue.		
Mobile IPv6 [104-106]	**Description**	An Enhanced version of mobile IPv4 with an extra-large address space. Doesnt require any foreign agent. Employs the use of binding cache mechanism to link a mobile nodes home address, i.e., the permanent address of a node present within the home network with its relative care-of address, i.e., the nodes new address in a foreign network.		
	Packet Reordering	Yes	**Mobility Scope & Management Class**	Global & Host Based.
	Mobility Issue addressed	Briefly addresses the issues of packet loss, handover latency and end-end delay. [6]		
	Other problems with the protocol	Doesnt solve the issues of high signaling cost and energy consumption. Hidden Terminal problems. No way to find the reasons for packet loss. Includes links that could be utilized only partly.		
Hierarchical Mobility IPv6 (HMIPv6) [107]	**Description**	Pressure on the speed of handover is witnessed in mobile IPv6 because of the signalling processes that exist among the mobile node, it's home agent and it's correspondent node (a node from outside the home network that tries to communicate with a mobile node) HMIPv6 comes as an extension to Mobile IPv6 to improve its performance and reduce the amount of signalling required, by employing a new node called Mobility Anchor Point (MAP) that deals with the delays resulting from signaling.		
	Packet Reordering	No	**Mobility Scope & Management Class**	Global & Host Based.
	Mobility Issue addressed	Briefly addresses the issues of packet loss, handover latency and end-end delay [6].		
	Other problems with the protocol	Cannot address issues like high signaling cost and huge energy consumption.		
Network Mobility (NEMO) [108]	**Description**	Employs the compressed mobility header to deal with the problem of signalling cost. A new node called the mobile router manages mobility services like sending binding updates to home agents etc. instead of the node itself.		
	Packet Reordering	No	**Mobility Scope & Management Class**	Local & Host Based.
	Mobility Issue addressed	Signaling cost packet loss, handover latency, and end-end delay addressed to a lesser extent [6].		
	Other problems	Doesnt address the issue of energy efficiency		
Proxy Mobile IPv6 (PMIPv6) [109,110]	**Description**	It has two important elements that perform all the mobility functions: Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG).		
	Packet Reordering	No	**Mobility Scope & Management Class**	Local & Network Based.
	Mobility Issue addressed	Addresses the issues of signaling cost packet loss, handover latency ,and end-end delay to a lesser extent [6].		
	Other problems	Doesnt address the issue of energy efficiency.		
Sensor Proxy Mobile IPv6 (SPMIPv6) [111]	**Description**	Overcomes the problems of PMIPv6 like it solves the bottleneck ,and non-optimized path problems.		
	Packet Reordering	No	**Mobility Scope & Management Class**	Local & Network Based.
	Mobility Issue addressed	Addresses all the issues briefly [6].		
	Other problems	Issues not addressed efficiently.		
ClusteredSPMIP v6 (CSPMIPv6) [112]	**Description**	The problems in PMIPv6 arise because they use single LMAs (their load is not distributed). CSPMIPv6 uses clusters of MAGs and each cluster has its unique cluster head which perform all handover and signalling operations implying the load on LMAs getting balanced.		
	Packet Reordering	Yes	**Mobility Scope & Management Class**	Local & Network Based.
	Mobility Issue addressed	Addresses all the issues briefly [6].		
	Other problems	Issues not addressed efficiently.		
Overlapping Mobile Access Gateway (OMAG) [113]	**Description**	An extended version of PMIPv6. Covers inter-domain level. Utilizes pseudo-code to reduce latency caused by handovers.		
	Packet Reordering	Yes	**Mobility Scope & Management Class**	Global/Local & Network Based.

	Mobility Issue addressed	Addresses the issues of packet loss, handover latency and end-end delay to a lesser extent [6].		
	Other problems	Cannot address issues like high signaling cost and huge energy consumption.		
Constrained Application Protocol (CoAP) [114,115]	**Description**	Designed for low power and lossy networks. Excels in reducing handover latencies, signalling costs and packet loss.		
	Packet Reordering	Not required	**Mobility Scope & Management Class**	Doesnt apply.
	Mobility Issue addressed	Addresses all the issues to a moderate extent. Is better than other protocols [6].		
	Other problems	Best mobility management protocol till date.		

2. **Challenges:** To enjoy the services offered by various service providers one needs to share his/her personal information with the company, e.g., to give you the discounts, a vehicle insurance company wants to collect your driving data. Driven by profit, these companies usually store critical personal information with other companies and thus cause the information leak.
   The researchers need to focus on developing a proper privacy preserving mechanism. To avoid these problems researches in the direction of privacy at four stages is needed: privacy at the device, privacy at communication, privacy at storage, and privacy at processing.
3. **Solutions and opportunities:** Data masking and encryption solutions have been proposed to secure sensitive data from leaking, but they suffer from the problem of increasing time delays and reducing the easy availability of original data. Hence, proper and generic privacy protection mechanisms need to be made that may include proper steps to be taken in the phases of data collection, data transit, data usage, data storage and finally data sharing.

5.7. Threats, Challenges and Solutions in Mobility.

1. **Threats caused by Mobility:** Mobile devices utilize volatile, and vulnerable wireless connections to append themselves to the internet. The lossy nature of these links gives rise to many problems like increased rate of error and decreased bandwidth [6] and since mobile devices have the tendency to join more and more networks, it tempts the attackers to push malicious software into them to accelerate the infection of the malicious code quickly.
2. **Challenges:** This mobility nature raises the need to develop mobility resilient security algorithms for IoT devices. The main challenge posed by the mobility feature is the cross-domain trust and identification. For example, when a mobile IoT device enters a new network, how the network should verify its credentials, and what permissions should it be provided with/limited to.
   Also, when this mobile device tends to share the data in the new network,several things need to be done, e.g., key negotiation, data confidentiality, data integrity, protection etc. Table 5.5 illustrates some of the most important challenges related to the mobility feature of the IoT devices.
3. **Solutions and opportunities:** [102] tries to deal with the problem by making changes in mobile devices configuration as it joins a new network to comply with its new networks needs. However, this doesnt address the root cause of the problem. Moreover, a lot of mobility management protocols have been designed to deal with the issues in mobility.
   Table 5.6 gives a view of their description as well as the issues they address. It is found that there is still scope of research in this direction and that mobility issues in IoT need to be taken more seriously.

5.8. Proposed solutions for the identified threats and challenges. Through the rigorous examination of the solutions given to various security threats and challenges of IoT in the previous sections, we comprehend that security professionals are trying to ease these threats. However, these studies need applicability and are still in the stage of infancy. As such, numerous issues still starve for efficient and IoT acceptable solutions.

In this section we propose some of the solutions (table 5.7) that could be taken up as research opportunities by the scholars, academicians or people of the industry to tackle the security threats and challenges arising from the intrinsic features of IoT devices.

6. A simple security mechanism for Smart Transport. In this section, we have explored the threats to availability of VANETs that form the basis of ITS. Though the threat on availability exists in all the discussed

Table 5.7
Proposed Solutions for the Identified Threats and Challenges

Solution	**Description**	**Challenge addressed**
Context-based permission systems	Such a system will help to refrain the environment and other devices from changing the devices behavior by recording and comparing parameters like procedure control flow, data source and devices behavior periodically.	Interdependence: Such a system will solve the threats discussed in section 5.1 as even if the attacker is successful at executing the misbehavior around the similar physical conditions like that of the normal, it is extremely hard to duplicate the exact context information.
Know your IoT network	The users need to keep a track of the devices and the permissions they give out. All the points in the network of an individual need to be well secured. Not only the data, but the installed IoT devices could be hacked.	Interdependence, Pervasiveness, Unattended, Affinity.
Use of anomaly based Intrusion Detection Systems	Such systems would note and report any anomalous behavior shown by the network in real-time and would work in a generic manner. Devices could be hacked to launch massive attacks.	Heterogeneity, Mobility.
Combination of IDS and honeypots	A real-time monitoring of the network can be performed. Such a system shall offer added security to the IoT without requiring putting extra pressure on resource-constrained devices.	Heterogeneity, Constrained.
Employ multi-layer protection i.e., edge layer, fog layer, and cloud layer arch.	Make the execution of attackers actions extremely difficult by having multi-layer protection for resource -constrained IoT devices as they cannot protect themselves.	Constrained, and Unattended. By having multi-layer protection, it wont be necessary to be physically present near the device.
Design lightweight cryptographic & authentication procedures	IoT devices cannot run heavy-weight cryptographic procedures.	Constrained
Run in-depth forensic analysis periodically	Regular forensic analysis over the organization by security professionals will save the network from breaches like Mirai, Reaper etc.	Pervasiveness, Mobility.
Flag any suspicious traffic	We keep a check on what comes inside but forget about doing the same with the outbound connections. When a ransomware enters the device, it needs to connect back to its Command and Control (C&C) to carry out the attack. If we are able to prevent this connection, ransomware will not be able to get off the ground at the first place. Therefore, any suspicious traffic must be stamped and investigated.	Pervasiveness, Unattended.
Up-to date device firmware	Attack success can be made difficult by plugging out any vulnerabilities and misconfigurations which might be used to penetrate the network by periodically updating the device firmware.	Heterogeneity, Pervasiveness, Interdependence.
Development of new lightweight encryption techniques	The data sent out by the IoT devices need to be secured but the existing encryption cannot be used as they are heavy weight and costly for application in these devices.	Constrained.
Use of Edge computing	Instead of sending the data out, the end devices can themselves perform computations; hence no encryption scheme will be required.	Constrained.

use cases of IoT, we have chosen to discuss the availability attack on VANETs as they are particularly vulnerable to such attacks given their typical characteristics of high mobility, dynamic topology, and lack of any centralized monitoring entity. The type of availability attack that we have studied here is the black-hole attack in which the offender ruses the sender node into forwarding all its data through it by offering the best and the shortest available route to the destination even if it doesnt even know it. Once it receives the senders traffic, it attacks by dropping the entire data. The thing that makes the black-hole attack more dangerous in smart transport environments is that even the internal and most authentic nodes can launch it, rendering the cryptographic

Table 6.1
Simulation Parameters

Parameters	**Values**
Simulation tool	NS2(2.35) + SUMO
No. of vehicles	51
No.of RSUs	5
Malicious behavior studied	Black-hole attack
No of attack scenarios	6 (with 2,4,6,8,10,12 attacker nodes respectively).
Speed of vehicles	Between 20m/s and 70 m/s
Size of packet	512 bytes.
Type of Antenna	Omni-directional
Type of MAC	802.11
Simulation time	30 minutes
Type of Data traffic	Constant Bit Rate (CBR)
Routing Protocol	Ad-hoc on-demand Vector (AODV)

techniques useless.

As such, a technique other than cryptography is required to eliminate these attacks. In this section, we propose the VANET Black-hole Prevention (VBP) algorithm that is explained below.

The implementation of proposed algorithm depends on following points:

- Each time a node (Smart Vehicle) has to send data to another node in the network, it first finds the shortest path to destination node before sending data packets.
- Shortest path to destination node is calculated using two special control packets: Route Request Packet (RREQ) and Route Reply Packet (RREP).
- RREQ packet is generated and flooded by the source node, and contains the address of source and destination node.
- RREP packet is generated by the destination node when it receives RREQ packet. It is appended with the shortest path to source node (which has been calculated during the process of flooding of RREQ packet). It is sent as an acknowledgement to source node.
- Each intermediate node on receiving RREQ packet sends an RREP packet to source node if it has the shortest path to destination, otherwise it appends its address to RREQ packet and forwards it to neighbouring nodes.
- The source node on receiving RREP packets, extracts shortest path to destination node and uses this path to forward all the packets to destination node.
- Since the availability of computing resources at Road Side Unit (RSU) is high as compared to the smart vehicles, the nodes prefer to forward packets to destination via RSU (if it is in between source and destination node).
- RSUs not only acts as a high computing node in the smart vehicular network but also monitors the packets exchanged between smart vehicles.
- A list is maintained by an RSU: Blacklist(B), which contains the IDs of all those vehicles for which any malicious activity has been reported. Initially this list is empty.

The proposed security algorithm is executed by each node when it receives an RREP packet and its detailed working is explained as:

Algorithm:

Step-1: If the non-destination node initially generating an RREP packet, then report it to RSU which will put it in the blacklist (B), and discard the reply.

Step-2: Else if the node sending the RREP packet is already in the RSUs blacklist (B), then simply discard its reply and inform source node to re-initiate route request process.

Step-3: Else accept the RREP packet and forward it to the source node.

6.1. Experimental set-up and Evaluation. Our simulation settings and the parameters are listed in table 6.1. In every simulation, VBP is perfectly able to separate the attacks from the network.

The effect of the black-hole attack on throughput and Packet Delivery Ratios (PDR) are noted in figure

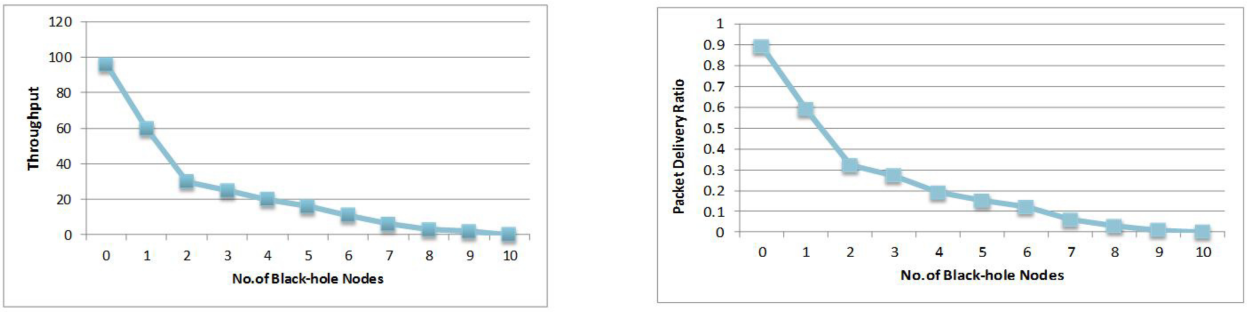


FIG. 6.1. *Effect of Black-hole attack on Throughput and Packet Delivery Ratio*

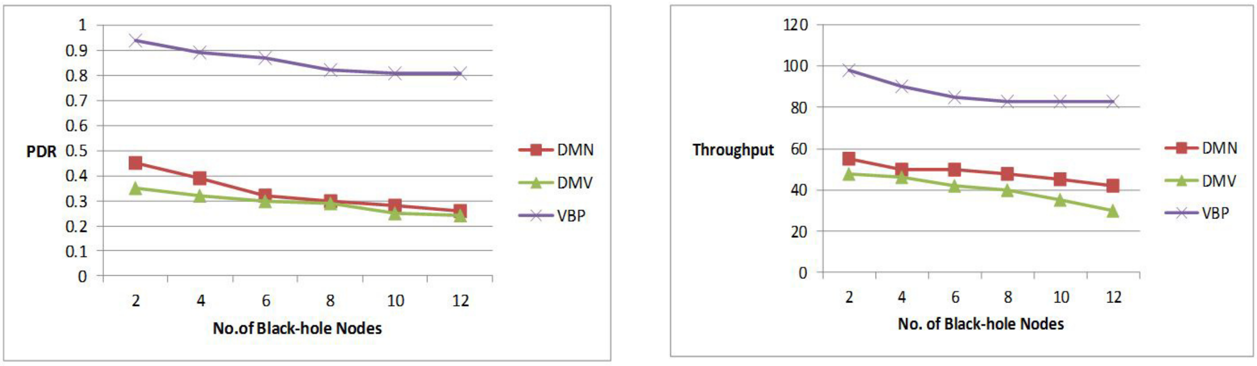


FIG. 6.2. *Comparison of Proposed VBP with DMN and DMV*

6.1. The attacker nodes have been chosen randomly and a realistic scenario of traffic has been created using SUMO.

Figure 6.1 demonstrates that as the number of attacker nodes increase, the throughput and the PDR parameters decrease by a considerable amount, and touch zero when the number of attacker nodes reach to a value of ten. These figures orchestrate how badly the attacks on availability can affect the VANETs.

After analyzing the effect of black-hole attack, we have applied our VBP algorithm on smart transport network and compared it with two of the most famous malicious node detection techniques namely, Detection of Malicious Vehicle (DMV) [116] and Detection of Malicious Node (DMN) [117].The comparison charts are displayed in figure 6.2.

Figure 6.2 indicates that with VBP applied on the network, the PDR and throughput remain almost constant and high as compared to DMV and DMN under the influence of attacks. This is for the reason that DMV calculates trust values for each vehicle by assigning the job of verifiers to some other vehicles. All the verifiers work continuously in their clusters which put unrequired pressure on them, leading to wastage of resources. DMN on the other hand, uses some verifiers for the process of trust calculation. DMV and DMN give lesser values of throughput and PDR for the reason that by the time malicious nodes are detected, crucial data packets are already lost. VBP is better as it eliminates the malicious nodes right at the beginning without requiring dropping of essential packets thereby maintaining high PDR and throughput rates.

7. Conclusion and Future Work. The features peculiar to IoT devices suggest that they are helpless when it comes to securing themselves. It was observed that even the proposed security mechanisms for alleviating the possible threats suffer from a lot of problems and are not sufficient in the IoT world. Most of these security and privacy solutions are WSN inspired and thus cannot display the same degree of efficacy in IoT.

The classical security solutions are ineffective in todays IoT deployment for so many more reasons. Firstly, because of the constrained nature of the IoT devices, they do not run full-fledged operating systems. In addition, these devices have long lives-ones in which they remain unattended and unsupported by their vendors. Secondly, IoT devices dont get automated software updates because they run long after the vendor stops producing/ supporting them. Thirdly, the prevalent security procedures stem from a static perimeter defense mindset (IDS or firewall at Gateways). Since the behavior of IoT devices and their environments flip, such approaches quickly become ineffective in IoT environments. It is concluded that more effective and practical solutions are needed to address the security issues of IoT, solutions that would not put unnecessary pressure on IoT devices rendering them exhausted for performing their intended functions, solutions that do not come from a static perimeter defense mindset but rather the ones that take into account the heterogeneous, mobile and unattended natures of IoT devices. Talking about the efficacy of the security solution, if the solutions that are already available for networks like WSNs or other ad-hoc networks are employed in IoT, they would not be 100% efficient because as discussed in this article, the features of IoT are very unique.

One of the most interesting future research tendencies lies in developing more efficient Intrusion Detection and Prevention Systems to deal with the problems of IoT devices. Researchers can also find an opportunity in the creation of secure procedures for remote attestation of unattended IoT devices. There is still a lot of potential in the development of efficient context-based permission systems for dealing with issues arising from implicit dependence and in the creation of a Dynamic Analysis Simulation Platform for covering the heterogeneity in IoT firmware.

REFERENCES

[1] Fari Assaderaghi et.al, *Privacy and Security: Key Requirements for Sustainable IoT Growth*, in Symposium on VLSI Technology Digest of Technical Papers, (2017).

[2] Djamel Eddine Kouicem, Abdelmadjid Bouabdallah , Hicham Lakhlef, *Internet of things security: A top-down survey*, in Computer Networks ,Elsevier, (2018).

[3] Wei Zhou et.al, *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, (2018).

[4] IETF, Available: https://tools.ietf.org/id/draft-feeney-t2trg-inter-network-02.html (accessed on 27 August 2018).

[5] Shen Bin et.al, *Research on Data Mining Models for the Internet of Things*, in IEEE, (2010).

[6] Muneer Bani Yassein et.al, *Mobility Management of Internet of Things: Protocols, Challenges and Open Issues*, in IEEE (2017).

[7] C. Kruger, G. Hancke, *Implementing the internet of things vision in industrial wireless sensor networks*, in Proceedings of the 12th IEEE International Conference on Industrial Informatics (2014).

[8] A. Perrig, J. Stankovic, D. Wagner, *Security in wireless sensor networks*, in Commun ACM (2004).

[9] Kewei Sha , Wei Wei , T. Andrew Yang , Zhiwei Wang, Weisong Shi, *On security challenges and open issues in Internet of Things*, in Future Generation Computer Systems, Elsevier (2018).

[10] K. Sha, J. Gehlot, R. Greve, *Multipath routing techniques in wireless sensor networks: A survey*, in Wirel. Pers. Commun. (2013).

[11] Johana A. Manrique, Johan S. Rueda-Rueda, Jesus M.T. Portocarrero, *Contrasting Internet of Things and Wireless Sensor Network from a conceptual overview*, in IEEE International Conference on Internet of Things, (2016).

[12] I. I. Initiative, *Towards a definition of the internet of things (iot)*, In Tech.Rep. (2015).

[13] G.A.Y. Wang, B. Ramamurthy, *A survey of security issues in wireless sensor networks*, in IEEE Commun. Surv. Tutor. (2006).

[14] T. Milbourn, Available:https://www.u-blox.com/en/blog/ip-versus-coap-iot-communications (accessed on August 2018).

[15] T. Bokareva, et al., *Wireless sensor networks for battlefield surveillance*, in Proceedings of Land Warfare Conference (2006).

[16] L. Larkey, L. Bettencourt, A. Hagberg, *In-situ data quality assurance for environmental applications of wireless sensor networks*, in Tech. Rep. Report LAUR-06-1117, Los Alamos National Laboratory, (Oct. 2006).

[17] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, Faiz Alotaibi, *Internet of Things security: A survey*,in Journal of Network and Computer Applications, Elsevier, (2017).

[18] H. Chan, A. Perrig, D. Song, *Random key predistribution schemes for sensor networks*, in: Proceedings of ACM CCS03, (2003).

[19] W. Du, J. Deng, Y. Han, P. Varshney, *A pairwise key pre-distribution scheme for wireless sensor networks*, in: Proceedings of ACM CCS03, (2003).

[20] M. Anita, R. Geetha, E. Kannan, *A novel hybrid key management scheme for establishing secure communication in wireless sensor networks*, in Wirel. Pers. Commun (2015).

[21] D. Liu, P. Ning, R. Li, *Establishing pairwise keys in distributed sensor networks*, in ACM Trans. Inf. Syst. Secur. (TISSEC) (2005).

[22] B. Bowerman, J. Braverman, J. Taylor, H. Todosow, U. Von Wimmersperg, *The vision of a smart city*, In: 2nd

International Life Extension Technology Workshop, Paris, vol. 28 , (2000).

[23] R.G. Hollands, *Will the real smart city please stand up? intelligent, progressive or entrepreneurial? City*, 12(3), 303 - 320 , (2008).

[24] Tai-hoon Kim, Carlos Ramos, Sabah Mohammed, *Smart City and IoT*, in Future Generation Computer Systems, Elsevier (2017).

[25] United Nations Population Fund (UNFPA) (2012), *Ageing in the twenty-first century: a Celebration and A Challenge*, Available: http://www.unfpa.org/publications/ageing-twenty-first-century (Accessed: August 2018).

[26] Global Health Workforce Alliance, World Health Organization (2013), *A universal truth: No health without a Workforce*, Available: http://www.who.int/workforcealliance/knowledge/resources/hrhreport2013/en/ (Accessed: August 2018).

[27] Haider Mshali, Tayeb Lemlouma , Maria Moloney, Damien Magoni, *A survey on health monitoring systems for health smart homes*, in International Journal of Industrial Ergonomics, Elsevier, vol:66, pp:26-56 (2018).

[28] Kirsten K. B. Peetoom, Monique A. S. Lexis, Manuela Joore, Carmen D. Dirksen, Luc P. De Witte, *Literature review on monitoring technologies and their outcomes in independently living elderly people*, in Disabil Rehabil Assist Techno, UK, (2014).

[29] Van der Gaag, N. De potentiele, beroepsbevolking , in de Europese Unie: van groei naar krimp. Den Haag/Heerlen: Statistics Netherlands [CBS] (2012).

[30] Van Duin CG J. Bevolkingsonderzoek 2010-2060, in sterkere vergrijzing, langere levensduur. Den Haag/Heerlen: Statistics Netherlands [CBS] (2010).

[31] W. AL-mawee, *Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey*, Western Michigan University, 1903 W Michigan Ave, Kalamazoo, MI 49008, USA, (2012) Masters thesis .

[32] T.D.J. Clements-Croome, *What do we mean by intelligent buildings?*, in Automation in Construction 6 (1997) 395-399.

[33] W.M. Kroner, *An intelligent and responsive architecture*, in Automation in Construction 6,381393 (1997).

[34] M. Wigginton, J. Harris, *Intelligent Skin*, in Architectural Press, Oxford, UK, (2002).

[35] Terence K.L. Huia, R. Simon Sherratt, Daniel Daz Snchez, *Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies*, in Future Generation Computer Systems, Elsevier (2016).

[36] Syed Rameem Zahra, *MNP: malicious node prevention in vehicular ad hoc networks*, in International Journal of Computer Networks and Applications (2018).

[37] Debasis Bandyopadhyay, Jaydip Sen, *Internet of Things: Applications and Challenges in Technology and Standardization*, in Wireless Pers Commun,Springer (2011).

[38] M.N. Mejri , J. Ben-Othman , M. Hamdi, *Survey on vanet security challenges and possible cryptographic solutions*, in Veh. Commun. 1 (2), 53-66 (2014).

[39] M. Brettel, N. Friederichsen, M. Keller, and M. Rosenberg, *How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective*, in International Journal of Mechanical, Industrial Science and Engineering, vol. 8, no. 1, pp. 37-44 (2014).

[40] J. Wan, D. Zhang, Y. Sun, K. Lin, C. Zou, and H. Cai, *VCMIA: a novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing*, in Mobile Networks and Applications, vol. 19, no. 2, pp. 153-160 (2014).

[41] Baotong Chen, Jiafu Wan, Lei Shu, Peng Li, Mithun Mukherjee and Boxing Yin, *Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges*, in IEEE Access (2017).

[42] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, *Edge computing: Vision and challenges*, in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646 (2016).

[43] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, *Industry 4.0*, in Business & Information Systems Engineering, vol. 6, no. 4, pp.239-242 (2014).

[44] E. Commission, *Europe 2020: A Strategy for smart, sustainable and inclusive growth*, Working paper [COM (2010) 2020], (2010).

[45] J. Holdren, T. Power, G. Tassey, A. Ratcliff, and L. Christodoulou, *A National strategic plan for advanced manufacturing*, in US National Science and Technology Council, Washington, DC (2012).

[46] A.-R. Sadeghi, C. Wachsmann, M. Waidner, *Security and privacy challenges in industrial internet of things*, in: 2015 52nd ACM/EDAC/IEEE on Design Automation Conference (DAC), IEEE, pp. 1-6 (2015).

[47] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, Chenren Xu, *Handling a trillion (unfixable) flaws on a billion devices:Rethinking network security for the Internet-of-Things*, in HotNets, ACM (2015).

[48] Jia, Yunhan Jack, et al., *ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms*, in Network and Distributed System Security Symposium , pp. 1-15 (2017).

[49] Luca Mainetti, Luigi Patrono, Andrea Secco, and Ilaria Sergi, *An IoT-aware AAL System for Elderly People*, in International Multidisciplinary Conference on Computer and Energy Science (SpliTech), IEEE (2016).

[50] Ali (2015), *Internet of things security report[Online]*, Available: https://jaq.alibaba.com/community/art/show?articleid =195 (accessed july 2018).

[51] JD. (2015). *Joylink*, Available: http://smartdev.jd.com/ (accessed july 2018).

[52] Yang Yu, *BadTunnel:NetBIOS Name Service spoofing over the Internet*, in Tencents Xuanwu Lab (2016).

[53] File Manipulation, Available: https://capec.mitre.org/data/definitions/165.html (accessed august 2018).

[54] File Discosure, Available: https://teamultimate.in/full-path-disclosure-attack-explained-tutorial/ (accessed august 2018).

[55] Command Injection , Available: http://cwe.mitre.org/data/definitions/77.html (accessed august 2018).

[56] Code Injection, Available: https://www.owasp.org/index.php/Code_Injection (accessed august 2018).

[57] Unserialize, Available: http://php.net/manual/en/function.unserialize.php (accessed august 2018).

[58] Andrei Costin, Jonas Zaddach, Aurelien Francillon and Davide Balzarotti, *A Large-Scale Analysis of the Security*

of Embedded Firmwares, in 23rd USENIX Security Symposium (2014).

[59] Drew Davidson,Benjamin Moench, Somesh Jha, Thomas Ristenpart, *FIE on Firmware: Finding Vulnerabilities in Embedded Systems using Symbolic Execution*, in 22nd USENIX Security Symposium (2013).

[60] Jonas Zaddach, Luca Bruno, Aurelien Francillon and Davide Balzarotti, *Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares*, in Internet Society (2014).

[61] Daming D. Chen, Manuel Egele, Maverick Woo, and David Brumley, *Towards Automated Dynamic Analysis for Linux-based Embedded Firmware*, in Internet Society (2016).

[62] Franqueira, Virginia Nunes Leal and Wieringa, Roel J, *Role Based Access Control in Retrospect*, in Central Lancashire online Knowledge (2012).

[63] OASIS, *eXtensible Access Control Markup Language (XACML) Version 3.0*

[64] Sergio Gusmeroli a, Salvatore Piccione, Domenico Rotondi, *capability-based security approach to manage access control in the Internet of Things*, in Mathematical and Computer Modelling,Elsevier 58, 1189-1205 (2013).

[65] Ki-Wook Kim , Youn-Hee Han, Sung-Gi Min, *An Authentication and Key Management Mechanism for Resource Constrained Devices in IEEE 802.11-based IoT Access Networks*, in Sensors (2017).

[66] Zhao, Lu, et al., *ARMor: fully verified software fault isolation*, In Proceedings of the International Conference on Embedded Software IEEE, 289-298 (2011).

[67] Schulz, Patrick Koeberl Steffen, Ahmad-Reza Sadeghi, and Vijay Varadharajan, *Trustlite: A security architecture for tiny embedded devices*, In EuroSys. ACM, pp:1-14 (2014).

[68] Guo, Fuchun, et al. , *CP-ABE With Constant-Size Keys for Lightweight Devices*, In IEEE Transactions on Information Forensics & Security 9.5, pp. 763-771 (2014).

[69] Fan, Hongfei, et al., *An ultra-lightweight white-box encryption scheme for securing resource-constrained IoT devices*, In Conference on Computer Security Applications ACM, pp.16-29 (2016).

[70] Buchmann, Johannes, et al., *High-performance and lightweight lattice-based public-key encryption*, In Proceedings of the 2nd ACM 10 International Workshop on IoT Privacy, Trust, and Security. ACM, pp. 2-9 (2016).

[71] Rauter, Tobias, N. Kajtazovic, and C. Kreiner, *Privilege-Based Remote Attestation: Towards Integrity Assurance for Lightweight Clients*, in ACM Workshop on IoT Privacy, Trust, and Security .ACM,pp. 3-9 (2015).

[72] B. Hayes, *Cloud Computing*, Commun. ACM, vol. 51, no. 7, pp. 9-11 (2008).

[73] N. C. Luong et al., *Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey*, in IEEE Commun. Surveys Tuts., vol. 18, no. 4, pp. 25462590, 4th Quart. (2016).

[74] R. Roman, J. Lopez, and M. Manbo, *Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges*, Future Gener. Comput. Syst., vol. 78, pp. 680-698 (Jan. 2018).

[75] Mithun Mukherjee, Rakesh Matam, Lei Shu, Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury, Vikas Kumar, *Security and Privacy in Fog Computing: Challenges*, in IEEE Access (2017).

[76] Multitude threat, *Available: https://www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/ (accessed august 2018).*

[77] Mirai, Available: https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/ (accessed august 2018).

[78] Mirai, Available: https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html(accessed august 2018).

[79] Mirai, Available:http://effortlessoffice.com/mirai-botnet-attack-costs-companies-hundreds-of-millions/(accessed august 2018).

[80] Mirai, Available: https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html(accessed august 2018).

[81] Reaper, Available: https://krebsonsecurity.com/2017/10/reaper-calm-before-the-iot-security-storm/(accessed august 2018).

[82] Reaper, Available: https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/(accessed august 2018).

[83] Reaper, Available: https://www.fortinet.com/blog/threat-research/reaper-the-next-evolution-of-iot-botnets.html(accessed august 2018).

[84] Reaper, Available: https://www.zdnet.com/article/reaper-botnet-experts-reassess-size-and-firepower/(accessed august 2018).

[85] Sam Edwards, Ioannis Profetis, *Hajime: Analysis of a decentralized internet worm for IoT devices*, in Rapidity Networks Security Research Group (2016).

[86] Hajime, Available: https://www.corero.com/blog/882-hajime-botnet-scanning-for-vulnerable-mikrotik-routers.html (accessed august 2018).

[87] Hajime, Available: https://indianexpress.com/article/technology/tech-news-technology/mysterious-hajime-malware-infecting-iot-network-globally-4631556/ (accessed august 2018).

[88] Wannacry, Available: http://www.hendonpub.com/resources/article_archive/results/details?id=5903 (accessed august 2018).

[89] Perseria, Available: https://www.theinquirer.net/inquirer/news/3009839/persirai-mirai-a-like-malware-is-your-latest-iot-security-worry(accessed august 2018).

[90] Perseria, Available: https://securityaffairs.co/wordpress/59900/malware/persirai-iot-botnets.html(accessed august 2018).

[91] Bushra Zaheer Abbasi, Munam Ali Shah, *Fog Computing: Security Issues, Solutions and Robust Practices*, in Proceedings of the 23rd International Conference on Automation & Computing, University of Hudders field, Hudders field, UK, 7-8 (September 2017).

[92] Zhang, Congyingzi, and R. Green, *Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network*, Symposium on Communications & NETWORKING Society for Computer Simulation International,

pp. 8-15 (2015).

[93] Guan, Le, et al., *TrustShadow: Secure execution of unmodified applications with ARM trustzone*, in Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services, ACM (2017).

[94] K. E. Defrawy, A. Francillon, D. Perito, and G. Tsudik, *SMART: Secure and minimal architecture for (establishing a dynamic) root of trust*, in Network. & Distribution. System. Security Symp (2012).

[95] Copos, Bogdan, et al., *Is Anybody Home? Inferring Activity From Smart Home Network Traffic*, In Security and Privacy Workshops IEEE, pp. 245-251 (2016).

[96] K. Ki-Sik, S. MoonBae, Kwang Jin, P.A.R.K. and C.S Hwang, *A comparative analysis on the signaling load of Mobile IPv6 and Hierarchical Mobile IPv6: Analytical approach*, in IEICE Transactions on Information and Systems, 89(1), 139-149 (2006).

[97] Wikipedia contributors, Packet loss (2016), Available: https://en.wikipedia.org/wiki/Packet_loss (accessed july 2018).

[98] K. S. Kong, W. Lee, Y. H. Han and M. K. Shin, *Handover latency analysis of a network-based localized mobility management protocol*, In IEEE International Conference on Communications, pp. 5838-5843 (2008).

[99] Wikipedia contributors, End-to-end delay, Available: https://en.wikipedia.org/wiki/End-to-end_delay (accessed july 2018).

[100] Y. Xu, *Minimize end-to-end delay through cross-layer optimization in multi-hop wireless sensor networks* (2010).

[101] H. Y. Hwang, S. J. Kwon, Y. W. Chung, D. K. Sung and S. Park, *Modeling and Analysis of an Energy-Efficient Mobility Management Scheme in IP-Based Wireless Networks*, in Sensors, 11(12), pp.11273-11294 (2011).

[102] Samsung SmartThings, Available: https://www.smartthings.com/ (accessed july 2018).

[103] C. Perkins, *IP mobility support for IPv4*, No. RFC 3344 (2002).

[104] D. Johnson, C. Perkins and J. Arkko, *Mobility support in IPv6*, No. RFC 3775 (2004).

[105] N. Jora, *Mobile IP and Comparison between Mobile IPv4 and IPv6. Journal of Network Communications and Emerging Technologies*, in (JNCET) www. jncet. org, 2(1) (2015).

[106] T. Narten, W.A. Simpson, E. Nordmark, and H. Soliman, *Neighbor discovery for IP version 6 (IPv6)*, (2007).

[107] H. Soliman, L. Bellier and K.E. Malki, *Hierarchical mobile IPv6 mobility management (HMIPv6)*, (2005).

[108] V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert, *Network mobility (NEMO) basic support protocol*, No. RFC 3963 (2004).

[109] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil, *Proxy mobile ipv6*, No. RFC 5213 (2008).

[110] I. Joe & H. Lee, *An efficient inter-domain handover scheme with minimized latency for PMIPv6*, In Computing, Networking and Communications, in (ICNC). Proceedings of International Conference on IEEE, pp.332-336 (2012).

[111] M.M. Islam and E.N. Huh, *Sensor proxy mobile IPv6(SPMIPv6)-A novel scheme for mobility supported IP-WSNs*, in Sensors, 11(2), pp.1865-1887 (2011).

[112] A.J. Jabir, S.K. Subramaniam, Z.Z. Ahmad and N.A. Hamid, *A cluster-based proxy mobile IPv6 for IP-WSNs*, EURASIP Journal on Wireless Communications and networking, (1), pp.1-17 (2012).

[113] S. Ro and V.H. Nguyen, *Inter-domain mobility support in Proxy Mobile IPv6 using overlap function of mobile access gateway*, in Wireless Networks, 21(3), pp.899-910 (2015).

[114] Z. Shelby, K. Hartke and C. Bormann, *The constrained application protocol (CoAP)*, in No. RFC 7252 (2014).

[115] S.M. Chun, H.S. Kim, and J.T. Park, *CoAP-Based Mobility Management for the Internet of Thing*, in Sensors, 15(7), pp.16060-16082 (2015).

[116] Ameneh Daeinabi, Akbar Ghaffarpour Rahbar, *Detection of malicious vehicles (DMV) through monitoring in vehicular Ad-hoc Networks*, Springer, pp. 325-338 (2013).

[117] Uzma Khan, Shikha Agarwal, Sanjay Silakari, *Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks*, Elsevier, pp 965- 972 (2015).

Edited by: Shajulin Benedict
Received: March 31, 2019
Accepted: August 30, 2019