Computer Networks 129 (2017) 444–458

Contents lists available at ScienceDirect

Computer Networks

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

The rise of ransomware and emerging security challenges in the Internet of Things

Ibrar Yaqoob[a,*], Ejaz Ahmed[a,1], Muhammad Habib ur Rehman[b], Abdelmuttlib Ibrahim Abdalla Ahmed[a], Mohammed Ali Al-garadi[c], Muhammad Imran[d,2], Mohsen Guizani[e,3]

[a] Centre for Mobile Cloud Computing Research, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia
[b] COMSATS Institute of Information Technology, Wah Campus, 47040 Pakistan
[c] Department of Information Systems, University of Malaya, Malaysia
[d] College of Computer and Information Sciences, King Saud University, Saudi Arabia
[e] Department of Electrical and Computer Engineering, University of Idaho, USA

ARTICLE INFO

Article history:
Received 16 December 2016
Revised 31 August 2017
Accepted 6 September 2017
Available online 6 September 2017

Keywords:
Internet of Things
Security
Authentication
Ransomware
Trust

ABSTRACT

With the increasing miniaturization of smartphones, computers, and sensors in the Internet of Things (IoT) paradigm, strengthening the security and preventing ransomware attacks have become key concerns. Traditional security mechanisms are no longer applicable because of the involvement of resource-constrained devices, which require more computation power and resources. This paper presents the ransomware attacks and security concerns in IoT. We initially discuss the rise of ransomware attacks and outline the associated challenges. Then, we investigate, report, and highlight the state-of-the-art research efforts directed at IoT from a security perspective. A taxonomy is devised by classifying and categorizing the literature based on important parameters (e.g., threats, requirements, IEEE standards, deployment level, and technologies). Furthermore, a few credible case studies are outlined to alert people regarding how seriously IoT devices are vulnerable to threats. We enumerate the requirements that need to be met for securing IoT. Several indispensable open research challenges (e.g., data integrity, lightweight security mechanisms, lack of security software's upgradability and patchability features, physical protection of trillions of devices, privacy, and trust) are identified and discussed. Several prominent future research directions are provided.

1. Introduction

Immigrating to a promising era of the Internet of Things (IoT), ubiquitously small embedded devices are implanted with various sensors to sense data from their surroundings and provide smart controlling decisions. The proliferation of miniaturized sensors and connected IoT devices is expected to reach 26 billion by 2020, most of which are wearable devices [1]. In this modern era of technology, people have started to deploy real-world IoT applications, from connected smart homes [2], connected cars [3,4], smart parking [5], and health monitoring [6,7] to smart utility meters [8], as shown in Fig. 1. Although IoT can facilitate different aspects of people's lives, enabling high security, developing ransomware prevention, and establishing solutions are the key remaining concerns, given that IoT devices hold sensitive information [9].

A HP study reveals that 70% of IoT devices are vulnerable to attacks[4]. Hacking of smart cars is also one of the security threats in IoT [10]. According to recent market data, the IoT security market is expected to rise to $28.90 billion by 2020, which indicates that high-security threats are expected to rise substantially in the foreseeable future[5]. On the other hand, ransomware continues to experience record growth in 2017. Therefore, ensuring that each device has the appropriate control to maintain data confidentiality and in-

* Corresponding author.
E-mail addresses: ibraryaqoob@siswa.um.edu.my (I. Yaqoob), ejazahmed@ieee.org (E. Ahmed), habibcomsats@gmail.com (M.H.u. Rehman), abdelmuttlib@siswa.um.edu.my (A.I.A. Ahmed), mohammedali@siswa.um.edu.my (M.A. Al-garadi), dr.m.imran@ieee.org (M. Imran), mguizani@ieee.org (M. Guizani).
[1] Member, IEEE.
[2] Member, IEEE.
[3] Fellow, IEEE.

[4] http://www.itpro.co.uk/security/22804/hp-70-of-internet-of-things-devices-vulnerable-to-attack .
[5] http://formtek.com/blog/internet-of-things-security-most-early-entry-iot-devices-have-weak-security-at-best/.

http://dx.doi.org/10.1016/j.comnet.2017.09.003
1389-1286/

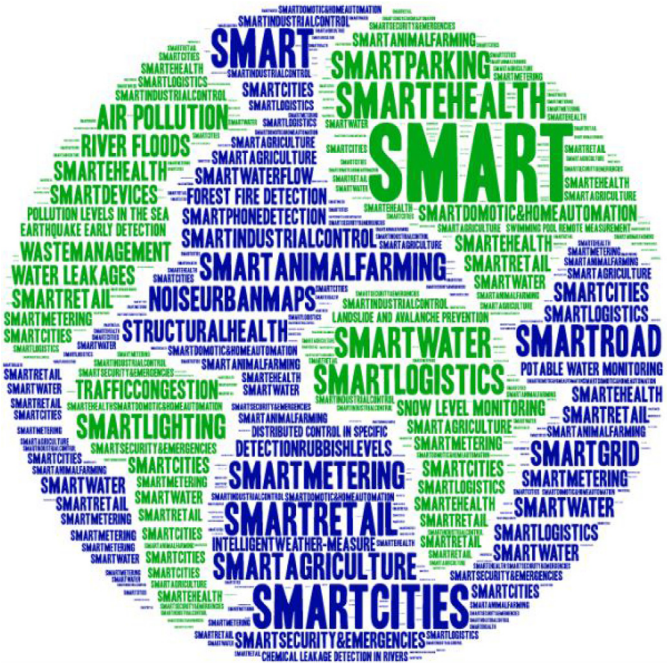

Fig. 1. Illustration of IoT applications.

tegrity within an organization is necessary [11]. In addition, investigation of IoT security along with data integrity holds practical significance in IoT development. Fig. 2 illustrates the security threats in IoT. Traditional security mechanisms will be unable to accommodate IoT devices completely because most of these devices have battery constraints and limited resources; however, these mechanisms require more resources [12]. Therefore, the prime focus of this study is on exposing emerging IoT threats, challenges, and potential solutions.

In general, IoT security has been widely investigated [13–22]; however, to the best of our knowledge, none of the existing studies specifically focused on emerging threats and challenges, such as ransomware. In addition, several other important aspects of IoT security, which are discussed in the current study, have not been reported.

The contributions of this study can be summarized as follows.

- We initially discuss the rise of ransomware attacks and outline the associated challenges.
- We investigate, report, and highlight the state-of-the-art research efforts directed at IoT from the security perspective.
- We devise a taxonomy of IoT security by classifying and categorizing the literature.
- A few notable reported case studies on IoT security are outlined.
- We enumerate the requirements for securing IoT.
- We identify and discuss indispensable open challenges in strengthening the security in IoT.
- Several prominent future research directions are provided.

These contributions are provided separately from Sections 2 to 8; the concluding remarks are provided in Section 9.

2. Ransomware

This section describes the basic working of ransomware in an IoT context and discusses their common types. We also discuss some of the approaches used by ransomware to penetrate in the IoT network and provided some examples of IoT-based ransomwares. Finally, some remedies and challenges are highlighted.

Unlike traditional malware threats, a ransomware attack in IoT can be more devastating as it may affect an entire landscape of security services, i.e., confidentiality, integrity, and availability, which may not only result in financial losses but may also result in important information breaches [23]. A ransomware may take entire control of data or a system and allow limited access for user interaction with the devices, ask for a hefty sum as a ransom, and release data to the user only after successful payment. In case a user does not pay, ransomware either extends the payment periods and ransom amount or deletes the data from the devices [24].

Initially, ransomware was named “AIDS”, as reported in 1989, when Joseph Popp distributed 20,000 infected floppy disk drives to the participants of the World Health Organizations’ AIDS conference [25]. AIDS monitored the systems and counted number of times for which the systems were rebooted. It used to either encrypt data files or hide directory folders in the C drive of infected computers. AIDS used to silently stay in the systems and get activated after a system reboots for 90 times. AIDS did not proliferate at massive scale because of less connectivity of computers and absence of large-scale exposure with other devices and systems.

Later, ransomware appeared and infiltrated computers using different fraudulent, malicious, and fake applications [26]. Such software tricked users by generating false alarms (e.g., falsely reporting that users’ data and system are compromised) and ask for money to recover the data.

From 2005 to March 2016, approximately 7600 ransomware attacks were reported by Internet Crime Complaint Center (IC3). The literature review shows that early attacks were not immensely dangerous because of less connectivity of computers and difficulties in collection of ransom money from users. However, current technology trends such as gigantic growth of IoT devices, connectivity of devices and users, exposure of users’ personal data through social media, and the prevalence of cryptocurrencies have enabled hackers to easily infiltrate devices and collect ransom money from device owners.

Ransomware works differently in display-based and display-less IoT devices [27,28]. IoT devices generally have minimal-sized display screens or come without display screens. In the case of former, ransomware attacks work in a way similar to that in legacy computers [29]. Hackers first penetrate IoT devices, encrypt the data files, ask for a ransom amount, and issue the decryption key to unlock the devices in case of successful receipt of ransom money. However, penetrating ransomware in IoT devices is challenging because attackers need to determine the right owners of the devices to demand ransom money. In addition, most IoT devices are controlled/managed by other devices; hence, the attacker need to find the controlling device to penetrate and encrypt the data. In case of IoT, the successful attacks can take place only if the attacker is fully aware of topological settings of the IoT network.

Considering the history, tiny IoT devices have not been an attractive target of ransomware attacks so far. This is mainly because these devices usually collect data streams from onboard sensory and non-sensory sources and immediately transfer it to application servers or cloud data centers. Therefore, gaining control over IoT data has less attraction as compared to legacy computers. Similarly, due to large-scale deployment, determining the right owner of IoT devices (especially in mobile IoT) is difficult. In traditional ransomware attacks, an attacker can easily launch the attack and enable the user to transfer the money from the same system. However, in IoT devices, an attacker may need to launch a ransomware attack from multiple devices due to limitation in interaction interfaces. On the other hand, ransomware is a big attraction for attackers focusing on mission critical and real-time systems [30]. These types of IoT devices and systems include life-support systems, industrial robotics, smart manufacturing machinery, smart railway systems, smart cars, and smart airplanes.

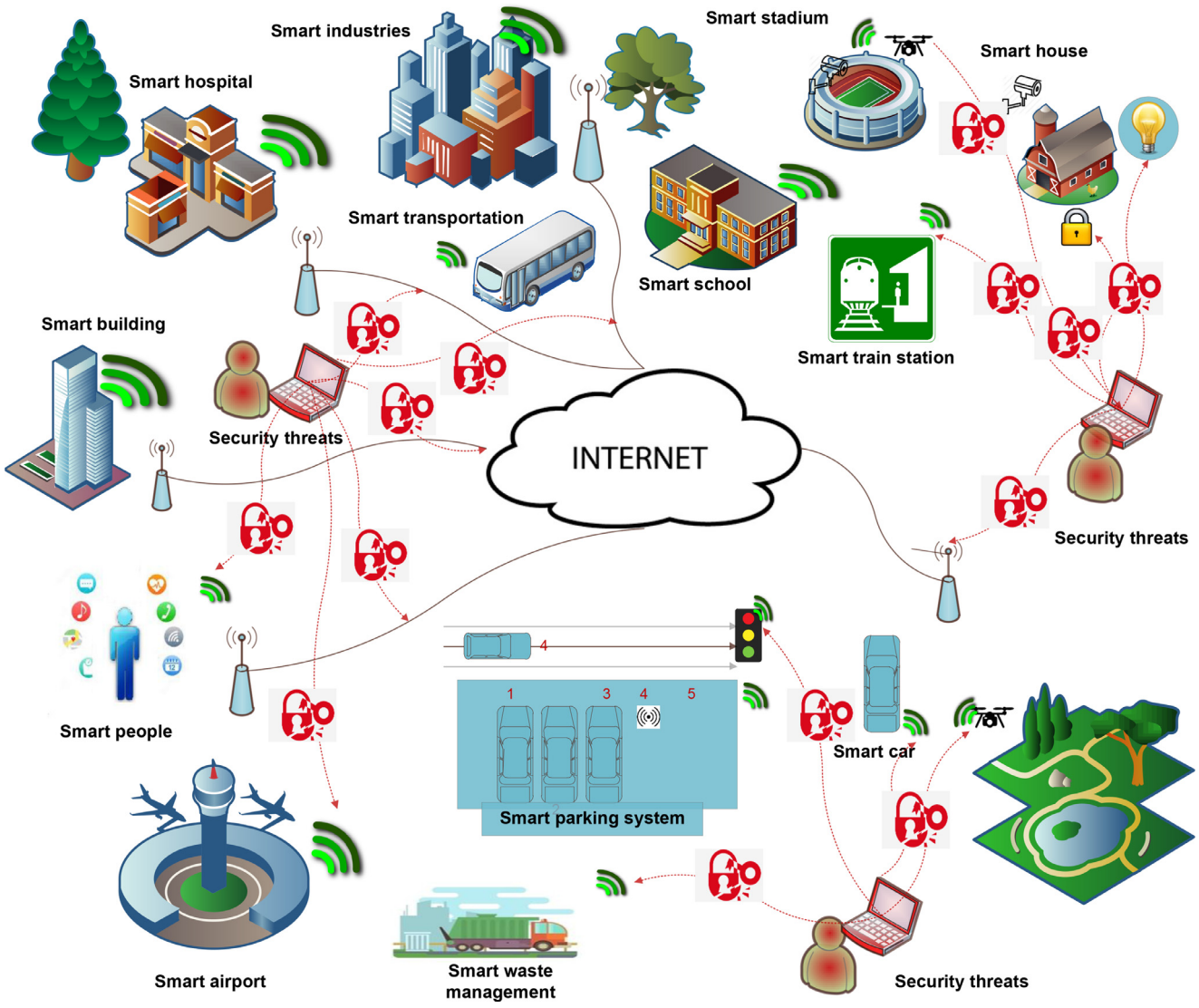

Fig. 2. Illustration of security concerns in an Internet of Things environment.

2.1. Common types of ransomware

Ransomware are categorized into three basic types.

2.1.1. Crypto ransomware

A crypto ransomware works by applying encryption and decryption algorithms on device data. Such ransomware usually works on public-private key relationships whereby data is encrypted using public keys and users are given back the private keys to decrypt their data. In the case of IoT devices, a crypto ransomware is more dangerous when it attacks back-end application servers because IoT devices at the forefront do not contain a large amount of data.

2.1.2. Locker ransomware

A locker ransomware works by restricting user access to device/system functionalities. In addition, more dangerous Locker ransomware may alter the functionality of IoT devices to persuade device owners to pay ransom money. In typical IoT scenarios, restricting user access is subject to disabling user interfaces, inactivating onboard sensors, and generating Denial of Service (DoS) attacks to degrade the device performance. A locker ransomware can also alter the operating behavior of IoT devices and locks the device until the device owner pays the ransom. For example, controlling the thermostat in an industrial production unit may increase the energy consumption, thus causing monetary loss. Locker ransomware attacks are usually launched at the front-end IoT devices.

2.1.3. Hybrid ransomware

Hybrid ransomware attacks that enable encryption and locking mechanisms are more dangerous because the device data and functionality could be compromised. A hybrid ransomware attack could become more vicious because it can target front-end and back-end IoT devices and systems. Although technically, launching hybrid ransomware attacks are difficult due to device heterogeneity, ownership, and multilayer deployment of IoT systems, such attacks could easily paralyze an entire IoT network, including front-end devices and back-end application servers.

2.2. Ransomware penetration methods

In the case of IoT devices, ransomware may penetrate in multiple ways.

2.2.1. Content delivery network (CDN) and malvertisement

Massive distribution of ransomware can take place if the malware is embedded in multimedia and Internet traffic [31]. Attackers can intercept CDN traffic in the back-end edge networks and at the front-end IoT devices. The ransomware can hold the CDN traffic using back-end cache servers and onboard memory of IoT devices. Attackers can also trap IoT device users through malvertisement, wherein the advertised material through CDN seems legitimate but contains malware, which users erroneously install on their devices and compromise data/device security.

2.2.2. Botnets and downloaders

Ransomware can also be penetrated using botnets that silently roam inside IoT networks. Attackers may use phishing emails, in which users are asked to download attached files or click on certain links. Once a botnet gets activated in result of users' or devices' activities in response to a phishing email, the entire IoT network is compromised. A botnet could also become a vehicle for self-propagating ransomware, which may cause flooding and DoS attacks within an IoT network [32]. When a device/network security is compromised, the related information of the device/data could be sold to other ransomware attackers and botnet operators. Therefore, compromised data and devices remain under constant threat even after removing the ransomware from the network.

2.2.3. Social engineering

Ransomware using social engineering tactics is an easy tool to trap users whereby attackers portray themselves as legal authorities and collect user information to penetrate user systems. However, IoT devices usually do not provide direct interaction with external users. Ransomware attacks in this case could be launched by external users by presenting themselves as legitimate users/devices within the IoT network.

2.2.4. Ransomware-as-a-service

Given that IoT devices heavily depend on application services and cloud data centers, attackers can intercept device-cloud traffic and inject ransomware. At the device end, the ransomware may appear as a subscribed service. However, when the IoT device uses the infected services, the entire IoT network is under threat.

2.3. Current ransomware

Given that IoT devices and systems are a relatively new research field, only a few ransomware attacks have been reported in the literature. Table 1 presents a comprehensive list of notable ransomware attacks. Few IoT-related ransomware attacks are presented and discussed below.

2.3.1. Thermostat hacking

Tierney and Munro hacked a thermostat device to prove that IoT devices could be hacked for ransom. The researchers had no malicious intent but wanted to show that such an attack is possible. The idea behind their research was to highlight the importance of IoT device security to create awareness against malicious attacks. The ransomware was downloaded by exploiting an undisclosed bug in an IoT application, which was then revealed to a thermostat vendor to fix for future devices. The hacked thermostat device was running on Linux OS and included a large display screen and external SD memory card for data storage. The researchers found that the thermostat device was not checking and verifying the files that were being executed, thus creating an opportunity to execute the ransomware and control device operations. Tierney and Munro argued that, similar to this experiment, other IoT devices in smart home settings could be hacked for ransom.

2.3.2. Flocker

Frantic Locker (i.e., Flocker) is a locker ransomware that penetrates in smart TV systems and locks the display screen. The ransomware was bundled in a fake movie screening application, and then activated when the user installed the application in a smart TV. It not only locks the screen but also disables the factory reset option. Flocker was originally developed in 2015 by security researchers of Trend Micro. Attackers are still re-engineering the application and penetrating in different devices by social engineering, spamming, downloading, and clicking on malicious links. Flocker asks $500 USD with a strict deadline of three days.

2.3.3. Android simplocker

Cybersecurity researchers at Symantec performed an experiment in which Android Simplocker ransomware is repackaged in an Android wear project. Given that the wearable devices need to be paired with Android smartphones, the ransomware penetrated in the devices when the Android wear application was installed in the device and the smartphones. Researchers demonstrated that Android Simplocker can lock the display of Android wearable devices. They suggested that in case of a ransomware attack, the wearable device must be rebooted before the ransomware reboots the device. Otherwise, factory reset is needed to remove the ransomware from the wearable device.

2.3.4. Smart bulb

Nassi, Shamir, and Elovici [24] presented a proof-of-concept ransomware to infiltrate business organizations using IoT devices and office equipment. The ransomware was injected in the organization's network using light that was transmitted into a flatbed scanner. The scanner was exploited as a gateway to establish a covert channel for the ransomware attack. The ransomware attack worked in three steps. First, a laser device was placed in a clear line-of-sight with the scanner. Second, the attackers used a drone device to launch the attack using an onboard laser device in the proximity of the targeted scanner. Third, the internal smart bulb was hacked using an Android device from a nearby car. The proof-of-concept application shows that ransomware attacks could become vicious and silently control the entire IoT network in the organizations.

Ransomware attacks on IoT devices and systems are still not prevailing because research on IoT devices and systems is slowly taking pace. Considering the initial experimental studies and recent attacks, such as WannaCry and Petya, IoT devices and systems must be carefully designed to mitigate ransomware-related risks.

2.4. Mitigation

Ransomware attacks could be mitigated by adopting multiple strategies. Given that ransomware attacks differ in nature, therefore, a dedicated team of cybersecurity professionals should be hired to perform in-depth forensic analysis and scan the entire network traffic periodically. In addition, device users must be trained to restart, switch-off, and upgrade the device firmware. Another mitigation could be the deployment of layered defense strategies whereby ransomware must be scanned at multiple layers (i.e., IoT device, edge/application servers, and cloud data centers) [33,34].

2.5. Remedies (solutions)

Despite deploying highly sophisticated security mechanisms, attackers can find a way to penetrate systems. When the device/network is compromised, cybersecurity teams must instantly take the following measures.

- The incidence response teams must be immediately engaged to reduce the damage and stop further propagation of ransomware

Table 1
Popular ransomware attacks.

Ransomware	Year	Type	**Target devices and systems**
AIDS Trojan	1989	Locker ransomware	Floppy diskettes, Computers
Archievus	2005	Crypto ransomware	Computers
Gpcode.AK	2008	Crypto ransomware	Computers
Unnamed Trojan	2011	Locker ransomware	Computers, Operating systems
Reveton	2012	Social engineering	Computers, Mobile devices
CryptoLocker	2013	Crypto ransomware	Computers, Mobile devices
CryptoDefense	2014	Crypto ransomware	Computers, Mobile devices, Wearable devices
CryptoWall	2014	Crypto ransomware	Computers
Sypeng	2014	Social engineering	Android mobile devices
Koler	2014	Locker Ransomware	Android mobile devices
CTB-Locker	2014	Hybrid ransomware	Computers
SimplLocker	2014	Crypto ransomware	Mobile devices
LockerPin	2015	Locker ransomware	Mobile devices
TeslaCrypt	2015	Crypto ransomware	Data encryption on disk
Chimera	2015	Malvetisement	Data encryption on disk
LowLevel04	2015	Crypto ransomware	Remote desktop computers
7ev3n	2016	Crypto ransomware	Data encryption on disk
Ransomware32	2016	Locker ransomware	Computers
SamSam (SAMAS)	2016	Crypto ransomware	Computers
Locky	2016	Downloader	Computers
Petya	2016	Locker ransomware	Windows computers
KeRanger	2016	Crypto ransomware	Mac computers
Jigsaw	2016	Crypto ransomware	Windows computers
Maktub	2016	Crypto ransomware	Data encryption on disk
Cryptxxx	2016	Crypto ransomware	Windows operating system
PowerWare	2016	Locker ransomware	Windows operating system
ZCryptor	2016	Crypto ransomware	Data encryption on disk
GoldenEye	2016	Locker ransomware	Windows operating system
Crysis	2016	Crypto ransomware	Data encryption on disk
zCrypt	2016	Cryto ransomware	Data encryption on disk
WannaCry/WannaDecryptor	2017	Cryptoware	Data encryption on disk

inside IoT networks. These teams must immediately notify device users/owners and switch-off the infected devices. In addition, a backup device should be turned-on to run the network smoothly.

- In most cases, device owners cannot afford hiring a large team of security professionals. In this case, users must be trained on how to respond initially in case of a ransomware attack. In addition, device users must install and update reliable security scanning software to improve the overall security of an IoT network.
- Data from IoT devices/networks must be continuously backup in the back-end servers. A backup of application and device configuration files should also be prepared to restore the devices safely from a previous restore points. In this case, if the IoT data and device configuration files are stored in a reliable back-end data storage, users do not need to pay ransom for data recovery.
- Depending upon the value of data to users and devices, and critical level of IoT applications, the ransom amount must be paid sometimes.
- Device/network owners may negotiate with attackers for partial data release by paying a minimum amount of money. However, this situation may occur only rarely.

2.6. Ransomware challenges

Few notable challenges may arise during mitigation and application of remedies:

- Resetting IoT devices may not work in most cases because the devices are already compromised and owners are left with no option except paying the ransom amount. To address this challenge, researchers can develop new strategies for early ransomware detection before the devices are compromised. In case of known ransomware attacks, the devices must not be able to download certain file extensions or files having certain names as identifiers. To this end, IoT device vendors can provide a predefined list of data files that are interoperable and safe for execution inside an IoT device/network.
- The heterogeneity (in terms of operating systems, network topologies, communication interfaces, data, and sensors) in IoT devices brings immense challenge to incorporate security by design. To fully implement security by design, IoT devices/systems should be able to mitigate ransomware during the entire lifecycle of the application execution. This lifecycle begins from installation of security software to secure authentication and registration of devices in IoT networks. Furthermore, IoT devices should perform commissioning, configuring, monitoring, controlling, and decommissioning functions only within the networks.

3. State-of-the-art research on IoT security

Although various aspects of security are extensively investigated in different domains, such as ad hoc and sensor networks [35,36] and software defined networks [37,38], however, IoT security is still largely unexplored.

For example, the authors in [39] proposed a secure Message Queue Telemetry Transport (MQTT) mechanism called AUPS (Authenticated Publish Subscribe). The mechanism is developed by extending MQTT, which is a popular communication protocol in the IoT paradigm, by introducing a secure publish/subscribe system within the protocol. The developed mechanism proposed a key management framework, and introduces new policies, thus allowing flexible control of the flow of information in MQTT-powered IoT systems. The proposed system has been released as open source under an Apache v.2 license. In the future, the system must be tested in a larger and more complex environment in the presence of various networked brokers and Networked Smart Objects (NOSs), where issues related to synchronization of policies among hosts may arise.

A novel cloud architectural model is developed in [40] to provide better services in a smart home. The model enables secure seamless interaction among heterogeneous smart home devices provided by different vendors. Furthermore, this study reveals that the use of ontology methods is a better solution for the heterogeneity issues within the developed model by ensuring high security and privacy in IoT-based smart homes. However, the proposed solution is still in its infancy, and future advanced home services, (i.e., home device remote monitoring and control, and multimedia entertainment) need to be provided and deployed. In addition, secure intelligence extraction methods are still required in IoT-based smart homes.

An end-to-end security solution is proposed in [41] to secure a mobility-enabled healthcare IoT. The proposed solution is designed by employing a certificate based Datagram Transport Layer Security (DTLS) handshake between end-users and smart gateways as well as utilizing the session resumption technique. The proposed solution significantly outperforms the existing end-to-end security solutions in terms of communication overhead, energy consumption, and communication latency. However, the solution still needs to focus on further reducing the energy consumption while strengthening end-to-end security.

The authors in [42] proposed a novel framework that helps to detect sinkhole and selective-forwarding attacks in IoT. The framework comprised two modules: anomaly-based and specification-based intrusion detection modules. The specification-based anomaly module helps to analyze the behavior of the host nodes and send their data to the root nodes, whereas a anomaly-based agent employs the unsupervised optimum-path forest algorithm for projecting clustering models. In addition, the anomaly-based agent works in a distributed manner because it is based on a MapReduce framework. The proposed solution employs a voting method to analyze the suspicious behavior. Results of the proposed solution show that it outperforms the existing solutions. In the future, incorporation of the data mining techniques and intelligence-based methods may improve the performance of the proposed framework.

A previous study [43] proposed a privacy-preserving smart parking application system, which ensures that there is no leakage of confidential information between the system agents. In this context, the study adopts Elliptic Curve Cryptography (ECC), which is very suitable for resource-constraint devices. Furthermore, the study provides a generic implementation of ECC that runs on different host operating systems, such as Contiki, TinyOS, iSenseOS, ScatterWeb, and Arduino. Despite many advantages of the proposed system, implementation of the attribute-based credentials on embedded devices is still lacking, which can be performed in the future.

The researchers in [44] presented a distributed middleware layer called NOS, which helps to manage heterogeneous data and evaluates the security and quality level associated with each data unit. In addition, a security algorithm that helps to measure the trustworthiness of registered IoT data sources is proposed. The results of the proposed scheme are very promising. In the future, a key management system needs to be introduced in the proposed platform.

A Forensics-aware IoT (FAIoT) model is proposed in [45]. The model allows investigators to identify necessary pieces of evidence from the IoT environment, and then collects and analyzes the potential evidence in an efficient manner. In another study [46], a Digital Forensic Investigation Framework for IoT (DFIF-IoT) is proposed, which extends the investigation capabilities with a high degree of certainty. One of the key strengths of the framework is that *it complies with the ISO/IEC 27043: 2015, which is an international standard for information technology, security techniques, incident investigation principles, and process.*" The qualitative results reveal that incorporation of the DFIT-IoT in future digital forensic tools can facilitate effective forensic crime investigation in the IoT environment.

A model was proposed in [47] to help forensic experts in conducting investigations in the IoT paradigm. The model is based on triage and 1-2-3 zone models for a volatile-based data preservation. Although the proposed approach can help forensics experts in conducting investigations in the IoT environment with large-size-based perspective, the automation of this model is quite difficult in a practical environment. The authors in [48,49] proposed automatic authentication/forensics systems to identify, detect, and recognize audio forgery.

Arias *et al.* [50] investigated security-related concerns of wearable devices by considering the manufacturing practices and their consequence on both security and privacy issues. In this study, different types of devices, such as Google Nest Thermostat and the Nike+ Fuelband, are used to evaluate how the processes of manufacturing deals with the security and privacy issues. Moreover, the authors proposed a set of suggestions to enhance the current design flow with consideration of the security mechanisms, which can be implemented capably into wearable devices for a better security concept than the traditional manufacturing practice.

A previous work [51] aimed to improve the security level for smart home systems. In this context, equipment such as air conditioners, doors' control, thermostat, and lighting systems are linked with one another through IoT technologies. To have a robust security system, this study proposed encryption and hash algorithms through which the devices in the loT can perform secure communication. This encryption approach aims to ensure confidentiality while transmitting the messages. However, there are still two ways to compromise the security in this approach. First, the storing mechanism can be compromised with SQL injection. Second, the operating system (OS) itself may be compromised.

Bing *et al.* [52] enabled users to utilize the "multi-application RFID (Radio Frequency Identification)" in smart applications with a higher security level and greater performance efficiency. The proposed scheme implements the hash function and a random number to produce the respective module using a representative challenge response mechanism. Furthermore, the study proposes a new approach that can be used in "multi-application RFID" and "one-application RFID". This scheme claims to have higher security level and better performance than other existing schemes. However, for ensuring privacy and security, IoT still requires to have certain strict security mechanisms that can efficiently block malicious messages within the IoT structure.

The authors in [53] focused on enabling secure communication among IoT devices (a limited resource in terms of computational and networking capabilities). Consequently, these devices have become possible targets for conventional Internet attacks (i.e., Denial of Service and man-in-the-middle). To cope with these issues, this study presented an architecture that permits IoT devices to use DTLS with a mutual authentication mechanism. This task is achieved by introducing an IoT Security Support Provider (IoTSSP), which is a third party device that offers two main features: (i) optional handshaking delegation and (ii) transfer of session.

The authors in [54] proposed a scheme to automatically measure quality of security services to be provided in IoT products and devices. Moreover, the study introduced the concept of "Utility Matrix" that measures the needs of users in terms of security and legal necessities. However, this work has not been evaluated in actual application.

A previous study [55] dealt with embedded device security and suggested the embedded security requirements using the concept of trusted computing. In addition, the study elucidated various attacks that resist temper proofing of the embedded devices. The work specifically resolves the security issue related to data at rest.

Despite many advantages of the work, this study only has partially addressed data security problem in IoT. In addition, certain other issues related to the embedded systems adaptability and their dynamic adjustment remained to be addressed.

The IoT needs traceability and visibility of devices during the entire processing lifecycle. Consequently, the protocol has to confirm security concerns, such as non-injection of fake tags and privacy breaching, to solve the issues regarding vulnerabilities of current approaches given that they cannot be applied in a passive RFID tag system. The authors of [56] proposed a tracker protocol for IoT, which enhances the devices' tracking and improves the visibility of devices in IoT. The proposed protocol is proved to be computationally reasonable for use in low-cost RFID tags. However, it requires further improvement to construct a generalized protocol that can accumulate significant context information of a device to guarantee context awareness and enhance control over a device.

Key management is one of the crucial issues in cybersecurity and is more complex in the IoT, wherein many devices are resource-constrained. Consequently, IoT tiny objects either use Pre-shared Key (PSK) mode or Raw Public Key (RPK) mode. These modes both either need a pre-provisioning of wholly likely-trusted users for every separate object before implementation or needs out-of-band validation of RPKs. These modes are not scalable to a huge number of objects. Consequently, the research in [57] aimed to address this issue by proposing a key management architecture called S3K for resource-constrained devices. The proposed S3K is practical for use in resource-constrained devices, and scalable to a huge number of IoT objects. Nevertheless, the implementation and investigation of the feasibility of S3K with further security protocols such as IPsec (Internet Protocol Security)/IKE (Internet Key Exchange) are recommended.

The authors of [58] recommended an IoT architecture to implement vital security and privacy essentials throughout the lifespan of an IoT device. The recommended architectural design in this research is based on the design of diverse security and privacy mechanisms. This study also emphasizes that the suitable application of revocation processes becomes one of the major issues for the entire security and privacy range requirements during the lifespan of smart devices.

Fifth Generation (5G) mobile networks and wireless systems can permit a unified communication among diverse types of things. Nevertheless, 5G heterogeneous networks make the IoT communication susceptible to an eavesdropping attack. In this context, the authors of [59] investigated secure relay communications networks of IoT devices against unsystematically distributed eavesdroppers in view of two scenarios: using single and multiple antennas. This study concluded that suitable establishment of relay transmission can improve throughput rate and increases the secure coverage area.

In the current healthcare systems, the deployment of IoT applications provides advanced and convenient health services for doctors and patients, as they are useful to numerous medical areas with help of Body Sensor Network (BSN) technology. However, the lack of security and privacy insurance solutions hinder the adoption of BSN. In this context, the work in [60] proposed a secure IoT-based healthcare method by means of BSN, called BSN-Care. The proposed scheme is mainly intended to achieve mutual authentication and anonymity property, secure localization property, eliminate forgery attacks, and decrease computation overhead.

4. Taxonomy

Fig. 3 depicts the taxonomy that is devised based on various parameters, including threats, requirements, IEEE standards, deployment levels, and technologies.

4.1. Threats

In the IoT paradigm, numerous threats that include improper or unsafe operation, malicious code modifications, and bypassing of controls and tampering with data integrity are arising. Information exposure or loss can occur in IoT applications. Therefore, protecting private information, keys, and credentials is important [61]. Intellectual property can be compromised given that unprotected IoT applications and devices expose embedded proprietary algorithms that can easily be pirated or analyzed [62]. To prevent exposure of unknown vulnerabilities, it is recommended to make it generally more difficult for the hackers to reverse-engineer, analyze, or exploit the code.

4.2. Requirements

Integrity mechanisms are used to assure consistency and accuracy of data. Hash functions and digital signatures are used to ensure the integrity of data. Moreover, in the IoT environment, data confidentiality also needs to be preserved at the level of storage and on the network path. This refers to protecting information against unauthorized access and disclosure. For instance, an IoT network should not reveal the sensor readings to its neighbors.

Anonymity is the service of hiding data sources. This service also helps in terms of assuring data confidentiality and privacy. In IoT, non-repudiation helps in ensuring that a party to the contract cannot deny the authenticity of their signature on official documents. Finally, freshness guarantees that the data are recent and no old messages have been replayed.

4.3. IEEE standards

The IEEE P1363 standard identifies specifications of asymmetric encryption techniques, such as mathematical fundamental for private key generation. Moreover, it uses the same mathematical bases for the cryptosystem scheme. The IEEE P1619 specifies elements of cryptographic architecture for data protection on block-oriented storage devices and describes the methods, algorithms, and data protection modes. Specification of such a mechanism supports the development of powerful tools for implementation of highly secure and interoperable protection of stored data.

The IEEE P2600 standard addresses the security of peripherals devices, such as copiers and printers. The IEEE 802.1AE standard specifies provision of connectionless user data, confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC clients. IEEE 802.1X enables interoperable user identification, centralized authentication, and key management. User-based identification is based on network access identifier that enables support for roaming access in public spaces through dynamic key management.

4.4. Deployment level

Device or equipment protection is an important issue, and various ways to secure them include adopting best practices, such as restricting external device connection, disabling sensitive devices/endpoints from direct Internet access, ensuring that just specified services are enabled, secure booting (using keys) and secure firmware, applying device authentication in each connection establishment, applying updates and patches on devices' OS, building connection whitelisting, and implementing secure key exchanges [63]. IoT gateway security against intrusions and malware must be preserved by employing different mechanisms, such as filtering and access control lists (gateway or hub).

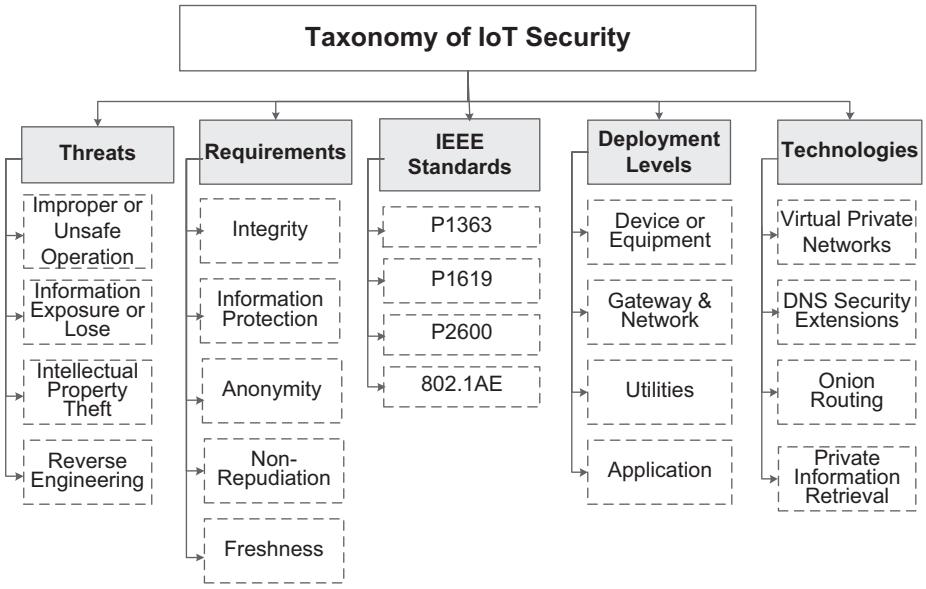

Fig. 3. Taxonomy of IoT security.

Physical and network security are effective solutions in terms of isolating sensitive information. The service provider must obtain and produce assurance certifications [64]. This procedure can be performed in several ways, such as by applying remote access security, allowing only strong authentication for remote access to privileged users like administrators, employing maintenance technicians for logging in securely from remote places to the network, and running secure channels, such as Virtual Private Networks (VPNs) for regular partners accessing the network from outside locations. Wireless communications security ensures secure configurations when communicating across wireless networks and devices/sensors to gateways using encryption and authentication mechanisms.

Cloud security and management need special attention from IT industries. Data generated by IoT devices is mostly stored in the cloud [65]. Therefore, Virtual Machines (VMs) security blocks unauthorized access to VMs, wherein applications need to have strong control mechanisms. Data security within the cloud with appropriate technologies and approved encryption algorithms, including strong key management procedures, need to be properly established. Protection of the web facing cloud instances must be ensured with IDS/IPS, host-based firewalls. In addition, log monitoring especially for privileged users and log management integrating logs from multiple and disparate sources should be handled very carefully.

In the applications development phase, standard secure coding practices must be considered to minimize the risk of application-related attacks, such as preventing session replay, XSS, SQLite, and buffer. To mitigate these attacks, some of the approaches that can be considered as best practices include scanning/fuzz testing the applications (dynamic, static, and hybrid) for vulnerabilities and taking corrective actions to fix them. Moreover, code signing can also be employed to assure customers in terms of authenticity of the software and non-repudiation.

Critical information and files must be monitored and protected against any unauthorized changes or alteration; for example, traffic and configuration files must be monitored against intentional or accidental unwanted changes (i.e., integrity monitoring). Appropriate technologies such as integrity monitoring tools must be applied to prevent or keep the alert on the above concern and must be complemented with strong change approval and review processes.

4.5. Technologies

VPNs are extranets that allow access only to partners, which they promise to keep confidential and have ensured the integrity. However, this technology is not visible for a dynamic global information exchange and not safe for third parties beyond the extranet borders. DNS Security Extensions (DNSSEC), uses asymmetric cryptography for signing resource records to achieve origin authenticity and integrity of received or delivered information.

Onion routing technology encrypts and mixes Internet traffic coming from many senders; for example, data are wrapped in multiple encryption layers, employing the public keys of the onion routers on the transmission path. This process can impede matching an Internet protocol packet to a particular source. However, onion routing increases waiting times, thereby resulting in performance issues.

Private Information Retrieval (PIR) systems are used to hide customer information interest. However, problems of scalability and key management, as well as performance issues, would be encountered in a globally accessible system. Thus, this method can be impractical.

5. Case studies on IoT security

This section discusses different case studies that aim to alert users on how serious IoT devices are vulnerable to exploitation. This section is also a motivation for the need to strengthen the security in the IoT paradigm. Table 2 provides a summary of the case studies.

5.1. Fiat Chrysler

Fiat Chrysler[6] is the world's seventh largest automaker company. In 2015, the company launched a recall of 1.4 million cars that were vulnerable to exploitation. The Jeep Cherokee (2014–2015) was one of fourteen models that made the news for being hacked. Cyber criminals were able to control and access this car remotely due to the weak security, as reported by Wired. The

[6] http://www.pcworld.com/article/2952592/car-tech/chrysler-recalls-14m-cars-that-were-vulnerable-to-remote-hacking.html .

Table 2
Summary of the case study.

Case study	Description	News source	Target	Country	Year
Fiat Chrysler	The company launched a recall of 1.4 million cars which were vulnerable to the exploit	PCWorld	Smart cars	USA	2015
Eurecom	French researchers aim at finding the vulnerabilities in the potential IoT devices	Securing tomorrow	Potential IoT devices	France	–
Interconnected baby monitors	The aim of the hacker was to monitor the movement of the baby with some bad intentions.	CBS News	Baby monitors (Cameras)	USA	2015
Lizard stressor	Six young males down the gaming network.	Alias forensics	Gaming networks (Xbox and PlayStation)	UK	2014

complete hack details were provided in the Wired article, which states that this incident happened on the busy interstate (Highway number 64 near St. Louis, Missouri, USA) under controlled conditions. After some time, it has been revealed that the purpose of this hacking was to determine the loophole in the cars considering that anyone can access and control them remotely and can use them for criminal purposes.

5.2. Eurecom

Eurecom[7] is a graduate school and a research center in France. Researchers working in Eurecom downloaded 32,000 firmware images of IoT devices to understand their security strengths. After analyzing the images, they found 38 vulnerabilities across 123 products. Thus, Eurecom declared that the lack of encryption mechanisms was the major reason of the weak security. Moreover, Eurecom declared that weak security can provide backdoors that can allow unauthorized access. In addition, one weak link can open access to hundreds of thousands of devices on a network with potentially serious consequences.

5.3. Internet-connected baby monitors

In New York, internet-connected baby monitors[8] have gained much attention. The baby monitors allow parents/guardians to keep an eye on their babies. In September 2015, baby monitors were found to lack a security feature, which made them vulnerable even for basic hacking attempts, as stated by CBS news. The possibility of an unknown person monitoring every activity of their babies worried parents who were relying on cameras. In addition, access to a hacked camera can also allow the use of other WiFi-enabled devices, which may provide hackers with financial and other personal information.

5.4. Lizard Stressor

In December 2014, the gaming networks of Microsoft Xbox and Sony PlayStation were down for a few hours. An investigation revealed that a group of hackers named "Lizard Squad"[9] was involved in this incident. They hacked the gaming networks with the help of a tool to which they added their own developed module named "Lizard Stressor". They bought the tool using an alternative payment service, namely, Bitcoin, as stated by the National Crime Agency (NCA). The story was released by KrebsOnSecurity. When the story was released, the service of the Lizard Stressor was hacked by a group named White Hats.

[7] http://www.securingtomorrow.com/blog/knowledge/3-key-security-challenges-internet-things/.
[8] http://www.cbsnews.com/news/baby-monitors-connect-internet-vulnerable-hackers-cybersecurity/ .
[9] http://www.aliasforensics.com/policing-the-people-lizard-stressor/ .

6. New requirements for securing IoT

An IoT framework can be divided into three layers: device, gateway, and service. The security implementation at each of these layer is vital for securing the entire IoT. However, the requirements of security model for each layer are different. Herein, we discuss the security requirements for each layer of the IoT framework.

6.1. Device layer security requirements

The device layer is involved with people, things, and places. To secure the IoT, the security must be implemented in the devices, i.e., the process through which devices perform their operations and interact with users should be secure. The key security requirements in the context of the device layer are secure booting, secure code updates, access control, and device authentication.

6.1.1. Secure booting
When IoT devices power up, the integrity and authenticity of the installed software should be verified to ensure that only the authorized software can run on the device.

6.1.2. Secure code updates
Similar to other devices, IoT devices receive software patches and updates to enhance their functionalities over time. The IoT devices should only install signed patches and software to avoid malicious activities.

6.1.3. Access control
Access control mechanisms are also required to define the limits on the privileges of applications and device components in an IoT environment [66]. The implementation of access control should be compartmentalized so that in case of any compromise, the compromised information can be limited to specific areas of the network.

6.1.4. Device authentication
New devices should be able to authenticate themselves when they are connected to a network. There is a need to design a machine authentication mechanism for IoT devices so that device spoofing can be considerably nullified in an IoT environment.

6.2. Gateway layer security requirements

Gateway layer security is mainly related to the gateway that is deployed between the IoT devices and the Internet. These gateway devices are mainly subject to physical intrusion and have limited functional redundancy. The network designers should ensure that the IoT gateway is protected from malware and intrusions by applying access control lists, filtering, etc. Further, message integrity should be guaranteed by applying hash functions and verification protocols.

Table 3
IoT security startups.

IoT security startups	Objective/Description
ZingBox	To offer security-as-a-service in the IoT paradigm
Visual threat	Strengthening the cybersecurity in smart cars
Bastille network	To secure the enterprise by identifying the airborne threats
Mocana	To provide a software platform for enabling companies to develop, test, and distribute secure IoT devices
TrustWave	To provide security in terms of network, database, endpoints, and application in the IoT Paradigm
Symantec	To protect over one billion IoT devices, from smart television to critical infrastructure and detect advanced threats to the IoT systems through analytics

6.3. Service layer security requirements

The service layer in an IoT framework that deals with the device interactions involved in acquiring data from IoT devices and sending control commands to them. The service layer handles the communication between the device and gateway layer. The interaction should proceed in a way that the changes made by users and devices cannot be refuted. This non-repudiation is achieved by an audit trail of the changes. Therefore, dynamic auditing mechanisms should be implemented to enable the security at the service layer.

7. Open research challenges

This section discusses the research challenges on security in the IoT paradigm. In Table 3, we enlist some of IoT security startups.

7.1. Data integrity

Ensuring data integrity in an IoT environment has become very challenging due to the flood of large data generated by a large number of connected smart devices. Ensuring that the collected data is not compromised is very difficult [67]. In a scenario where utility companies are collecting data from the customers' smart meters in an automated manner, a hacker can send false data from the meter to show an under-reported energy use. Such false data can mislead the utility companies in terms of knowing the exact energy consumption. Several research efforts have been conducted for ensuring data integrity [68]; however, these efforts are in their infancy. In the future, data integrity in IoT should be given considerable attention.

7.2. Lightweight security mechanisms

Devices involved in the IoT have limited resources in terms of CPU power, storage, and battery. Existing encryption mechanisms require high processing power. However, IoT devices have less processing power and antivirus software cannot be installed on all devices, as in a case of IP-addressable light bulbs [69]. The design of lightweight security mechanisms, such as encryption, decryption, and digital signatures, are very challenging because IoT inherits the attributes of WSNs and the Internet, such as limited battery constraints, multi-hop communications, scalability, and global accessibility. Although several research efforts have been conducted to develop lightweight security mechanisms [70–72], these efforts are in early stage of development. Nevertheless, the developments can act as guidelines for researchers working in this domain.

7.3. Lack of security software's upgradability and patchability features

In IoT paradigms, wherein mostly tiny devices are connected to the Internet, security has become a serious concern due to the lack of support of upgradability and patchability of the security software installed on the devices for protection. Companies do not like adding upgradability and patchability features due to the limited resources of these devices, as these processes require a lot of resources from the devices [73]. In this context, several new alternatives would be required that allowing devices to support the upgradability and patchability because virus signatures in databases of the devices must be upgraded. Researchers need to think out of the box in terms of resolving this matter considering the unavailability of the lightweight mechanisms in terms of upgradability in tiny devices.

7.4. Physical protection of trillions of devices

Physical protection of IoT devices is very challenging due to the placement and distribution of voluminous amounts of devices in different areas [74]. The lack of physical security can allow unauthorized users to access devices by using an available Universal Serial Bus (USB) port, thus posing serious problems [75]. Although basic security is present on devices, such as password, manipulating the basic security is not very difficult, as can be demonstrated by the above case studies. Physical protection of trillions of IoT devices seems very challenging because of multiple factors, such as 24 hour protection, tiny devices, and countless individuals are needed to monitor every device to prevent unauthorized physical access.

7.5. Privacy

IoT privacy requires special considerations to prevent exposure of individuals' information. In an IoT environment, when data is collected from multiple connected devices in the form of the segment, sensitive information can be acquired. The leakage of this sensitive information can help competitors in outranking other companies by designing the same product (if leaked information is related to the product) [76]. Ensuring privacy in an IoT environment would become increasingly difficult because if someone's data is compromised once, then he/she may lose trust in the IoT. In [77,78], several privacy-enhancing techniques are discussed for IoT that can act as guidelines for researchers working in the domain.

7.6. Trust

Trust is based on the assumption that nothing will harm the desired entity. Given that an IoT system comprises many heterogeneous networks connected via the Internet, network interaction with other systems of lower security standards can raise trust issues. The current trust system must be upgraded to meet the growth of IoT devices to remain fully feasible [79]. To achieve trust in the IoT, two principles can be considered [80]: first, the device and the linked service must have positive intentions; second, predictability and transparency, i.e., the functional scope of the service provided by devices need to be known and well-defined. Moreover, the IoT system behavior can be checked at any time by independent third parties. Although several solutions have been proposed for evaluating positive interaction and reputation, such

as TripAdvisor [81], Trivago, and HolidayCheck, further research is required.

8. Future research directions

In this section, a few prominent security-related research directions in IoT are provided.

8.1. Application programs security

In IoT, several problems can hinder software applications from providing adequate level of services or even lead to unreliable authentication [82]. In such scenarios, malicious attacks can generate bugs in the application program code, which can easily lead to malfunctioning of the applications or, in worst case, complete failure. The severity of this problem is intensified with the increase in number of devices [83,84]. Some possible attacks on application program in an IoT environment include inability to receive security patches, malicious code attacks, and tampering with node-based applications.

8.1.1. Inability to receive security patches

In certain environments, such as nuclear reactors and chemical factories, if the software bugs in the constantly controlling node are not fixed by updating through software patches, then this case may lead to catastrophic consequences [85].

8.1.2. Malicious code attacks

Several types of attacks that target application programs of IoT exist, such as worms, which could attack home routers, set-top boxes, and security cameras. Moreover, worms can exploit the presence of well-known software vulnerabilities. Such types of code attacks may break into automobile's WiFi to seize the control of the steering wheel, which can result in car damages, injuries, or even deaths.

8.1.3. Tampering with node-based applications

In this type of attack, application vulnerabilities in IoT devices are exploited to install malicious kits [86]. Different types of threats can manipulate a specific environment to induce devices malfunctioning. For example, a tampered weather-monitoring sensor will just display a fixed value of humidity or temperature, while a tampered camera may convey outdated videos and pictures. Device buyers need to consider tamper-resistant issues by purchasing products from reliable manufacturers. Moreover, protecting only specific parts of devices is insufficient.

8.2. Secure data perception

The threats of data perception are at the device level where devices, such as sensors or embedded RFID tags, are prime targets for the attackers. Attackers either replace or modify the device software to achieve their own illegal purposes by exploiting the device [87].

At the data perception level, the threats mainly come from outside entities, typically with respect to data gathering utilities. The main security threats in data perception level are discussed below.

8.2.1. Eavesdropping

Given that communication between IoT devices can be carried out through wireless connection and via the Internet, the devices in the networks can be vulnerable to an eavesdropping attack. For example, in a smart home, a compromised sensor can push notification to the user's phone or peer's sensors and collect sensitive information from them.

8.2.2. Sniffing problem

In this type of attacks, malicious devices/sensors are placed near the targeted sensors of IoT devices to obtain desired information. The availability of IoT devices in a smart environment enables human identification, tracking, and profiling via the physical environment, without their consent.

8.2.3. Data noise

Given that data transmission is done mostly via wireless network, the possibility of a noise-data problem, such as incomplete or false information, is imminent.

8.3. Data transmission security

An IoT network is highly vulnerable to noise data because it carries massive data, leading to frequent network congestion [88]. In data transmission level, the major security threat is related to integrity and authentication. An attacker and malicious devices can compromise the network during data transmission and cause severe problems. The main threats to data transmission in IoT are DoS attack, gateway attack, and unauthorized access.

8.3.1. Denial of service

In this type of attack, IoT devices or servers are the target. Attackers bombard them to stop their services. The DoS attack can appear in different forms, such as machine shutdown or data transfer interruption [89].

8.3.2. Gateway attack

The gateway attack aims to cut-off the connection between the sensing devices and the Internet infrastructure. Such attacks can include routing attacks or DoS attacks targeting the gateway to stop transmission or transmit wrong information via the Internet from or to actuators/sensors [90].

8.3.3. Unauthorized access

Omission may happen from the owner of the sensor or actuator by leaving their devices unsecured. In an IoT environment, devices follow a Machine-to-Machine communication mechanism to transfer and receive data. Consequently, malicious entities may act as authenticated machines to access other devices without having an actual authority.

8.4. Physical protection and availability

In certain scenarios, IoT devices are deployed in remote and insecure spaces. In such situations, the devices become vulnerable to theft and damages. Thus, sensors and actuators must be secure enough to prevent such attacks. Moreover, power efficiency is one of the crucial factors for the availability of the services. Batteries need to be charged frequently, and thus energy-harvesting mechanisms should be utilized to keep the devices active and running.

9. Conclusion

Remarkable advances in smart technologies have paved the way toward a new computing paradigm called the IoT. This study discussed the ransomware attacks and security concerns in IoT. First, we discussed the rise of ransomware attacks and outlined the associated challenges. Second, we investigated, reported, and highlighted the state-of-the-art research efforts on IoT security. Third, a taxonomy is devised by classifying and categorizing the literature. Fourth, a few credible case studies are presented to alert people on the vulnerability of IoT devices to threats. Fifth, we enumerated the requirements for securing IoT. Sixth, several indispensable research challenges are identified and discussed. Seventh, several

prominent research directions are provided. Finally, we conclude that although IoT can facilitate different aspects of people's lives, most IoT devices are vulnerable to ransomware attacks. Therefore, strengthening of the IoT security and mitigation of ransomware attacks should be given great importance to build user trust in the IoT.

Acknowledgement

Imran's work is supported by the Deanship of Scientific Research at King Saud University through Research group No. (RG # 1435-051).

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.comnet.2017.09.003

References

[1] R.J. Tobias, Wireless communication of real-time ultrasound data and control, SPIE Medical Imaging, International Society for Optics and Photonics, 2015. 94190M–94190M
[2] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, M. Guizani, Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges, IEEE Wireless Commun. 23 (5) (2016) 10–16.
[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tut. 17 (4) (2015) 2347–2376.
[4] D. Lin, Y. Tang, F. Labeau, Y. Yao, M. Imran, A.V. Vasilakos, Internet of vehicles for e-health applications: a potential game for optimal network capacity, IEEE Syst. J. PP (99) (2017) 1–9.
[5] C. Perera, A. Zaslavsky, P. Christen, D. Georgakopoulos, Context aware computing for the internet of things: a survey, IEEE Commun. Surv. Tut. 16 (1) (2014) 414–454.
[6] A.M. Ghosh, D. Halder, S.K.A. Hossain, Remote health monitoring system through iot, in: 5th International Conference on Informatics, Electronics and Vision (ICIEV), 2016, pp. 921–926, doi:10.1109/ICIEV.2016.7760135.
[7] N.M. Khoi, S. Saguna, K. Mitra, C. hlund, Irehmo: an efficient iot-based remote health monitoring system for smart regions, in: 17th International Conference on E-health Networking, Application Services (HealthCom), 2015, pp. 563–568, doi:10.1109/HealthCom.2015.7454565.
[8] M. Sanduleac, C.L. Chimirel, M. Eremia, L. Toma, C. Cristian, D. Stanescu, Unleashing smart cities efficient and sustainable energy policies with iot based unbundled smart meters, in: IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), 2016, pp. 112–117, doi:10.1109/EmergiTech.2016.7737321.
[9] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, Wireless Netw. 20 (8) (2014) 2481–2501.
[10] J. Pacheco, S. Satam, S. Hariri, C. Grijalva, H. Berkenbrock, Iot security development framework for building trustworthy smart car services, in: IEEE Conference on Intelligence and Security Informatics (ISI), 2016, pp. 237–242, doi:10.1109/ISI.2016.7745481.
[11] Q. Wen, X. Dong, R. Zhang, Application of dynamic variable cipher security certificate in internet of things, in: Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on, vol. 3, IEEE, 2012, pp. 1062–1066.
[12] G. Ketema, J. Hoebeke, I. Moerman, P. Demeester, L.S. Tao, A.J. Jara, Efficiently observing internet of things resources, in: IEEE International Conference on Green Computing and Communications, 2012, pp. 446–449, doi:10.1109/GreenCom.2012.70.
[13] J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tut. 17 (3) (2015) 1294–1312.
[14] K. Zhao, L. Ge, A survey on the internet of things security, in: Computational Intelligence and Security (CIS), 2013 9th International Conference on, IEEE, 2013, pp. 663–667.
[15] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134.
[16] F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of things security: a survey, J. Netw. Comput. Appl. 88 (2017) 10–28. http://dx.doi.org/10.1016/j.jnca.2017.04.002.
[17] R.H. Weber, Internet of things–new security and privacy challenges, Comput. Law Security Rev. 26 (1) (2010) 23–30.
[18] H. Suo, J. Wan, C. Zou, J. Liu, Security in the internet of things: a review, in: Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3, IEEE, 2012, pp. 648–651.
[19] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279.
[20] J.S. Kumar, D.R. Patel, A survey on internet of things: security and privacy issues, Int. J. Comput. Appl. 90 (11) (2014).
[21] E. Bertino, N. Islam, Botnets and internet of things security, Computer 50 (2) (2017) 76–79.
[22] L. Chen, S. Thombre, K. Jarvinen, E.S. Lohan, A.K. Alen-Savikko, H. Leppakoski, M.Z.H. Bhuiyan, S. Bu-Pasha, G.N. Ferrara, S. Honkala, et al., Robustness, security and privacy in location-based services for future iot: a survey, IEEE Access (2017).
[23] E. Bertino, N. Islam, Botnets and internet of things security, Computer 50 (2017) 76–79.
[24] B. Nassi, A. Shamir, Y. Elovici, Oops!...i think i scanned a malware, arXiv preprint arXiv:1703.07751(2017).
[25] R. Richardson, M. North, Ransomware: evolution, mitigation and prevention, Int. Manage. Rev. 13 (1) (2017) 10.
[26] J. Bugeja, A. Jacobsson, P. Davidsson, An analysis of malicious threat agents for the smart connected home, in: Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on, IEEE, 2017, pp. 557–562.
[27] D. Kavya, Ransomware of things (rot), Fuzzy Syst. 9 (2) (2017) 29–32.
[28] V. Adat, B. Gupta, Security in internet of things: issues, challenges, taxonomy, and architecture, Telecommun. Syst. (2017) 1–19.
[29] C.J. DOrazio, K.-K.R. Choo, L.T. Yang, Data exfiltration from internet of things devices: ios devices as case studies, IEEE Internet Things J. 4 (2) (2017) 524–535.
[30] T. Ring, Connected cars–the next target for hackers, Netw. Security 2015 (11) (2015) 11–16.
[31] K. Cabaj, M. Gregorczyk, W. Mazurczyk, Software-defined networking-based crypto ransomware detection using http traffic characteristics, arXiv preprint arXiv:1611.08294 (2016).
[32] S.-M. Cheng, P.-Y. Chen, C.-C. Lin, H.-C. Hsiao, Traffic-aware patching for cyber security in mobile iot, arXiv preprint arXiv:1703.05400(2017).
[33] S.D. Castilho, E.P. Godoy, T.W. Castilho, F. Salmen, Proposed model to implement high-level information security in internet of things, in: Fog and Mobile Edge Computing (FMEC), 2017 Second International Conference on, IEEE, 2017, pp. 165–170.
[34] C.E. Stewart, A.M. Vasu, E. Keller, Communityguard: a crowdsourced home cyber-security system, in: Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, ACM, 2017, pp. 1–6.
[35] A. Derhab, A. Bouras, M.R. Senouci, M. Imran, Fortifying intrusion detection systems in dynamic ad hoc and wireless sensor networks, Int. J. Distrib. Sens. Netw. 10 (12) (2014) 608162, doi:10.1155/2014/608162.
[36] T. Hayajneh, B.J. Mohd, M. Imran, G. Almashaqbeh, A.V. Vasilakos, Secure authentication for remote patient monitoring with wireless medical sensor networks, Sensors 16 (4) (2016).
[37] A. Akhunzada, E. Ahmed, A. Gani, M.K. Khan, M. Imran, S. Guizani, Securing software defined networks: taxonomy, requirements, and open issues, IEEE Commun. Mag. 53 (4) (2015) 36–44.
[38] Z. Shu, J. Wan, D. Li, J. Lin, A.V. Vasilakos, M. Imran, Security in software-defined networking: threats and countermeasures, Mob. Netw. Appl. 21 (5) (2016) 764–776, doi:10.1007/s11036-016-0676-x.
[39] A. Rizzardi, S. Sicari, D. Miorandi, A. Coen-Porisini, Aups: an open source authenticated publish/subscribe system for the internet of things, Inf. Syst. (2016).
[40] M. Tao, J. Zuo, Z. Liu, A. Castiglione, F. Palmieri, Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes, Fut. Generat. Comput. Syst. (2016).
[41] S.R. Moosavi, T.N. Gia, E. Nigussie, A.M. Rahmani, S. Virtanen, H. Tenhunen, J. Isoaho, End-to-end security scheme for mobility enabled healthcare internet of things, Fut. Generat. Comput. Syst. 64 (2016) 108–124.
[42] H. Bostani, M. Sheikhan, Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach, Comput. Commun. 98 (2017) 52–71.
[43] I. Chatzigiannakis, A. Vitaletti, A. Pyrgelis, A privacy-preserving smart parking system using an iot elliptic curve based security platform, Comput. Commun. (2016).
[44] S. Sicari, A. Rizzardi, D. Miorandi, C. Cappiello, A. Coen-Porisini, A secure and quality-aware prototypical architecture for the internet of things, Inf. Syst. 58 (2016) 43–55.
[45] S. Zawoad, R. Hasan, Faiot: Towards building a forensics aware eco system for the internet of things, in: Services Computing (SCC), 2015 IEEE International Conference on, IEEE, 2015, pp. 279–284.
[46] V.R. Kebande, I. Ray, A generic digital forensic investigation framework for internet of things (iot), in: Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on, IEEE, 2016, pp. 356–362.
[47] S. Perumal, N.M. Norwawi, V. Raman, Internet of things (iot) digital forensic investigation model: top-down forensic approach methodology, in: Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on, IEEE, 2015, pp. 19–23.
[48] Z. Ali, M. Imran, M. Alsulaiman, An automatic digital audio authentication/forensics system, IEEE Access 5 (2017) 2994–3007.
[49] M. Imran, Z. Ali, S.T. Bakhsh, S. Akram, Blind detection of copy-move forgery in digital audio forensics, IEEE Access PP (99) (2017). 1–1
[50] O. Arias, J. Wurm, K. Hoang, Y. Jin, Privacy and security in internet of things and wearable devices, Multi Scale Comput. Syst. IEEE Trans. 1 (2) (2015) 99–109.

[51] B. Vinayaga Sundaram, M. Ramnath, M. Prasanth, J. Varsha Sundaram, Encryption and hash based security in internet of things, in: Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference on, IEEE, 2015, pp. 1–6.
[52] K. Fan, Y. Gong, Z. Du, H. Li, Y. Yang, Rfid secure application revocation for iot in 5g, in: Trustcom/BigDataSE/ISPA, 2015 IEEE, vol. 1, IEEE, 2015, pp. 175–181.
[53] G.L. dos Santos, G. da Cunha Rodrigues, L.Z. Granville, L.M.R. Tarouco, et al., A dtls-based security architecture for the internet of things, in: 2015 IEEE Symposium on Computers and Communication (ISCC), IEEE, 2015, pp. 809–815.
[54] J.-A. Sanchez Alcon, L. Lopez, J.-F. Martinez, P. Castillejo, Automated determination of security services to ensure personal data protection in the internet of things applications, in: Innovative Computing Technology (INTECH), 2013 Third International Conference on, IEEE, 2013, pp. 71–76.
[55] A. Ukil, J. Sen, S. Koilakonda, Embedded security for internet of things, in: Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on, IEEE, 2011, pp. 1–6.
[56] B.R. Ray, M.U. Chowdhury, J.H. Abawajy, Secure object tracking protocol for the internet of things, IEEE Internet Things J. 3 (4) (2016) 544–553.
[57] S. Raza, L. Seitz, D. Sitenkov, G. Selander, S3k: scalable security with symmetric keysdtls key establishment for the internet of things, IEEE Trans. Autom. Sci. Eng. 13 (3) (2016) 1270–1280.
[58] J.L. Hernandez-Ramos, J.B. Bernabé, A. Skarmeta, Army: architecture for a secure and privacy-aware lifecycle of smart objects in the internet of my things, IEEE Commun. Mag. 54 (9) (2016) 28–35.
[59] Q. Xu, P. Ren, H. Song, Q. Du, Security enhancement for iot communications exposed to eavesdroppers with uncertain locations, IEEE Access 4 (2016) 2840–2853.
[60] P. Gope, T. Hwang, Bsn-care: a secure iot-based modern healthcare system using body sensor network, IEEE Sens. J. 16 (5) (2016) 1368–1376.
[61] B. Daghighi, M.L.M. Kiah, S. Iqbal, M.H. Rehman, K. Martin, Host mobility key management in dynamic secure group communication, Wireless Netw. (2017) 1–19.
[62] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, A. Iera, A systemic and cognitive approach for iot security, in: Computing, Networking and Communications (ICNC), 2014 International Conference on, IEEE, 2014, pp. 183–188.
[63] B. Daghighi, M.L.M. Kiah, S. Shamshirband, M.H.-u. Rehman, Toward secure group communication in wireless mobile environments: issues, solutions, and challenges, J. Netw. Comput. Appl. 50 (2015) 1–14.
[64] I. Yaqoob, E. Ahmed, I.A.T. Hashem, A.I.A. Ahmed, A. Gani, M. Imran, M. Guizani, Internet of things architecture: recent advances, taxonomy, requirements, and open challenges, IEEE Wireless Commun. 24 (3) (2017) 10–16.
[65] E. Ahmed, I. Yaqoob, I.A.T. Hashem, I. Khan, A.I.A. Ahmed, M. Imran, A.V. Vasilakos, The role of big data analytics in internet of things, Comput. Netw. (2017). http://dx.doi.org/10.1016/j.comnet.2017.06.013.
[66] R. Giuliano, F. Mazzenga, A. Neri, A.M. Vegni, Security access protocols in iot capillary networks, IEEE Internet Things J. 4 (3) (2017) 645–657.
[67] J.-H. Lee, H. Kim, Security and privacy challenges in the internet of things [security and privacy matters], IEEE Consum. Electron. Mag. 6 (3) (2017) 134–136.
[68] C. Liu, C. Yang, X. Zhang, J. Chen, External integrity verification for outsourced big data in cloud and iot: a big picture, Fut. Generat. Comput. Syst. 49 (2015) 58–67.
[69] M. Gao, Q. Wang, M.T. Arafin, Y. Lyu, G. Qu, Approximate computing for low power and security in the internet of things, Computer 50 (6) (2017) 27–34.
[70] S. Al Salami, J. Baek, K. Salah, E. Damiani, Lightweight encryption for smart home, in: Availability, Reliability and Security (ARES), 2016 11th International Conference on, IEEE, 2016, pp. 382–388.
[71] S. Raza, H. Shafagh, K. Hewage, R. Hummen, T. Voigt, Lithe: lightweight secure coap for the internet of things, Sensors J. IEEE 13 (10) (2013) 3711–3720.
[72] S. Challa, M. Wazid, A.K. Das, N. Kumar, A.G. Reddy, E.-J. Yoon, K.-Y. Yoo, Secure signature-based authenticated key establishment scheme for future iot applications, IEEE Access 5 (2017) 3028–3043.
[73] H. Ko, J. Jin, S.L. Keoh, Secure service virtualization in iot by dynamic service dependency verification, IEEE Internet Things J. 3 (6) (2016) 1006–1014.
[74] C. Cheng, R. Lu, A. Petzoldt, T. Takagi, Securing the internet of things in a quantum world, IEEE Commun. Mag. 55 (2) (2017) 116–120.
[75] E. Al Alkeem, C.Y. Yeun, M.J. Zemerly, Security and privacy framework for ubiquitous healthcare iot devices, in: Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for, IEEE, 2015, pp. 70–75.
[76] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: the road ahead, Comput. Netw. 76 (2015) 146–164.
[77] C. Tian, X. Chen, D. Guo, J. Sun, L. Liu, J. Hong, Analysis and design of security in internet of things, in: 2015 8th International Conference on Biomedical Engineering and Informatics (BMEI), IEEE, 2015, pp. 678–684.
[78] S.N. Premnath, Z.J. Haas, Security and privacy in the internet-of-things under time-and-budget-limited adversary model, IEEE Wireless Commun. Lett. 4 (3) (2015) 277–280.
[79] R. Chen, F. Bao, J. Guo, Trust-based service management for social internet of things systems, IEEE Trans. Depend. Secure Comput. 13 (6) (2016) 684–696.
[80] G. Lize, W. Jingpei, S. Bin, Trust management mechanism for internet of things, China Commun. 11 (2) (2014) 148–156.
[81] F. Buccafurri, G. Lax, S. Nicolazzo, A. Nocera, A model implementing certified reputation and its application to tripadvisor, in: 10th International Conference on Availability, Reliability and Security, 2015, pp. 218–223.
[82] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, R. Kuhn, Learning internet-of-things security "hands-on", IEEE Secur. Priv. 14 (1) (2016) 37–46.
[83] X. Xiaohui, Study on security problems and key technologies of the internet of things, in: Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on, IEEE, 2013, pp. 407–410.
[84] D. Kozlov, J. Veijalainen, Y. Ali, Security and privacy threats in iot architectures, in: Proceedings of the 7th International Conference on Body Area Networks, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 256–262.
[85] D.-Y. Kim, Cyber security issues imposed on nuclear power plants, Ann. Nucl. Energy 65 (2014) 141–143.
[86] H. Ning, H. Liu, L.T. Yang, Cyberentity security in the internet of things, Computer 46 (4) (2013) 46–53.
[87] S. Li, L. Da Xu, S. Zhao, The internet of things: a survey, Inf. Syst. Front. 17 (2) (2015) 243.
[88] H. Bostani, M. Sheikhan, Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach, Comput. Commun. (2016).
[89] R.M. Savola, H. Abie, M. Sihvonen, Towards metrics-driven adaptive security management in e-health iot applications, in: Proceedings of the 7th International Conference on Body Area Networks, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2012, pp. 276–281.
[90] A. Kanuparthi, R. Karri, S. Addepalli, Hardware and embedded security in the context of internet of things, in: Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles, ACM, 2013, pp. 61–64.

Ibrar Yaqoob received his Ph.D. degree in Computer Science from the University of Malaya, Malaysia, in 2017. He earned 550 plus citations, and 50 plus impact factor during his Ph.D. candidature. He worked as a researcher at Centre for Mobile Cloud Computing Research (C4MCCR), University of Malaya. His research experience spans over more than three and half years. He has published a number of research articles in refereed international journals and magazines. His numerous research articles are very famous and among the most downloaded in top journals. His research interests include big data, mobile cloud, the Internet of Things, cloud computing, and wireless networks.

Ejaz Ahmed worked at Centre for Mobile Cloud Computing Research (C4MCCR), University of Malaya, Malaysia. Before that, he has worked as Research Associate in CogNet Research Lab NUST, Pakistan, (December 2009 to September 2012) and in CoReNet, CUST, Pakistan, (January 2008 to December 2009). His research experience spans over more than Eleven years. He is associate editor of *IEEE Communication Magazine, IEEE Access, Elsevier Journal of Network and Computer Applications*, and *KSII TIIS*. He has also served as a Lead Guest Editor/Guest Editor and Chair/Co-chair in international journals and international conferences, respectively. His areas of interest include Mobile Cloud Computing, Mobile Edge Computing, Internet of Things, Cognitive Radio Networks, and Smart Cities. He has successfully published his research work in more than sixty international journals and conferences. He has received several performance awards during his research career.

Muhammad Habib ur Rehman is an assistant professor at COMSATS Institute of IT, Wah Cantt Pakistan, where he works on data stream mining systems for the Internet of Things. His research covers a wide spectrum of application areas, including smart cities, mobile social networks, quantified self, and mobile health. He received a PhD in mobile distributed analytics systems from the Faculty of Computer Science and Information Technology at the University of Malaya, Malaysia.

Abdelmuttlib Ibrahim Abdalla Ahmed received his B.Sc. degree in computer science from OIU, Sudan, and his M.S. degree in computer science from IIUI, Pakistan. He is currently pursuing a Ph.D. degree at the University of Malaya. His research Interest areas include trust and reputation systems, security and digital forensics, Internet of Things, mobile and cloud computing, and vehicular networks.

Mohammed Ali Al-Garadi received the M.Tech. degree in electronic and communication engineering from Jawaharlal Nehru Technological University, Hyderabad, India. He is currently pursuing the Ph.D. degree with the Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia. He has published several articles in academic journals indexed in well reputed databases such as ISI-indexed and Scopus-indexed.

Muhammad Imran is an assistant professor in the College of Computer and Information Science, King Saud University. His research interests include mobile ad hoc and sensor networks, WBANs, IoT, M2M, multihop wireless networks, and fault-tolerant computing. He has published a number of research papers in peer reviewed international journals and conferences. His research is financially supported by several grants. He is serving as a Co-Editor-in-Chief for EAI Transactions on Pervasive Health and Technology. He also serves as an Associate Editor for the Wireless Communication and Mobile Computing Journal (Wiley), the Inderscience International Journal of Autonomous and Adaptive Communications Systems, Wireless Sensor Systems (IET), and the International Journal of Information Technology and Electrical Engineering. He has served/serves as a Guest Editor for IEEE Communications Magazine, IJAACS, and the International Journal of Distributed Sensor Networks. He has been involved in a number of conferences and workshops in various capacities such as a Program Co-Chair, Track Chair/Co-Chair, and Technical Program Committee member. These include IEEE GLOBECOM, ICC, AINA, LCN, IWCMC, IFIP WWIC, and BWCCA. He has received a number of awards such as an Asia Pacific Advanced Network fellowship.

Mohsen Guizani (S'85-M'89-SM'99-F'09) received all of his degrees from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a Professor and the ECE Department Chair at the University of Idaho. He served in a number of academic positions in the USA. His research interests include wireless communications, mobile computing, computer networks, cloud computing, IoT, security, and smart grid. He currently serves on the editorial boards of several international technical journals and the Founder and the Editor-in-Chief of Wireless Communications and Mobile Computing journal (Wiley). He is the author of nine books and more than 400 publications in refereed journals and conferences. He guest edited a number of special issues in IEEE journals and magazines. He also served as a member, Chair, and the General Chair of a number of international conferences. He was selected as the Best Teaching Assistant for two consecutive years at Syracuse University. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker from 2003 to 2005. He is a Fellow of IEEE and a senior member of ACM.