IoT Security Evolution: Challenges and Countermeasures Review

Ali M A Abuagoub

Department of Computer Engineering, College of Computer Engineering and Sciences, Prince Sattam bin Abdulaziz University, Kingdom of Saudi Arabia

Abstract: Internet of Things (IoT) architecture, technologies, applications and security problems have been recently addressed by a number of researchers. Basically, IoT adds internet connectivity to a system of intelligent devices, machines, objects and/or people. Devices are allowed to automatically collect and transmit data over the Internet, which exposes them to serious attacks and threats. This paper provides an intensive review of IoT evolution with primary focusing on security issues together with the proposed countermeasures. Thus, it outlines the IoT security challenges as a future roadmap of research for new researchers in this domain.

Keywords: IoT, security services, security mechanisms, security challenges.

1. Introduction

Today, Internet of Things (IoT) creates an architectural model from a huge amount of intelligent devices and smart tools which are connected with each other through cloud networking. IoT creates an environment for monitoring, collecting data and controlling systems. Recently, a number of projects and proposals on IoT applications have been discussed in the literature. Popular IoT-based smart applications include home, healthcare, industry, city, grid, building, appliances, wearables, car, communications, farming, factory/manufacturing, power/utilities, TV, retail, supply chain and robotics. Thus, the connectivity of IoT devices is steadily increasing, for instance the IoT will reach about 50 billion devices by 2020 as predicted in [1] or it will reach 75 billions by 2025 as reported in [2]. This expectation adds another dimension to the significance of IoT security [3]. For instance, everything like car, fridge, TV, console, and smartphone could be hacked, i.e., anybody can access and take some information and abused it. In IoT-based smart healthcare systems the compromise of a medical network sensor could lead to the loss of patient life(s). IoT-based devices in smart home are typically configured with built-in sensors for real-time monitoring, remote control, safety from intruders, gas/fire alarm, etc., thus the personal information could be leaked in absence of strong security. Security attacks in IoT-based smart industry may damage one of the devices of the IoT infrastructure or interrupt communication between two systems, which may affect other devices or systems and consequently leading to serious problems. Similarly, without secure IoT-based smart grid communications an attacker could spoof the identity of some one's smart meter. Also in IoT-based smart city the attacks or illegal access to information could cause physical disruptions in service availability.

Therefore, this paper reviews a number of recent research works that have been conducted in 2018-2019 with primary focusing on IoT security. In particular, its contributions can be pointed out as follows:

- Reviews of published research works’ findings on IoT security, i.e., it summarizes major outcomes on IoT-based smart applications, security services and new approaches as countermeasures against security attacks.
- Highlights of IoT security challenges as a roadmap for future research directions.

The rest of the paper is organized as follows: Section 2 summarizes major research outcomes in IoT security together with the related application domains, security services, and new approaches as countermeasures that proposed to protect IoT application environments. Section 3 discusses IoT security challenges and open issues as a future roadmap of research for new researchers in this domain. Finally, Section 4 concludes the paper by outlining IoT security applications, countermeasures, services and challenges.

2. Related Research Works

This section summarizes studies that have been recently proposed within the IoT security domain. In particular, it highlights the main IoT-based smart applications for a number of researches as presented in the literature. Figure 1 shows dominant application sectors, which have been recently addressed by various researchers, from IoT security perspectives. These applications include: smart health, smart home, smart industry, smart grid, and smart city. Critical IoT security threats and some proposed solutions were reviewed in [4-6]. Common IoT security architectures, frameworks and platforms were presented in [7-11]. Further analysis of IoT security issues can be found in [3, 12-18].

![Figure 1. IoT security application domains](image-url)
2.1 IoT security services

This subsection presents security services which have been explicitly mentioned in different studies that concern with IoT security. Table 1 records combinations of these security services with their references, whereas Figure 2 indicates that authentication has gained a great consideration within IoT security field, followed by privacy, access control, confidentiality and secure communication, respectively.

Table 1. Common security services

<table>
<thead>
<tr>
<th>Security services</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and trust management</td>
<td>[19 - 34]</td>
</tr>
<tr>
<td>Support of confidentiality and privacy</td>
<td>[35 - 53]</td>
</tr>
<tr>
<td>Control and verification of identification</td>
<td>[1, 54 - 64]</td>
</tr>
<tr>
<td>Security of communication</td>
<td>[65 - 71]</td>
</tr>
<tr>
<td>Prevention and detection</td>
<td>[72 - 82]</td>
</tr>
<tr>
<td>Enhancement of integrity and availability</td>
<td>[83 - 87]</td>
</tr>
</tbody>
</table>

![Figure 2. IoT security services](image)

2.2 Recent security approaches

This section describes new technologies, techniques and concepts which have been recently introduced as new approaches to enhance IoT security, for instance blockchain (BC) in [88 - 96], cloud-fog in [57, 97 - 111], software-define network (SDN) and network-function virtual (NFV) in [112 - 116], physical unclonable function (PUF) in [117 - 119], machine learning (ML) in [115, 118, 120 - 122], lightweight algorithms in [103, 119, 121, 123 - 129], neural network (NN) in [130 - 132], and security fusion as a service (SFaaS) in [73]. Fingerprinting of IoT devices was studied in [133, 134], while authors in [135, 136] proposed solutions for supporting multimedia data in secure IoT environment. Figure 3 shows percentages the most promising approaches as proposed by different researchers to enhance IoT security. Thus, contributions of these approaches as new countermeasures can be ordered, from high to low, as follows: cloud-fog, lightweight algorithms, blockchain, machine learning, SDN/NFV, PUF and NN. The following subsections summarize recent studies on these approaches.

2.2.1 Blockchain-based IoT Security

This subsection highlights some studies that significantly contributed in enhancing IoT security based on blockchain approach. Various designs and implementations of blockchain-based IoT security proposals were introduced in [88, 90, 95, 96]. Recently, few researchers analyzed and discussed some blockchain-based IoT security problems [89, 91 - 94].

2.2.2 IoT Security Based on AI Techniques

Machine learning techniques for IoT security were introduced in [120, 122, 137]. Analysis and implementation of neural network-based IoT security algorithms were presented in [118, 130 - 133]. Biometric and fingerprinting techniques for IoT applications were developed in [121, 134].

2.2.3 Security of Cloud-based IoT Environment

Security and privacy schemes for fog computing-based IoT services were proposed in [101, 105, 107, 110, 138, 139]. Authentication schemes for IoT cloud environment were developed in [98, 100, 104, 106]. In [99, 102, 108, 110, 135, 139] some security schemes were proposed for controlling data access in IoT cloud. Design and implementation of schemes for trusting and securing communication in cloud-based IoT environment can be found in [97, 111].

2.2.4 IoT Security Schemes

This subsection mentions studies which proposed and implemented different lightweight algorithms or schemes for securing IoT systems. A number of schemes or methods have been proposed for minimizing security vulnerabilities and threats in IoT devices [103, 124, 126, 127, 129, 136, 140 - 145], and for resource-constrained IoT platforms [125, 146 - 148]. Performance analyses and evaluations of IoT security solutions were provided in [119, 123, 128, 149 - 153].

![Figure 3. IoT security approaches](image)
2.2.5 IoT Security Using SDN/NFV/PUF

IoT frameworks were designed in [112, 116] using software-define network (SDN) and network-function virtualization (NFV), coupled with existing IoT security approaches. A Physical Unclonable Function (PUF) design based on piezo sensors in IoT devices was proposed as a cybersecurity solution [117]. Security features introduced by SDN/NFV against expected threats were analyzed in [113]. A fog-assisted SDN/IDPS system for securing IoT networks was proposed in [114].

3. Challenges and Future Directions

Although a number of studies have been conducted so far in the literature, to protect IoT applications, still there is a big security hole in IoT environment. IoT security issues and challenges have been analyzed in [12, 13, 16, 18, 21, 23, 29, 68, 115, 150, 153]. In [3, 6, 7, 9, 11, 15 - 17, 20, 37, 100] the authors reviewed recent IoT security research projects, tools, modelers and simulators. Researchers in [26, 28, 34, 65, 106, 142] tried to deploy the available cryptographic algorithms with slight enhancements for IoT security, whereas hardware ciphers have been addressed by authors in [13, 51, 60, 79, 125].

This section provides a number of IoT security challenges, as defined by other researchers, which can be considered as open issues for future research directions.

A. Limitation or constraints of device resources [1, 13, 17, 21, 23, 58, 90, 92, 93, 138, 154]: Manufacturers normally produce most of IoT equipment with low memories, computation capabilities, communication bandwidths and power supplies; on the other hand, classical security algorithms do not work well on IoT devices with limited capabilities [23]. Under tight IoT resource constraints the implementation of blockchain is required as a cost-effective solution [90]. In [13] limited computational resources were tackled by in-memory and near-memory computing. Storage capacity for sensors and actuators is limited, but in [92] the authors argued that the storage size can be increased if blockchain is used with IoT. In healthcare environment devices have less computation capabilities, memories and batteries which is a critical challenge for most of cryptographic solutions [17]. Similarly there are resource limitations for IoT devices and actuators in manufacturing [17]. Resource limitation is a challenge to protect communication in IoT environment [93]. Devices of small sizes with limited energies, memories, and processing capabilities is a real challenge for modeling access control in IoT environment [1]. Thus, deployment of IoT security still faces the biggest challenge of device resource constraints.

B. Heterogeneity and variation of devices, communication standards and information system technologies [17, 20, 23, 64, 92, 93, 100, 153]: IoT systems are diverse and connected over vast network with variation in computing capabilities for running encryption algorithms [92]. In [17] the authors discussed the heterogeneity as a challenge for different applications including: communication and information technologies in smart grids, network protocols and communication media in hospitals, heterogeneous elements in transportation, and heterogeneous smart devices in smart cities. Heterogeneity in cloud-based IoT environment is a challenge [100]. Implementation of a multi-layer security framework is critically needed for IoT environment to cope with various devices [93]. Heterogeneities of IoT devices and communication methods stand against deployment of traditional security solutions in IoT systems [23]. Therefore, heterogeneity of devices still represents a serious challenge to the IoT security.

C. Scalability of devices, application coverage and authentication schemes [1, 17, 23, 57, 64, 92, 100, 153]: This includes scalability, performance and integration of IoT technologies into the existing systems [57]. In [17] the researchers argued that scalability is a serious challenge for securing various IoT applications such as electrical energy consumption growth in smart grids, huge amount of IoT components in smart cities, and IoT systems grow continuously in manufacturing. Scalability in cloud-based IoT environment is a challenge for implementing authentication schemes [100]. In general scalability leads to great difficulties in key management and administration of large amount of devices [23]. Extension of IoT networks in terms of devices and sizes are critically important for designing a model for accessing the IoT system [1]. Thus, scalability of IoT systems remains a challenging to the adoption of effective IoT security mechanisms.

D. Mutual or common authentication [5, 9, 13, 20, 77, 100, 153]: Some researchers tried to protect authentication, however in a typical IoT network some issues still exist [9]. Security of cloud-based IoT authentication schemes against various attacks is a challenge [100]. Public key infrastructure and identity management system are main challenges to fully achieve mutual authentication [5].

E. Trust management [9, 12, 14, 23, 36, 93]: Trust is a very important technique that ensures credibility of dynamic IoT devices [14]. In [12] a gateway was proposed for analyzing and managing the security of the local IoT environment. Many unsuccessful techniques have been proposed for privacy and trust in IoT environment [9]. It is challenging to provide trust management for a great amount of IoT devices [93]. As a result of the absence of central administration for IoT infrastructure the trust management still remains as a significant challenge [23].

F. Standardization of protocols for IoT devices [10, 17, 21, 57, 77, 92]: Formation of an international body is critically needed for enforcing security standards in IoT products [77]. Global standards are required for IoT architecture, device interconnection and service integration [57]. Still there is no technical standards for data storing, communicating and processing [90]. There is no protocol standard for IoT-based SCADA systems in manufacturing [17].

G. Identity verification and integrity of IoT end devices [13, 36, 77, 88, 153]: Diversification of IoT devices resulted in complexity of identity verification [88]. A network identity verification method can be implemented in IoT environment to facilitate the exchange of information between devices [13].

H. Privacy preservation of data and information [9, 10, 13, 14, 17, 20, 21, 23, 36, 37, 57, 77, 100, 138, 153]: Privacy means the information of users that submitted to IoT applications is secure and cannot be accessible by others [9]. There is a lack of lightweight anti-malware solutions for IoT devices [14]. Although a number of researches considered privacy of users and data still there is a need for data privacy at different states including collection, aggregation, sharing and management [77]. Disclosure or
Unauthorized access of home or cloud services can be prevented by developing reliable and well-balanced security frameworks [57]. Technical standards are necessary to be considered for implementing privacy protection mechanisms [10]. It is challenging to protect exchange of user data between local smart meters and remote control center in smart grids [17]. Protecting vehicle drivers from different network attacks is challenge for smart transportation systems [17]. Privacy of data maintained in cloud-based IoT environment is a challenge [100]. Higher privacy requires weaker identity while strong security demands strong identity, thus a tradeoff between privacy and security is an open issue [23].

I. Modeling of IoT network traffic, threats and attacks [3, 37, 75, 90, 115, 153]: Although IoT traffic characterization, filtration and sampling are more complicated they are important to identify malicious nodes and to improve the effectiveness of trust computation [75]. Threat modeling is useful for effective IoT security mitigation [3]. Realistic attack models are necessary to detect cyber criminals that arise from interconnection of smart IoT devices [75]. Consistent formalization of inputs (data and attacks) and outputs (processed data) is needed for ML algorithm to properly work in IoT environment [115].

J. Integration of security mechanisms in IoT protocols and architectures [12, 23, 37, 57, 58]: It includes integration of security mechanisms in existing IoT platforms [12]. Integration of IoT with the open physical world may expose IoT applications to security compromising [23].

K. Access control and privilege management based on locations and rights [1, 5, 13, 21, 36, 57, 90]: Access control is essential specially for IoT devices which may be located on open areas and physically under control of opponents [90]. Contract management plays a centralized role for IoT systems in the future generations [5]. Delegation of authority to IoT devices has to be considered by an access model to enable usability and flexibility of IoT systems [1].

L. Lightweight cryptographic algorithms and effective key management [13, 14, 36, 58, 77]: Resource constraints of IoT devices as a challenge raises the requirements for designing lightweight algorithms to protect data confidentiality and integrity in IoT environment [14] and to support real-time fog-based IoT services [77].

M. Intrusion detection and prevention [20, 21, 36, 88]: It includes abnormal network traffic monitoring [88]. Adoption of intrusion detection and prevention is a challenge to avoid IoT botnet and DDoS attacks [36].

N. Mobility of devices, data management and routing protocols [14, 17, 21, 75, 100, 153]: Although routing protocols are insecure providing protection against routing threats is critically important in IoT environment [14]. Most of healthcare devices are embedded in human bodies, which makes security solutions for mobility is a serious challenge [17]. Security solutions are highly challenging for smart vehicles in high mobility environment [17]. Smart devices often generate huge traffic in modern cities and consequently raise several challenges to the data management [17].

O. Hardware/firmware vulnerabilities and consumer illiteracy with IoT devices [14, 17, 21, 23, 84, 90, 92, 93, 115]: Hardware security of most IoT devices is neglected by manufacturers [14]. IoT technology is still new, which means that its skilled force is very much limited and extremely less when it is integrated with blockchain [92]. Vulnerabilities related to information system technology can be found in smart grids as open systems subjected to a number of attacks [17]. Manufacturing systems including SCADA systems are vulnerable to several type of attacks [17]. Hardware level security is necessary for IoT systems to detect and alleviate vulnerabilities [93]. Breach of IoT security is mostly caused by less security preparation including user mindsets, design and manufacture of devices [23]. Security-by-design approach can be applied to software and hardware development to free systems from vulnerabilities [115].

P. Interoperability of security protocols and interaction between users and policies: Interoperability of security protocols implemented at different layers is a critical challenge to standardize an IoT security mechanism [93]. Interoperability of access policies with multiple users and organizations is a challenge for an access control model [1]. Thus, interoperability and interaction between protocols, users and policies are still challenges to the development of any IoT security model.

Q. Decentralized IoT security based on blockchain as a reliable platform [77, 90, 10, 91, 93, 115]: Further research is needed to adopt blockchain as a reliable and secure IoT platform [77]. Blockchain can reduce hard and soft compromising of physically accessible IoT devices [90]. However, blockchain vulnerabilities are challenges which need providing of effective security mechanisms [93]. Adoption of blockchain for decentralized IoT security can provide a privacy-preserving [115].

Figure 4 reflects the significance of each security challenge as compared with others. These security challenges can be ordered in the following list based on their critical roles in IoT environment:

1. Privacy preservation of data and information.
2. Limitation or constraints of device resources.
3. Hardware/firmware vulnerabilities and consumer illiteracy with IoT devices.
4. Heterogeneity and variation of devices, communication standards and information system technologies.
5. Scalability of devices, application coverage and authentication schemes.
6. Mutual or common authentication.
7. Access control and privilege management based on locations and rights.
8. Trust management.
9. Standardization of protocols for IoT devices and processing.
10. Modeling of IoT network traffic, threats and attacks.
11. Mobility of devices, data management and routing protocols.
12. Decentralization of IoT security based on blockchain as a reliable platform.
13. Identity verification and integrity of IoT end devices.
14. Integration of security mechanisms in IoT protocols and architectures.
15. Lightweight cryptographic algorithms and effective key management.
16. Intrusion detection and prevention.
17. Interoperability of security protocols and interaction between users and policies.
Thus, the above list summarizes the most important IoT security challenges, which can be adopted as open issues for future research directions.

4. Conclusion

Today, Internet of Things (IoT) applications are growing very fast. However, IoT devices are insecure due to a number of reasons including constrained resources, heterogeneity, scalability and lack of standards. This paper has studied a large no of IoT research works with a primary focusing on IoT security. Thus, it presents the main IoT application domains from security perspectives including industry, healthcare, home, city, grid, communications, building, car, factory, TV, supply chain, storehouse, social IoT(S-IoT), and transportation. Also the paper highlights new approaches as countermeasures, proposed by the researchers to enhance IoT security, such as cloud-fog, lightweight algorithms, blockchain, machine learning, SDN/NFV, PUF and NN. In contrast the paper points out the following IoT security services: authentication, privacy, access control, confidentiality and secure communication. Finally, the paper outlines IoT security challenges as a future roadmap of research for new researchers in this domain. Challenges and open issues include privacy, limitation of resources, vulnerabilities, heterogeneity, scalability, mutual authentication, access control, trust management, standardization, modeling, mobility, decentralization, identity verification, integration, lightweight algorithms, intrusion detection and interoperability.

Acknowledgement

This research work was supported by the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University.

References


[104] R. Amin, N. Kumar, G.P. Biswas, R. Iqbal, and V. Changd, A lightweight authentication protocol for IoT-


