Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 191 (2021) 425–430

Procedia Computer Science

www.elsevier.com/locate/procedia

The 7th International Workshop on Cyber Security and Digital Investigation (CSDI)
August 9-12, 2021, Leuven, Belgium

Security Challenges and Requirements for Smart Internet of Things Applications: A Comprehensive Analysis

Noshina Tariq[a], Farrukh Aslam Khan[b,*], Muhammad Asim[c]

[a]*Department of Computer Sciences, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad 44000, Pakistan*
[b]*Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh 11653, Saudi Arabia*
[c]*Department of Computer Science, National University of Computer and Emerging Sciences, Islamabad 44000, Pakistan*

Abstract

Smart homes, smart cities, smart grids, and smart vehicles are a few examples of the Internet of Things (IoT) applications. These applications possess distributed data delivery infrastructures for remote access, storage, distribution, and processing. As a result, the communication amongst such smart objects offers new horizons for applications to improve human well being. However, massive communication within such cyber-physical systems poses a wide variety of security challenges. These security malfunctions may disturb the entire applications/systems and lead to lethal consequences. Therefore, trust and security are major prerequisites in advanced IoT applications. To this end, there is a dire need to understand the key security challenges within smart IoT applications, such as e-health, agriculture, and energy sectors. Therefore, this paper provides and discusses major security challenges and requirements of smart IoT applications in order to enhance their security.

Keywords: Internet of Things; Smart Applications; Cyber Security; Security Requirements, Internet of Energy, e-Health, Smart Agriculture

1. Introduction

In our daily routine, various kinds of innovative devices have become ”smart” and pervasive. Since the Internet of Things (IoT) has grown tremendously, smart things (i.e., devices) can communicate and interact with people, devices, and the environment to accomplish a plethora of tasks. IoT has become very popular in every potential application sector, ranging from basic domestic electronics to massive industrial units [1]. In the accumulation and transmission of data, security and safety of resources, devices, and data must be ensured. However, due to their low power consumption and lack of embedded security, IoT devices provide a channel for attackers to penetrate residential and business networks [2]. There have recently been many efforts to exploit the security of connected devices. Attackers may

* Farrukh Aslam Khan. Tel.: +966-11-4697341 ; fax: +966-11-4695237.
E-mail address: fakhan@ksu.edu.sa

1877-0509
10.1016/j.procs.2021.07.053

target them to transmit harmful code or activate a malware message planted on a device, collect sensitive personal information across devices, or even extract encrypted information from device encryption and decryption keys. Mirai malware attack infected approximately 2.5 million inter-connected devices in 2016 [3]. Following that, a huge number of IoT devices were hit by Reaper, Star Wars, WireX, Satori, Hajime, and Neris botnet attacks [4].

In contrast to other conventional network systems, most IoT applications' sensory nodes are allocated in regions unaccompanied by physical inspection with limited computing, bandwidth, and storage resources, leading to major security concerns for the IoT. Since these devices have limited resources, the conventional security countermeasures (such as encryption) are not applicable in IoT-based networks [5]. Additionally, the features of IoT devices also make the security design tougher than ever, such as increased privacy concerns, scalability, preference for services than security, cost-effective architecture, heterogeneity of devices, resource restrictions, and rigorous management of the trust [6]. Due to the absence of secure IoT architecture, it is frequently easier to compromise IoT applications than to exploit conventional devices; for instance, hacking of a baby monitor at a remote location, financial violations in smart homes, smart plugs, DVRs, and smart cameras [7].

This paper attempts to highlight the security challenges and requirements of smart IoT applications. It intends to analyze the security concerns of IoT applications for improved security solutions. Various attacks on IoT applications are also discussed. The following are the main contributions of this work:

1. A discussion on cyber security in the IoT applications is provided featuring security requirements of smart IoT applications.
2. The goals of securing IoT applications are highlighted, emphasizing various limiting factors in their security and the impact of a security breach in the respective area.
3. Major attacks on IoT applications and their consequences are also discussed in this paper.

The rest of the paper is organized as follows: Section 2 briefs about cyber security and the Internet of Things focusing on major security features. Section 3 highlights crucial security requirement analysis in different IoT applications. Finally, the paper is concluded in Section 4.

2. Cyber Security and the Internet of Things

Attacks in the IoT system could be perceived or classified from various views based on whether the attacks are active or passive by nature. Additionally, these can be perceived as whether the attack is from inside the system (i.e., an internal attack, such as a black hole) or from exterior areas of the system (i.e., an external attack, such as Denial-of-Service (DoS) attack) [8]. In either case, the confidentiality and privacy of information must be preserved. Information confidentiality denotes a fundamental issue in IoT applications, where the user can access the information and the sanctioned device. It necessitates tackling two primary features: firstly, validation and identity verification mechanism, and secondly, entry restriction and sanction procedure. Verification of the identity of the IoT network for cloud or fog-based services is the authentication of a legitimate IoT device. IoT applications validate their identity in order to use cloud or fog services securely [9]. Another challenging problem with real-time applications is user confidentiality. Privacy is another prime concern in all-pervasive IoT applications, where objects are interlinked.

As mentioned earlier, the information is transmitted over the web; therefore, providing privacy is a sensitive topic as discussed in various existing and on-going research. Hence, information accumulation, information exchange and administration, and information safety concerns stay open research topics to be explored. Breaching confidential data, for instance, a specific location or other information using cloud/fog service, IoT, wireless, or cellular networks, are consumers' crucial concerns. Correspondingly, trust plays a prime part in initiating safe transmission when many entities transmit in an undetermined IoT territory. Two aspects of trust must be regarded in IoT: trust in the communication between things, and trust in the network from the users' point of view [10]. Since most sensor node-based IoT devices possess limited resources, the main concern is to conserve them. However, executing security mechanisms in IoT applications is still a demanding task. In a nutshell, for effective IoT safety and security, one should be mindful of the basic safety targets such as confidentiality, availability, accountability, auditing, and non-repudiation. Major attacks/threats on IoT applications have been put forward in Table 1 along with the potential consequences.

Table 1. Attacks on IoT applications and their consequences.

Attack	Consequences
Analysis of network traffic	Data and information leakage in transit and breached privacy of data and users.
Routing attacks	Data leakage, packet loss, delayed receiving, and degraded network performance.
Spoofing of RFID/sensors	Manipulation of packets and data modification.
Unauthorized access	Modification in data and information.
Selective forwarding attacks	Data leakage, packet loss, delayed receiving, and message overhead.
Internal attacks (e.g., blackhole, greyhole, Sybil)	Degraded network performance, data stealth and fabrication, minimized network lifetime.
External attacks	Degraded network performance, data leakage, system failure.
Man-in-the-Middle Attack	Compromised data and user privacy and confidentiality.
Denial-of-Service Attack	System crash, resource unavailability, network flooding.
Malware attacks (e.g., worms, adware, virus, spyware, trojan horses)	Resource consumption, data theft, data fabrication, data infection, and privacy breach.

3. Security Requirements of Smart IoT Applications

In any area of existence, IoT applications can be used. These smart networks work remotely and use wireless communication with other IoT nodes [11]. However, the media is prone to different network threats, such as eavesdropping. The wireless network is a class of networks that has high resource restrictions (i.e., power, memory, processing) with interconnected devices defined by high error rates and low data rates, and instability in the communication links. The power usage, energy, and computational capacity of conventional cryptography and secure security protocols result in network congestion and low confidence convergence. Current technologies seem to be ineffective in the IoT ecosystem regarding authentication and defence from internal threats. In addition, the effect of dynamicity that is crucial in situations, such as smart transportation, smart homes, and smart health, are not included in existing safety measures. Hackers from different network interfaces may also easily attack interconnecting devices, such as gateways or field devices. Therefore, all intelligent devices must be protected with robust protection mechanisms. An intrusion on a single system could cause the whole network to fail [12].

Therefore, secrecy, reliability, and accessibility are the prime protection attributes in terms of data storage. Confidentiality guarantees that adversaries cannot view data without authentication or authorization. Integrity leads to data accuracy and completeness. Availability promises that authenticated users can be provided with network services and data as needed. If attackers compromise these characteristics in IoT applications, the effect may be catastrophic [13]. The absence of standardised and legal protection is an important factor in the safety of IoT applications. IoT devices are mostly produced by various suppliers, and there are no industry-approved guidelines for their safety. Since there are several IoT protection mechanisms, no standard architecture has been agreed upon. Big enterprises and business groups can have exact requirements, although some markets are subject to industry leaders' patented and incompatible standards. The range of these requirements tends to make it troublesome to protect networks making it difficult to guarantee interoperability. Moreover, accredited establishments could exploit smart applications by false data injections or aggressive manipulation of data. Furthermore, IoT applications, including wireless sensor networks, smart healthcare, and smart city applications, are primarily used as Low-Power and Lossy Networks (LLNs) that are well-known for their constrained nature [14]. The key limiting factors in such applications are highlighted in Table 2.

3.1. Smart home

The safety and security of data collected by home sensors and detectors is a significant concern. Data is stored at various locations, such as centralized servers in the cloud, fog, and local networks. The findings of the analysis by cyber security researchers identifying vulnerabilities in the IoT networks (e.g., a smart city) often result in the hacking of consumer data, thus jeopardising the customer's security and safety. [15], [16]. 92.1% of the world's population relies on 10% of those connected to the Internet, according to the World Economic Forum [17]. For example, people may speak about the equipment (e.g., sensors or microphones) or assign some instruction that they want in-house equipment (e.g., coolers, air conditioners, smart TV) to be run. Only authorized operators of IoT mainly work in a smart home domain to monitor all smart things in the home [18]. Anonymity, self-resistance, identity, and reliability must be addressed concerning safety to protect a smart home from theft and infringement. IoT system passwords must remain confidential and may be changed frequently. The IoT network needs to avoid predicting or warning

Table 2. Security limiting factors in IoT applications.

Security feature	Description
Resource-constrained nature	The memory, computation, and energy level of the sensory nodes are restricted.
Energy-level	Many IoT devices, such as RFID tags have a limited battery life (i.e., seldom recharged).
Diversified networks	It is seen that IoT sensory nodes would be able to communicate with heterogeneous devices linked to the Internet through wireless and wired connections.
Mobility	Some IoT applications are mobile, such as smart vehicular systems and smart healthcare applications. Hence, it is pretty challenging to provide security when transmitting data.
Open wireless medium	Almost all the IoT nodes transmit data availing the IEEE 802.15.4 wireless means, which is free to access and greatly unsafe.
Scalable and distributive deployment	IoT devices are arbitrarily stationed in huge geographical areas and can mainly be left neglected through all their span of life (based on their utilization and application).
Inaccessibility of intermediate nodes	The data is sent in a multi-hop fashion without knowing the intermediate nodes.

about irregular measures. Self-resistance allows the home to be protected with alarming sound to warn of a possible infringement.

3.2. Smart cities

In smart city applications, the information is transmitted and used by various groups interacting and acquiring access to the data. From the developers of smart sensors to the city's transport administration including consumers interacting with the smart city (via smart mobiles, for instance), each entity distinctively utilizes and manages information, which might jeopardize an individual's privacy [19]. Additionally, as every smart city partner would have diverse prime concerns, differences exist amongst diverse partners' privacy regulations. Therefore, secure connections and authentication are equally significant in smart cities [20]. It may be facilitated by digital forensic analysis across linked devices and may implement and maintain edge privacy and security controls for data gathering, transit, and analysis. The system should be equipped with lightweight cryptography regulations and algorithms for resource-constrained IoT devices and applications, such as WSNs.

3.3. Smart health

The IoT concept incorporates authentication, automated data aggregation, and discrimination of fetched/processed data in the medical field. In general, health services in IoT applications handle patient data, which is vulnerable to a data leak if appropriate preventive controls are not taken [21]. Because the devices in such applications have poor computation and memory capabilities, additional security measures cannot be practised. Additionally, since these applications are dynamic (i.e., they may need connectivity to a public network, such as a workplace or home), they are more susceptible to manipulation and forging attacks. The myriad of IoT devices has further complicated developing a dynamic and reliable security system capable of defending against all conceivable security challenges [22]. For example, the historical data of a patient's health status is secret, necessitating a protection mechanism to reduce the information from being transmitted to an unauthorized organization. By working in this way, no one is able to see or edit the data, pass a patient's health record that contains errors, or prevent a physician from making a mistake during patient treatment. Without a safety protocol in place, the medical practitioner may administer the incorrect drug or provide inappropriate nursing care to their patients. For instance, altering a blood examination result may exacerbate the patient's condition by supplying incompatible blood throughout the transfusion procedure.

3.4. Smart agriculture and environment

Agriculture and the environment can be managed using smart networking/devices, as they can furnish several principle characteristics: i) the potential of gathering data from surroundings, ii) the feasibility of transferring instructions and feedback distantly, along with the real-time mode, and iii) the accessibility of the equipment to manage the significant quantity of information. To list a few important examples: wireless loops utilized to collect data from sensors, RFID stationed to examine the position of a device/equipment and the IoT state to access and manage devices or

objects [23]. Hence, all the data collected, interchanged, and reserved well inside smart systems might cause serious concerns regarding safety and privacy. For example, complex private data might be utilized for widespread profiling or social engineering attacks. Besides this, the inappropriate use of devices, unfair practices, and substandard knowledge of tools might cause serious safety infringements. For instance, smart mobiles are frequently utilized to manage diverse groups of smart systems (e.g., buildings) and malignant applications might attack the located equipment of the consumers' system.

Cloud of Things (CoT)-based technologies play an increasingly critical role in smart agriculture. However, any new user or sophisticated industrial technology, such as CoT-based technologies together with irrigation systems will go through many phases before becoming a standard [24]. Unfortunately, these technologies are prone to added attack trajectory (e.g., firmware, applications, and hardware based on CoT) that might be (distantly) misused by adversaries, primarily in the course of initial phases and in contrast to conventional/distant irrigation systems. The characteristics of source-restraint nodes in CoT-based networks and their mutual reliance need a safety procedure for re-evaluation of CoT technology. For instance, restrictions in the computational ability of the fundamental hardware (for instance, low energy and reduced processing abilities) denote that prevailing safety mechanisms (that usually need complicated cryptography calculations like modular-exponentiation operation) might be a misfit-for-use. The current tough task in creating trivial safety mechanisms for CoT-based technologies is to hit the appropriate equilibrium between securing a most favorable safety affirmation without suffering additional computational expenses and energy expenditure mainly on source-restrained nodes.

3.5. Smart energy

With the assistance of Information and Communications Technology (ICT), smart energy users can use and manage objectives based on the information obtained from distant services. Due to the collection, receiving, and exchange of data, smart grids essentially need protection against privacy breaches. If an attack succeeds, it can lead to cascading consequences [25] such as degradation of public utilities including telecommunication companies, energy delivery, and other associated services [26]. As a consequence, data or operation impairment may be the result of the malfunction. These attacks are mostly caused by unauthorised entry to the network resulting in the database being changed or destroyed. As smart grids stretch geographically, they might provide an interaction track between distant locations and the administrative hub. These abilities might also unlock the attackers' portal leading to interference to the regular performance. Unfortunately, cyber attackers can access power network transmission systems remotely to disrupt a smart energy infrastructure. It might cause severe and detrimental outcomes. In conclusion, the cyber safety of smart grids has been acknowledged as a crucial concern. It has to be noted that Ukraine power system had witnessed a massive power outage that occurred in December 2015 due to a malware attack. Nearly 225,000 users were troubled by this outage [27]. The human-machine interface was unlawfully seized and utilized by the attackers to distantly open a plethora of circuit crashes that straightly slashed power to the users. In addition, the restoration process was made complex as the DoS attack undermined the transmission system in a way that the call center could not take the incoming calls from the users.

4. Conclusion

With the proliferation of the IoT devices, the engineering industries and the research community have focused on a number of security weaknesses, including vulnerabilities of connected devices and data in transit. Additionally, the widespread use of IoT has established its applications as distinct study subjects. The coupling of physical and cyber worlds has exacerbated the vulnerabilities inherent in all IoT applications and systems. Given the widespread use of IoT, there is an urgent need for proactive threat mitigation and the development of strong security solutions using cutting-edge technology. The major setback in securing smart IoT applications is their restrained nature, which must be addressed while proposing promising security measures. In addition, the data is transferred further for processing and analysis, which calls for data privacy and secure transmission. This paper discussed crucial security challenges of IoT applications targeting smart cities, smart healthcare, smart agriculture, etc. It also discussed the security requirements and limiting factors in such applications considering the existing state-of-the-art research. In future, we aim to extend

this analysis to a Systematic Literature Review to dig down further details of cyber threats and their mitigation in IoT applications.

References

[1] N. Tariq, M. Asim, F. A. Khan, T. Baker, U. Khalid, A. Derhab, A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in internet of things, Sensors 21 (1) (2021) 23.

[2] R. Chawla, et al., Study of security threats and challenges in internet of things systems, Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12 (2) (2021) 1154–1166.

[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on iot security: application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.

[4] I. A. SALEH, M. A. KAMAL, L. M. IBRAHIM, Using monkey optimization algorithm to detect neris botnet, Journal of Engineering Science and Technology 16 (1) (2021) 152–164.

[5] N. Tariq, A. Qamar, M. Asim, F. A. Khan, Blockchain and smart healthcare security: A survey, Procedia Computer Science 175 (2020) 615–620.

[6] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, I. Ghafir, The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey, Sensors 19 (8) (2019) 1788.

[7] K. Sha, W. Wei, T. A. Yang, Z. Wang, W. Shi, On security challenges and open issues in internet of things, Future Generation Computer Systems 83 (2018) 326–337.

[8] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, T. Baker, A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered iot, Journal of Parallel and Distributed Computing 134 (2019) 198–206.

[9] N. Abbas, M. Asim, N. Tariq, T. Baker, S. Abbas, A Mechanism for Securing IoT-enabled Applications at the Fog Layer, Journal of Sensor and Actuator Networks 8 (1) (2019).

[10] A. Ahmed, R. Latif, S. Latif, H. Abbas, F. A. Khan, Malicious insiders attack in iot based multi-cloud e-healthcare environment: A systematic literature review, Multimedia Tools and Applications 77 (17) (2018) 21947–21965.

[11] T. ul Hassan, M. Asim, T. Baker, J. Hassan, N. Tariq, Ctrust-rpl: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based internet of things applications, Transactions on Emerging Telecommunications Technologies 32 (3) (2021) e4224.

[12] Z. A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, et al., Future challenges for smart cities: Cyber-security and digital forensics, Digital Investigation 22 (2017) 3–13.

[13] A. Ali, F. A. Khan, A broadcast-based key agreement scheme using set reconciliation for wireless body area networks, Journal of medical systems 38 (5) (2014) 1–12.

[14] S. Shukla, Reliable critical nodes detection for internet of things (iot), Wireless Networks 27 (4) (2021) 2931–2946.

[15] K. Govindan, P. Mohapatra, Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey, IEEE communications survey and tutorials 14 (2012).

[16] F. R. D. Kreutz, P. Verissimo, Towards secure and Dependable Software-Defined Networks, Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw. (2013).

[17] M. Nawir, A. Amir, N. Yaakob, O. B. Lynn, Internet of things (iot): Taxonomy of security attacks, in: 2016 3rd International Conference on Electronic Design (ICED), IEEE, 2016, pp. 321–326.

[18] M. Tariq, H. Majeed, M. O. Beg, F. A. Khan, A. Derhab, Accurate detection of sitting posture activities in a secure iot based assisted living environment, Future Generation Computer Systems 92 (2019) 745–757.

[19] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, J. Peng, Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in iot-based smart cities, Information Processing & Management 58 (4) (2021) 102549.

[20] M. Daneva, B. Lazarov, Requirements for smart cities: Results from a systematic review of literature, in: 2018 12th International Conference on Research Challenges in Information Science (RCIS), IEEE, 2018, pp. 1–6.

[21] A. Hussain, T. Ali, F. Althobiani, U. Draz, M. Irfan, S. Yasin, S. Shafiq, Z. Safdar, A. Glowacz, G. Nowakowski, et al., Security framework for iot based real-time health applications, Electronics 10 (6) (2021) 719.

[22] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, M. K. Ganapathiraju, Everything you wanted to know about smart health care: Evaluating the different technologies and components of the internet of things for better health, IEEE Consumer Electronics Magazine 7 (1) (2017) 18–28.

[23] H. N. Saha, R. Roy, M. Chakraborty, C. Sarkar, Iot-enabled agricultural system application, challenges and security issues, Agricultural Informatics: Automation Using the IoT and Machine Learning (2021) 223–247.

[24] M. Roopaei, P. Rad, K.-K. R. Choo, Cloud of things in smart agriculture: Intelligent irrigation monitoring by thermal imaging, IEEE Cloud computing 4 (1) (2017) 10–15.

[25] N. Tariq, M. Asim, F. A. Khan, Securing scada-based critical infrastructures: Challenges and open issues, Procedia Computer Science 155 (2019) 612–617.

[26] D. S. Terzi, B. Arslan, S. Sagiroglu, Smart grid security evaluation with a big data use case, in: 2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018), IEEE, 2018, pp. 1–6.

[27] A. Qiu, Z. Ding, S. Wang, A descriptor system design framework for false data injection attack toward power systems, Electric Power Systems Research 192 (2021) 106932.