Scientific Research Publishing

Journal of Computer and Communications, 2023, 11, 76-83
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Security Threads and IoT Security

Dona Alkunidry, Shahad Alhuwaysi, Rawan Alharbi

Information Technology (Network Administration and Security), Jeddah, Saudi Arabia
Email: dalkunidry@stu.kau.edu.sa, Salhoaissi@stu.kau.edu.sa, Ralharbi0471@stu.kau.edu.sa

How to cite this paper: Alkunidry, D., Alhuwaysi, S. and Alharbi, R. (2023) Security Threads and IoT Security. *Journal of Computer and Communications*, **11**, 76-83.
https://doi.org/10.4236/jcc.2023.119005

Received: August 4, 2023
Accepted: September 25, 2023
Published: September 28, 2023

Abstract

One of the technologies that have attracted the most attention recently across a variety of applications is the Internet of Things (IoT). The Internet of Things (IoT) is the combination of sensor, embedded computing, and communication technologies. The goal of the Internet of Things is to provide seamless services to anything, everywhere, at any time. The internet of things (IoT) technologies plays a vital role everywhere after the internet and information and communication technology, ushering in the fourth disruptive technology revolution (ICT). For real-time processing, communication, and monitoring, the smart items are linked together through wired or wireless connections. Implementing the IoT system presents security and privacy challenges since IoT devices are incompatible with current security standards based on tradition. This paper discusses IoT security strands, mitigation strategies, and privacy issues. This study's major objective is to get more knowledge about security threats, mitigation techniques, and privacy concerns in IoT devices. The authors also mentioned a few cutting-edge technologies that can address general security problems. This study's major objectives are to find research gaps in IoT security and match solution paradigms. The advent and rapid growth of the Internet of Things (IoT), which offers innumerable benefits, facilities, and applications including smart grids, smart homes, smart cities, and intelligent transportation systems (ITS), have an impact on everyone's life. However, the deployment and use of sensing devices exposes IoT-based systems and applications to many security flaws and attacks. Furthermore, the lack of standardization brought on by the diversity of devices and technologies makes integrating security in the IoT a severe problem. The purpose of this review paper is to highlight the numerous security threats, challenges, and attacks that IoT-enabled applications face.

Keywords

Internet of Things, Security Threads, Mitigation Measures, Privacy

1. Introduction

The Internet of Things (IoT) describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. It is a network of various linked devices, people, services, and things that may communicate and share information in order to accomplish a shared objective across a variety of domains and applications. There are various application areas for IoT, including transportation, agriculture, healthcare, and the generation and distribution of energy. IoT devices use an identity management strategy to distinguish themselves from a group of related and distinct devices. An IP address can similarly establish a region in the Internet of Things, but each entity within an area has its own unique address. By enabling the intelligent devices all around us to perform routine tasks, the Internet of Things (IoT) aims to fundamentally alter the way we live today. The words that are used in conjunction to IoT include "smart" homes, "smart cities," "smart infrastructure," etc. IoT applications can be found in a wide variety of environments, from private homes to commercial buildings [1].

IoT devices can be divided into two main groups: Edge devices and gateway devices. A low-power, low-resource device with sensors and/or actuators is called an edge device. Typically, edge devices provide a particular function, such as gathering temperature data and transmitting it to a gateway. Compared to edge devices, gateway devices often have more resources. The task of connecting edge devices to the Internet and collecting data from edge devices is carried out by a gateway device.

Security is essential due to the vast number of devices, the volume of data they exchange, and the influence they will have on our daily lives [2].

The main goal of this study is to learn more about security threads, mitigation strategies, and privacy issues in IoT systems. A few cutting-edge technologies that can address systemic security issues were also mentioned by the writers. The main goal of this study is to identify research gaps and match solution paradigms in IoT security.

The implementation of security within an IoT network is full of challenges. IoT systems are heterogeneous, to initiate. Different device types, communication channels, types of data being transported and shared, device resource levels, and system settings exist. The difficulty of effectively securing IoT is exacerbated by each unique component. The sheer quantity of devices that are interconnected presents a second difficulty. A new study area of attention when taking into account nominal function, robustness, and security is made possible by the billions of connected devices [3].

The Internet of Things (IoT) is a prime example of sustainable growth. It has aided in the creation of intelligent systems, industrialization, and modern living standards. One of the fundamental building blocks for comprehending the

widespread adoption of IoT is IoT architecture. For every technological infrastructure, security concerns are extremely important. IoT security challenges are varied because it includes a variety of devices. Confidentiality, integrity, and availability may be compromised as a result of various security assaults [4].

2. Structure of the IoT

The Internet of Things (IoT) is a technology with a wide range of applications (**Figure 1**). One such area is healthcare, which urgently needs to use technology to enable millions of people to take advantage of the attention and accessibility of healthcare specialists [5].

3. IoT Security Threads

In order to ensure confidentiality, authentication, and integrity, IoT requires security measures at each of the three layers: the physical layer for data collection, the network layer for routing, and the application layer for data transmission.

- **Authentication Measures**

A mutual authentication system for IoT between platforms and terminal nodes was introduced. Zhao, G., *et al.* [6] focused on the mutual identity authentication between the platform and terminal node. According to the proposed

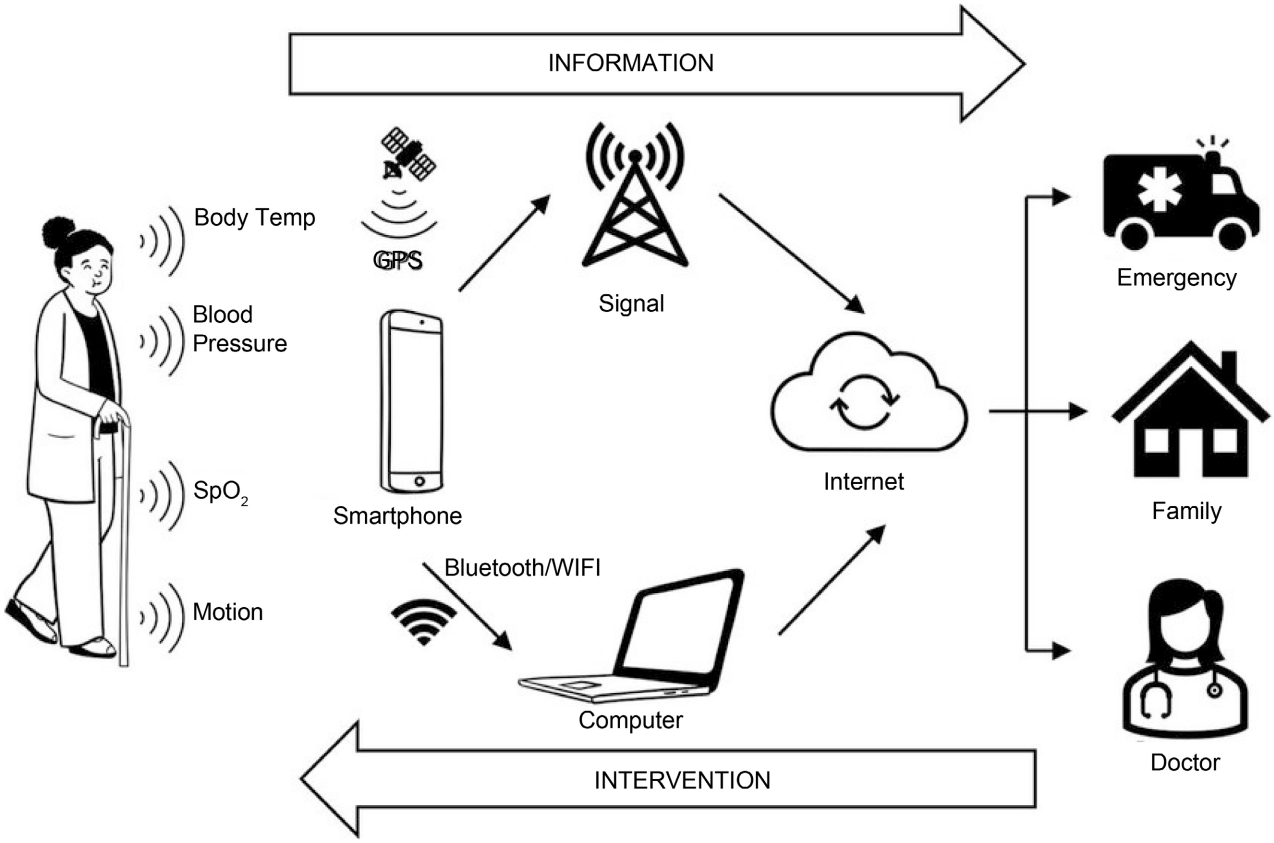

Figure 1. Structure of the IoT.

scheme, mutual authentication between terminal nodes can be easily inferred, and in the case of a large number of terminal nodes, we can use the hierarchical processing method in accordance with the platform's capabilities. On the one hand, the IOT's security can be enhanced by using the characteristics of feature extraction, while on the other hand, less data can be communicated through wireless networks. Feature extraction is a technique often used in pattern recognition and image processing; it can transform the input data into the set of features in order to perform the desired task using this reduced representation instead of the full-size input. Some necessary components are initially transferred to the platform and terminal node during the initialization process.

Mahalle, *et al.* [7] introduced an Identity Authentication and Capability based Access Control (IACAC) for the IoT to address these functionalities. In order to enable mutual identity establishing in the IoT, this research aims to close the gap for an integrated protocol with both authentication and access control capabilities. The suggested architecture employs a public key method and is compatible with existing access technologies like Bluetooth, 4G, WiMax, and Wi-Fi as well as the lightweight, mobile, distributed, and computationally constrained characteristics of IoT devices. By including a timestamp in the authentication message between the devices also known as the Message Authentication Code (MAC), it guards against man-in-the-middle attacks. The algorithm presented in [8] research addresses both authentication and access control.

- **Federated Architecture**

Controlling the security of algorithms in the IoT is challenging since there aren't any global policies and standards to regulate their design and implementation. To address the heterogeneity of multiple devices, software, and protocols, it is crucial for IoT design to have a federated architecture with an internal autonomous or centralized unit. A design was made in [8] to put out a framework for critical infrastructures called Secure Mediation GateWay (SMGW) (Illustrated in **Figure 2**). This method is an abstraction of IoT since it can be applied to any type of distributed infrastructure, regardless of how dissimilar it is from IoT in nature and operation. Whether it is a telecommunication, electricity, or water distribution node, SMGW can find all the pertinent distributed information from various nodes, overcome the heterogeneity of heterogeneous nodes, and exchange all the messages and information over the untrusted Internet network.

- **Trust Establishment**

R Since IoT devices can physically change hands, trust between the two owners is necessary for a seamless transfer of the IoT device's access control and permissions. By developing an item-level access-control framework, Xie. Y., & Wang. D. [9] introduce the idea of mutual trust for inter-system security in the IoT. From the IoT creation phase through to its operation and transmission phase, trust is established. The creation key and the token are the two processes that build this trust. A creation key is given to every newly formed device by an

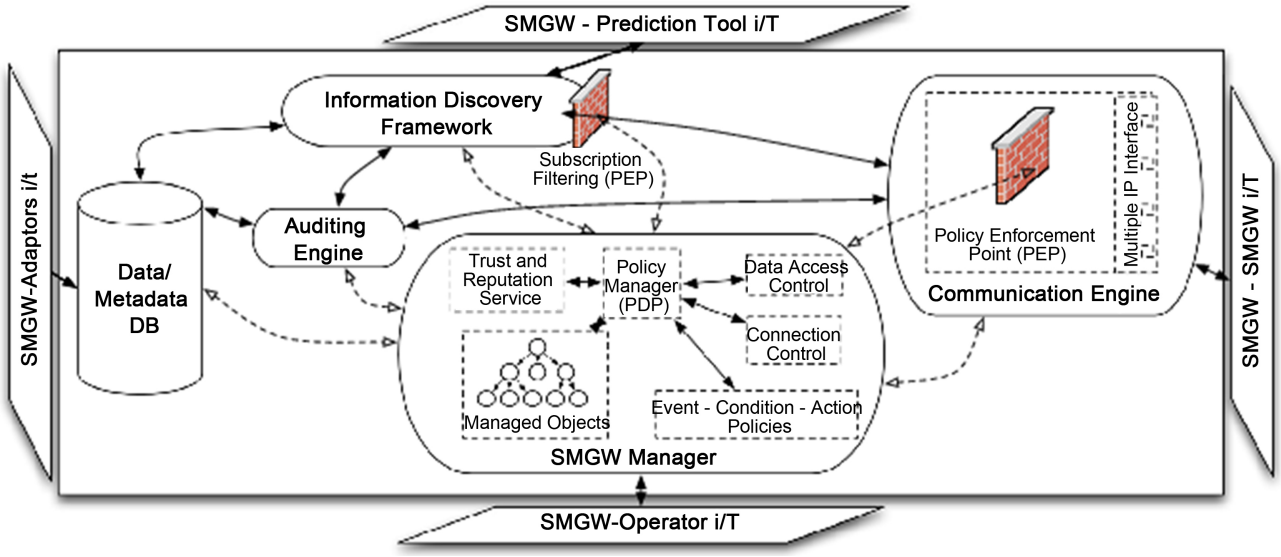

Figure 2. SMGW architecture.

entitlement system. The device's manufacturer needs to request this key. The manufacturer or current owner creates the token, which is paired with the RFID identification of the device. In the case that a device is given a new owner or is going to be used in a different division of the same organization, this technique ensures that permissions can be changed by the device itself, minimizing the burden on the new owner. Owners can replace these tokens, replacing the prior token's rights and access control, as long as the old token is still available. When a new home is purchased, this mechanism is comparable to changing the old key.

- **Machine learning**

Canedo, J., & Skjellum, A. [2] suggest employing machine learning within an IoT gateway to help secure the system in order to overcome the difficulties in securing IoT devices. In the field of machine learning, computer programs are given the ability to learn from previous performance, analogies, and examples. As learning takes place, the program's skills develop, making it more intelligent and able to make wise decisions. Artificial neural networks (ANN) and genetic algorithms are two of the most well-liked machine learning techniques. In order to convey data for communication, learning, and decision-making, ANNs imitate the neurons and synapses found in the brain. IoT systems employ ANNs to keep track of IoT device status and make wise judgments. To create an ANN, the authors [2] chose to use R which is a statistical programming tool that allows for computations. They began by collecting approximately 4000 data samples from the edge devices over the course of one hour and stored the data in a MySQL database within the gateway. Once the neural network was trained, the testing data was then used within the neural network to verify that each attribute is valid. Next, they simulated invalid data and retrained the neural network with both valid and invalid data.

- **Blockchain Technology**

Regarding the implementation of blockchain technology on the IoT, researchers have done several studies. Singh, M., *et al.* [10] explained that one of the difficulties in implementing the Internet of Things (IoT) was security. Blockchain technology, however, can be used to improve IoT security. The report also outlined four strategies for enhancing IoT security, including configuring IoT, finding valid IoT, authenticating users, and employing blockchain technology for secure communication.

Securing IoT devices with a blockchain network makes the system decentralized, in which there is no single authority which can approve any transaction. Each and every device will have a copy of the ever-growing chain of data. This means that whenever someone wishes to access the device and do some transaction, then all the members of the network must validate it. After the validation is done, the performed transaction is stored in a block and is sent to all the nodes of the network. All this make the system more secure and impossible for the un-authorized sources to breach into the security [10].

4. IoT Attacks Mitigation

Tens of billions of devices with a range of vulnerabilities will be connected to the IoT over the course of the next years. These networking devices lack a user interface, a security protocol, computing power, and storage space to support firewalls and diagnostic tools, and they also are unable to establish a WiFi direct connection to the Internet. These flaws create a temptation for those looking to spread DDoS attacks or other nefarious breaches, as well as for companies looking to collect data for intelligent management and digital evidence. Once a DDoS attack is successful, it may endanger human life safety and possibly directly or indirectly result in devastation and death. Recent DDoS attacks have shown that gaps are common in the Internet of Things, which is still in its early stages. The vast majority of Internet of Things (IoT) devices could unintentionally assist DDoS attacks if security measures aren't taken. The above-mentioned issues are addressed by the software-defined anything (SDx) concept. Software defined radio (SDR), software defined networking (SDN), software defined data centers (SDDC), software defined infrastructure (SDI), and software defined world (SDW) are all components of SDx. The separation of the control plane and data plane in the network is the fundamental component of SDN, which is unquestionably the most well-known technology. It achieves flexible network traffic control and offers a solid framework for the development of new core networks and applications [11].

The awareness among human users who are a member of the IoT network is another crucial mitigation measure for the development and success of the IoT framework. Patton M. [12] used numerical examples to describe the effects of failing to secure the IoT. They used either no-password or the default password to access IoT equipment (SCADA devices, web cameras, traffic control devices,

and printers) that were accessible to the general public. The recorded results, which demonstrated that many of these gadgets were genuinely accessible, were highly intriguing. The Internet of Things would do more harm than good if users continued to use the default password that comes with the product and show the same lack of concern for security.

The Internet of Things (IoT) is a well-known technology that significantly affects relationships, employment, healthcare, and the economy, among other things. By automating chores, improving output, and lowering anxiety, IoT has the potential to enhance life in a number of scenarios, from smart cities to classrooms. On the other hand, intelligent IoT applications are significantly impacted by cyberattacks and threats. Due to increasing risks and vulnerabilities, many conventional strategies for protecting the IoT are now inadequate. Future IoT systems will require machine learning and deep learning that is AI-efficient in order to maintain their security protocols [13].

5. Conclusion

Since every layer of the IoT framework is vulnerable to attacks, there are several security requirements and problems that must be fulfilled. IoT research now focuses mostly on access control and authentication protocols, but with technology advancing so quickly, it is crucial to include new networking protocols like IPv6 and 5G to achieve the dynamic mashup of IoT topology. We may soon see the Internet of Things (IoT) revolutionize everything, provided that security issues including privacy, confidentiality, authentication, access control, end-to-end security, trust management, and international regulations and standards are fully handled. In Internet of Things (IoT) systems, when changing or updating hardware components due to security concerns is expensive (or even impossible), security features are crucial. The Internet of Things security threats and recent malware are reviewed in this article, and we then suggest a way to run secure applications on IoT devices as a secure execution framework for the IoT. Verified bytecode execution in a separate framework will ensure that all security enforcement is carried out by software and does not rely on hardware-provided security capabilities.

Internet of Things (IoT) has received a lot of attention recently. IoT has a lot of potential, but it also has a lot of problems and difficulties. One of the biggest problems with IoT technology, apps, and platforms is security.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Abomhara, M. and Koien, G.M. (2014) Security and Privacy in the Internet of Things: Current Status and Open Issues. 2014 *International Conference on Privacy and Security in Mobile Systems* (*PRISMS*), Aalborg, 11-14 May 2014, 1-8.

https://doi.org/10.1109/PRISMS.2014.6970594

[2] Cañedo, J. and Skjellum, A. (2016) Using Machine Learning to Secure IoT Systems. 2016 14*th Annual Conference on Privacy*, *Security and Trust* (*PST*), Auckland, 12-14 December 2016, 219-222. https://doi.org/10.1109/PST.2016.7906930

[3] Mahmoud, R., Yousuf, T., Aloul, F. and Zualkernan, I. (2015) Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. 2015 10*th International Conference for Internet Technology and Secured Transactions* (*ICITST*), 336-341. https://doi.org/10.1109/ICITST.2015.7412116

[4] (2018) T1C: IOT Security: Threats, Security Challenges and IOT Security Research and Technology Trends. 2018 31*st IEEE International System-on-Chip Conference* (*SOCC*).

[5] Dutta, A., *et al.* (2023) Adoption of IOT-Based Healthcare Devices: An Empirical Study of End Consumers in an Emerging Economy. *Paladyn*, *Journal of Behavioral Robotics*. https://doi.org/10.1515/pjbr-2022-0106

[6] Zhao, G., Si, X., Wang, J., Long, X. and Hu, T. (2011) A Novel Mutual Authentication Scheme for Internet of Things. *Proceedings of* 2011 *International Conference on Modelling, Identification and Control*, Shanghai, 26-29 June 2011, 563-566. https://doi.org/10.1109/ICMIC.2011.5973767

[7] Mahalle, P.N., Anggorojati. B. Prasad, N.R. and Prasad. R. (2013) Identity Authentication and Capability-Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber Security and Mobility*, **1**, 309-348. https://doi.org/10.13052/jcsm2245-1439.142

[8] Castrucci, M., Neri, A., Caldeira, F., Aubert, J., Khadraoui, D., Aubigny, M., Harpes, C., Simões, P., Suraci, V. and Capodieci, P. (2012) Design and Implementation of a Mediation System Enabling Secure Communication among Critical Infrastructures. *International Journal of Critical Infrastructure Protection*, **5**, 86-97. https://doi.org/10.1016/j.ijcip.2012.04.001

[9] Xie, Y. and Wang, D. (2014) An Item-Level Access Control Framework for Inter-System Security in the Internet of Things. Applied Mechanics and Materials, **548**, 1430-1432. https://doi.org/10.4028/www.scientific.net/AMM.548-549.1430

[10] Singh, M., Singh, A. and Kim, S. (2018) Blockchain: A Game Changer for Securing IoT Data. 2018 *IEEE* 4*th World Forum on Internet of Things* (*WF-IoT*), Singapore, 5-8 February 2018, 51-55. https://doi.org/10.1109/WF-IoT.2018.8355182

[11] Yin, D., Zhang, L. and Yang, K. (2018) A DDoS Attack Detection and Mitigation with Software-Defined Internet of Things Framework. *IEEE Access*, **6**, 24694-24705. https://doi.org/10.1109/ACCESS.2018.2831284

[12] Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L. and Chen, H. (2014) Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT). 2014 *IEEE Joint Intelligence and Security Informatics Conference*, The Hague, 24-26 September 2014, 232-235. https://doi.org/10.1109/JISIC.2014.43

[13] Mazhar, T., *et al.* (2023) Analysis of IOT Security Challenges and Its Solutions Using Artificial Intelligence. *Brain Sciences*, **13**, 683. https://doi.org/10.3390/brainsci13040683