ISSN 2228-9860 eISSN 1906-9642 CODEN: ITJEA8

International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies

http://TuEngr.com

Internet of Things Major Security Issues: Challenges and Defense Strategies

Adel AlZahrani[1*], Abdullah Safhi[2], Mohammed Al-Hebbi[1]

[1] *King Abdulaziz Medical City NGHA, Jeddah, SAUDI ARABIA.*
[2] *King Abdulaziz University, Jeddah, SAUDI ARABIA.*
**Corresponding Author (Email: adelabz38@ngha.med.sa).*

Paper ID: 12A11S

Volume 12 Issue 11

Received 15 June 2021
Received in revised form 24 August 2021
Accepted 02 September 2021
Available online 10 September 2021

Keywords:
Internet-of-things; IoT security risk; Edge layer; IoT risk solutions; Application layer; Strategy; MIoT; Security challenges; Physical layer; Perception layer; Big data analytics.

Abstract

The Internet of Things (IoT) has enabled significant advancements in a wide variety of scientific fields, and as a result, it has emerged as a highly attractive subject in both academia and business. The IoT aims to achieve universal Internet connectivity by transforming everyday objects into connected gadgets. Regardless of whether it results in beneficial economic and social outcomes, protecting the security and privacy of objects and users remains a critical issue that must be addressed. Addressing and evaluating IoT security risks is critical, as IoT application operating techniques vary according to the variety of IoT environments. Thus, by discussing IoT security concerns alongside available and potential solutions, developers and businesses can identify relevant and timely responses to specific threats, resulting in the best possible IoT-based services. This article discusses the challenges inherent in implementing IoT security and some critical solutions for resolving these issues. Ten papers were extracted and analyzed to contribute to the corpus of literature by focusing on several critical challenges in the internet-of-things sector and shedding light on how these challenges affect a variety of domains, including healthcare, education, and business intelligence. The most frequently mentioned challenges were those related to privacy, as well as the application, network, perception, and edge layers. This paper addressed these issues by incorporating previously discovered solutions. There has been discussion of the implications for both researchers and practitioners.

Disciplinary: Information Technology.

Cite This Article:

AlZahrani, A., Safhi, A., Al-Hebbi, M. (2021). Internet of Things Major Security Issues: Challenges and Defense Strategies. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 12*(11), 12A11S, 1-13. http://TUENGR.COM/V12/12A11S.pdf DOI: 10.14456/ITJEMAST.2021.229

1 Introduction

The internet of things domain has grown in popularity in recent years as a result of considerable advancements in several facets of the human environment, including health, commerce, and transportation. The Internet of Things (IoT) is the next technology leap that will significantly improve several facets of the human environment, including health, commerce, smart cities, and transportation (Grammatikis et al., 2019). Additionally, IoT is becoming more integrated with human behaviors, systems, and processes (Sfar et al., 2018). IoT is a new area that promises universal Internet connectivity by transforming everyday things into connected gadgets. The Internet of Things paradigm is transforming how people interact with their environment, as it paves the way for ubiquitously connected infrastructures capable of supporting novel services and offers increased flexibility and efficiency (Sisinni et al., 2018). IoT is a far broader concept than machine-to-machine communication. IoT is a network of purpose-built physical objects (things) that are incorporated with technology that enables them to sense and interact with their internal state and external environment (Gupta & Shukla, 2016). Although it may result in favorable economic and societal improvements, protecting the security and privacy of objects and users remains a critical issue that must be addressed (Grammatikis et al., 2019).

Addressing and assessing IoT security risks is crucial, as the operating techniques of IoT applications vary according to the range of IoT environments. Thus, discussing IoT security concerns with available and potential solutions enables developers and businesses to identify relevant and timely responses to specific dangers, resulting in the best possible IoT-based services (HaddadPajouh & Parizi, 2019). As a result, researchers are attempting to examine IoT security concerns from a variety of angles. Several of these influence the security requirements and challenges posed by the IoT (Lin et al., 2017; Suo et al., 2012). Additional research identifies potential challenges, vulnerabilities, and responses (Andrea et al., 2015; Mosenia & Jha, 2017). Additionally, numerous publications analyze the security implications of IoT protocols (Granjal et al., 2015; Sain et al., 2017), while others focus on specific security procedures and processes that can help mitigate the effects of potential intrusions (Ouaddah et al., 2017; Sicari et al., 2015). While these works provide major and beneficial contributions, the continual evolution of cyber-attacks necessitates the concurrent investigation of sufficient solutions, necessitating and valuing thorough survey studies (Grammatikis et al., 2019). Due to the Internet of Things' relative youth, there are a few pieces of research examining its social, behavioral, economic, and management ramifications (Lee & Lee, 2015).

As a result, organizations face significant challenges when it comes to making educated decisions about IoT adoption and implementation (Lee & Lee, 2015). To close this gap and aid decision-makers in adopting and implementing IoT, this study attempted to highlight almost all of the obstacles associated with IoT in comparison to the solutions presented in previous research.

The study's objective is to identify the most serious security risks that could jeopardize IoT adoption and then establish how these threats can be managed. Thus, the article's research

challenge might be phrased as follows: What are the most serious IoT security challenges and how are they being addressed?

In this study, the documentary analytical descriptive strategy will be employed, which refers to documents and literature such as research, articles, and books, and addressing them in the study through description and analysis to extract the results and indications. To address the study's topic, this study will assess and critique existing publications on security issues in the internet of things environment. It will do so by utilizing the following research tools: databases accessible through the Saudi Digital Library and global search engines. Ten publications were extracted and examined in total. To achieve the study's aim, this study employs a qualitative approach to adequately describe the phenomenon under examination. According to Saunders et al. (2003), a quantitative method examines what happens during a phenomenon, whereas a qualitative approach elucidates why it occurs. The descriptive-analytical method is used to perform the research in this study. Descriptive assessments concentrate on direct observation of an individual's behavior and events occurring in his or her natural environment and place a larger emphasis on environmental variables (Anderson & Long, 2002). Descriptive studies may aid in our understanding of how reinforcement operates in nature (Anderson & Long, 2002).

2 Internet of Things Challenges

Dai et al. (2020) discussed big data analytics in manufacturing and the Internet of Things (MIoT), including the necessity and challenges of big data analytics in manufacturing data from the Internet of Things. Then, the enabling technologies for manufacturing data analytics are reviewed and explored. Additionally, this study discussed the future paths of this promising field. The authors outlined the challenges of big data analytics in manufacturing data from the Internet of Things as in Table 1.

Table 1: The challenges of big data analytics in manufacturing data from the Internet of Things

Big Data Analytics Phase	Challenges
Challenges in data acquisition	Difficulty in data representation - Efficient data transmission
Challenges in data preprocessing and storage	Data integration - Redundancy reduction - Data cleaning and data compression
Challenges in data analytics	Data temporal and spatial correlation - Efficient data mining schemes - Privacy and security

Grammatikis et al. (2019) gave a comprehensive security analysis of the IoT in this environment, by examining and evaluating potential threats and responses. More precisely, after evaluating and defining security needs for the IoT, it conducted a qualitative and quantitative risk analysis, examining security vulnerabilities at the layer level. Following that, it determined the appropriate countermeasures and their limits, with a particular emphasis on IoT protocols. Finally, it identified future research directions. This paper has provided security challenges in the IoT as follow:

- Interoperability: Security mechanisms developed and used in the IoT should not significantly impede the operating capabilities of IoT devices.

- Resource constraints: Because IoT devices have limited memory and processing capabilities, they may not be able to support expensive security methods like asymmetric encryption.
- Resilience to physical attacks and natural disasters: They are usually small and have little or no physical protection. Devices like smartphones and sensors can be stolen, while stationary devices can be destroyed by natural catastrophes.
- Autonomic control: Users must configure traditional information systems. But IoT devices must set their parameters.
- Information volume: Many IoT applications, such as smart grids and smart cities, consume vast amounts of sensitive and personal data, making them increasingly vulnerable to security risks.
- Privacy protection: Typically, IoT devices include sensitive data that must be encrypted and kept anonymous.
- Scalability: IoT networks typically have millions of objects. So security and privacy protection should be scalable.

HaddadPajouh & Parizi (2019) examined IoT security challenges, their benefits and drawbacks, as well as current and future solutions. Using this taxonomy, the article identified security attributes and requirements for each of the three IoT layers. This study's main contribution was the architectural classification of IoT security threats and problems. The layered architecture was used to categories IoT security issues and solutions to help readers better understand how to address and prevent current IoT security threats. Table 4 shows the IoT security challenges.

Table 2: The security challenges in IoT layers

Layers	challenges
Application Layer	The Constrained Application Protocol (CoAP) security - Insecure Interfaces - Insecure Software and OS - Middle-ware Security
Network Layer	Replay Attack - Insecure Nearest Node Discovery - Buffer Overflow Attack - RPL Routing Attack - Sybil Attack on Network Layer - Authentication and Secure Communication - End-to-end security - End-to-end security - Privacy Violation on the Cloud
Edge Layer	Frequency Jamming Adversaries - Insecure Boot-up/Initialization - Spoofing Attack - Insecure Interfaces - Deprivation Attack

Sisinni et al. (2018) defined IoT, Industrial IoT (IIoT), and Industry 4.0. It emphasized the benefits of the paradigm shift as well as the obstacles to its fulfillment. It addressed issues such as energy efficiency, real-time performance, cohabitation, interoperability, security, and privacy. Also, it included an overview of current research activities and possible research areas for Industrial IoT issues. Despite the huge potential, utilizing industrial IoT presents various challenges. Among the challenges are:

- Energy Efficiency: Much of the IIoT uses long-life batteries. This necessitates low-power sensors without batteries. Affordability is a must.
- Real-Time Performance: The IIoT's quality of service is frequently measured by how well it meets end-to-end (e2e) deadlines for real-time sensing and control.
- Coexistence and Interoperability: The limited spectrum will be shared by many devices as IIoT connectivity expands rapidly. C'est problematic in crowded ISM bands. So device interference must be controlled.
- Security and Privacy: Secure protocols, lightweight cryptography, and privacy assurance are insufficient to secure complex IIoT systems.

Conti et al. (2018) introduced existing significant security and forensics concerns in the IoT sector and then analyzed briefly the papers published in this special issue that addressed those challenges. This study examined the major security challenges that present in IoT contexts, including the following:

- Authentication: Authentication in the IoT domain aids in IoT device integration. Key management is required for IoT device authentication. Without a CA, cryptographic key validation and key transfer integrity require unique procedures.
- Authorization and access control: Access Control restricts access to only approved resources. Controlling access to an IoT network is difficult.
- Privacy: Surveillance by unmanned IoT devices collects personal data (like health records). Harder to find nodes with access to passive user data.
- Secure architecture: Any IoT design should address both security concerns and the challenges of installing IoT devices over SDN and cloud infrastructure.

Sfar et al. (2018) provided a roadmap overview based on a novel cognitive and systemic approach to IoT security. The role of each component of the method has been outlined, as well as their relationships with other major components and their impact on the entire system. A case study was presented to highlight systemic and cognitive components. Then came privacy, trust, identification, and access control issues. The innovative IoT taxonomy has revealed essential solutions and research activity, and fascinating research possibilities. Also, current standardization works for IoT components and applications were reviewed and debated. This study presented four nodes and seven edges for security issues related to IoT as Table 3.

Table 3: Nodes and edges for security issues related to IoT.

Nodes	Person - Process - Intelligent object - Technological ecosystem
Edges	Privacy – Trust - Identification / Access control – Reliability – Safety - Auto-immunity - Responsibility

While the IoT area is still evolving and has numerous unresolved difficulties, Gupta & Shukla (2016) focused on security concerns. Due to the devices' limited processing power and memory, existing security procedures (which are a requirement) should be optimized or a blank slate approach should be taken. This is a survey paper focusing on the security implications of the Internet of Things. Additionally, it explored the unresolved issues in this subject. To build an IoT protocol or architecture, certain challenges must be taken into account.

- Massive scaling: The network's smart devices abound. Authenticating, maintaining, preserving, using, and supporting such massive items is difficult.
- Architecture and dependencies: The internet connects many gadgets. To develop applications, a suitable architecture is required.
- Big Data being generated: There will be a massive amount of raw data collected continuously in the IoT. Techniques for converting raw data into usable information will need to be developed.
- Robustness: They combine sensing, automation, and computation. To cooperate, devices must know their positions, have synchronized clocks, and have a set of parameters such as communication power levels and sleep patterns.

- Privacy: The data stored in the cloud using big data should not be seen by anybody else. For each system, specific privacy policies should be defined.
- Security: The IoT is vulnerable to security attacks due to its small capacity, physical accessibility of sensors, actuators, and objects, and openness of the system, including most components communicating wirelessly.

De Cremer et al. (2017) examined the impact of the Internet of Things on marketing strategies and delves into the often-overlooked subject of the IoT's dark side. Taxonomy for classifying the various sorts of IoT dark-side activity has been devised based on a thorough literature review and expert insights gleaned from the authors' study of the IoT. The framework identified eight distinct types of dark-side behavior, which can be classified into four major categories. This classification demonstrated the relationship between various forms of dark-side behaviors and critical strategic IoT processes, as well as how these dark-side behaviors may be addressed through a more strategic and integrity-oriented approach. Figure 1: shows the summary of the dark side of the internet-of-things.

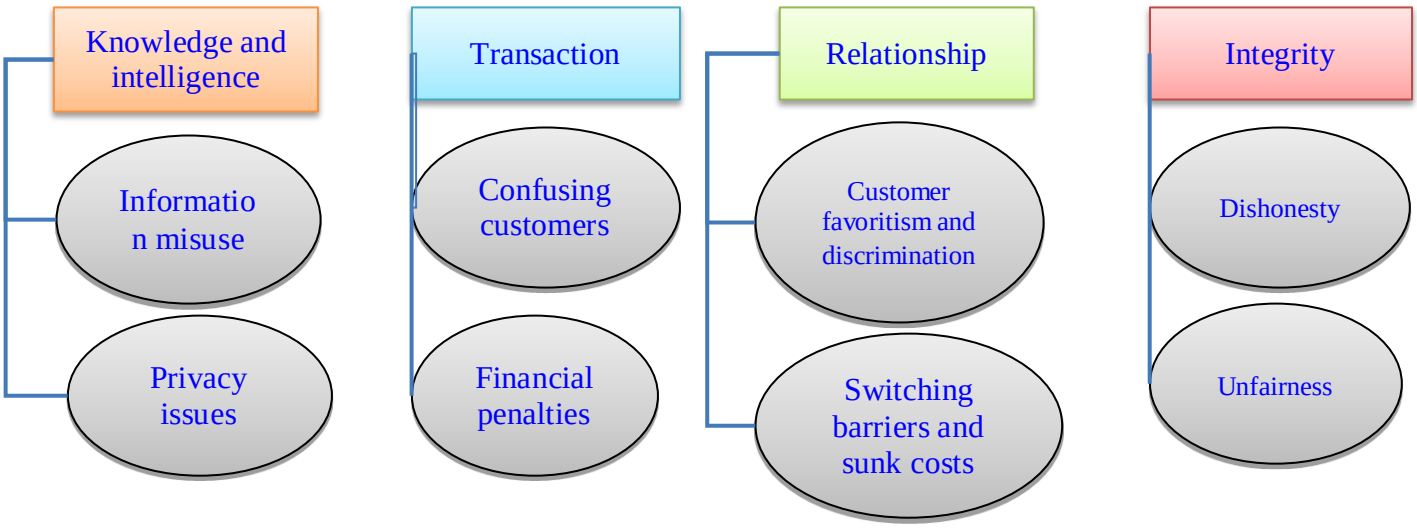

Figure 1: The dark side of internet-of-things

Kumar et al. (2016) reviewed security attacks from the perspective of the layers that form the Internet of Things, using example scenarios. Additionally, a summary of strategies for resolving these concerns has been provided, along with their inherent limitations. To circumvent these constraints, it has established a framework for future work proposals. This research conducted a review of prior works in order to extract the solutions presented in them. The security challenges in IoT layers are presented in Table 4.

Table 4: The security challenges in IoT layers.

Layers	challenges
Application Layer	Malicious code attacks - Tampering with node-based applications - Inability to receive security patches - Hacking into the smart meter/grid
Perception Layer	Eavesdropping - Sniffing Attacks - Noise in data
Network Layer	DoS attack - Gateway Attacks - Unauthorized Access - Storage Attacks - Injecting fake information
Physical Layer	Physical Damage - Environmental attacks - Loss of Power - Hardware Failure - Physical tampering

Lee & Lee (2015) study titled "The Internet of Things (IoT): Applications, investments, and challenges for enterprises" This review article highlighted five IoT technologies that are critical for the successful deployment of IoT-based products and services, as well as three IoT categories for enterprise applications that add value to customers. Additionally, it compared the net present value method and the real options approach, which are frequently used to justify technology initiatives, and demonstrated how the real options approach may be used to justify IoT investment. Finally, five technological and managerial issues were explored in this essay. The next section highlights enterprise-level IoT development challenges based on the survey of IoT practices.

- Data management challenge: There is an enormous amount of data generated by IoT sensors and devices. The present data center architecture cannot handle the heterogeneity and volume of personal and business data.
- Data mining challenges: Unstructured picture and video data cannot be mined using traditional data mining methods. In addition to a lack of advanced data mining technologies, there is a paucity of skilled data analysts.
- Privacy challenge: While the IoT continues to grow through smart home systems and wearable devices, user confidence and acceptance will be based on privacy protection.
- Security challenge: While the Internet of Things increases business productivity and improves people's lives, it also increases attack surfaces for hackers and other cybercriminals.
- Chaos challenge: Concerns about security and privacy continue to plague the industry as well as the proliferation of untested gadgets. Multi-purpose devices and collaborative applications can cause havoc if not developed appropriately.

3 Discussion

This study emphasized on how every study, included in this review, addressed IoT challenges from its standpoint.

Dai et al. (2020) concentrated on big data analytics in manufacturing and the Internet of Things (MIoT). The authors summarized data storage solutions in two ways: 1) infrastructure for data storage, and 2) data management software.

1- Infrastructure for data storage: Many networked storage devices exist. Hard drives, SSDs, cassettes, USB flash drives, SD cards; micro SD cards, Read-Only Memory (ROM), CD-ROMs, DVD-ROMs, etc. Industrial MIoT storage infrastructure can be built by connecting these devices (wired or wireless).
2- Data management software: The data management software has three layers:
    - Distributed file systems: This file system was designed to serve massive data-intensive distributed applications like search engines. Apache also proposed Hadoop Distributed File System (HDFS) as a replacement for GFS. There's also C# Open Source Managed Operating System (Cosmos) and Haystack.
    - Database management systems (DBMS): DBMS helps organise data efficiently and effectively. Traditional relational DBMS (aka SQL databases) and non-relational DBMS (aka Non-SQL databases).
    - Distributed computing models: Several distributed computing models for big data analytics are presented. E.g. Google MapReduce, Hadoop MapReduce.

The authors agreed that responding to malicious attacks is challenging. There are several possible solutions to this problem: Key management that includes key distribution and validation,

authentication that includes access control of files and data records, and data access tracing that allows malicious behavior to be discovered and avoided or cancelled.

Grammatikis et al. (2019) focused on IoT challenges in the level layer. The solutions for the attacks for layers are presented in the following Table 5.

Table 5: Layers and solutions for IoT challenges

Layer	Solutions
The perception layer	One can effectively deal with natural disasters and environmental risks by using particular technical approaches such as infrastructure design or sensor placement. For the physical dangers, it is needed for user identification, physical access control, and a trust foundation.
The communication layer	Intrusion detection and prevention systems may be regarded as a viable method for detecting, mitigating, or preventing these attacks promptly.
The support layer	Only legitimate users and objects should be allowed to access the storage systems' services and data. Secure programming, firewalls, and IDPS systems are crucial countermeasures to prevent data loss.
The business layer	Using a high-level programming language that automatically manages memory could be a security solution. Various security technologies and techniques, such as access control and IDPS systems, should be used to increase OS security.

Sisinni et al. (2018) focused on four challenges facing the Industrial Internet of Things (IIoT). Solutions are

- Energy Efficiency: A query or continuous delivery of sensing data consumes energy in dense deployments. IIoT green networking saves power and money. It will cut pollution, conserve energy, and raise awareness. Thermal, solar, vibration, and radiofrequency (RF) energy can all be captured. To harvest such natural resources, an energy source is required.
- Real-Time Performance: To achieve needed QoS in IIoT, time-slotted packet scheduling is vital. Many industrial wireless networks use static DLL scheduling for deterministic e2e real-time communication. A new network schedule is created and distributed using these techniques periodically obtaining network health data.
- Coexistence and Interoperability: They must be able to identify and reduce the external influence. The TelosB mote CA2400 with Texas Instrument CC2420 transceiver from Crossbow showed promise. Use SVMs with sensor durations < 300 ms to classify external interference.
- Security and Privacy: To protect IIoT infrastructure, existing industrial WSN encryption methods may need to be analyzed before applying to secure IIoT protocols. So, for example, the lack of processing and memory resources prevents the use of resource-intensive crypto-primitives like PKC (PKC).

Sfar et al. (2018) proposed solutions for IoT security challenges at every node and edge. Table 6 shows these solutions.

Table 6: Solutions for IoT security challenges at every node and edge

Challenge	Solution
Person	To emphasize the node's complexity, we should note that persons have varying levels of security. It is proposed that individuals complete duties related to security rule administration using the Plan-Do-Check-Act method established in ISO/IEC 27000 series.
Process	Each IoT architecture component must be fully compliant with all applicable security requirements such as policies, standards, strategies and processes.
Intelligent object	The designers of these things must contend with their ubiquitous nature in order to adhere to particular security requirements.
Technological ecosystem	To ensure a generic and efficient secure technological ecosystem, consider the following: (1) security process design and setup, (2) entity identification and authorization, (3) security perimeter precision, and (4) physical environment protection.
Privacy	In this case, privacy refers to allowing staff appropriate access credentials without disclosing sensitive information.
Trust	Trust management (creating, updating, and revoking credentials, keys, and certificates) is a critical security concern in IoT. Because human and non-human things are involved in the global system, trust is established between objects and people via technology ecosystems.
Identification / Access control	Identifying linked devices (vehicles, items, etc.) allows for their location and tracking. Clearly, instantaneous access to this information can improve global system efficiency and operation.
Reliability	Although research on IoT reliability is still in its infancy, this study identified two major projects: NEBULA (A Trustworthy, Secure, and Evolvable Future Internet Architecture) and the Soft Reliability Project.
Safety	Because software integrated with autonomous objects might generate unanticipated behavior, it must be closely monitored to avoid catastrophic system and environmental repercussions. The paper recommended the E-Safety Project, e-Crime Wales, and Internet Safety Project.
Auto-immunity	: Improving IoT system tolerance to electromagnetic interference is critical to reducing interception and detection risk. This study introduced two important works about immunity-based security and intrusion detection technology.
Responsibility	Contextual plans (safety, cyber-security, access, and security) are identified within the tetrahedron, and edges between nodes are classified accordingly. The security strategy shares an edge with the safety, access, and cyber-security plans.

While Gupta & Shukla (2016) concentrated exclusively on presenting challenges, De Cremer et al. (2017) provided potential solutions after evaluating the Internet of Things' impact on marketing strategies and delving into the sometimes overlooked subject of the Internet of Things' dark side. The authors affirmed that a holistic IoT strategy can develop to avoid dark practices for IoT. This holistic IoT strategy includes:

1- Strategy Development: The goal of this process is to match client requirements to organizational resources and skills. Integrity and manipulative dark-side actions should be addressed at this level.
2- Value Creation: Because the method emphasizes mutually beneficial relationships, it addresses relationship-based dark-side conduct and carelessness. The objective is to co-create a value exchange that benefits both parties.
3- Multi-channel Integration and Customer Experience: The idea is to give the user a consistent image of the IoT provider through interactions on their preferred channels. This process seeks to avoid transaction-based dark-side activities. The goal is to always provide great client service.
4- Information Management: The information management process addresses IoT providers' collection, storage, and use of customer data. Due to the urgency of the situation, it requires both strategic and tactical control. Here, knowledge-based and intelligence-based tasks are conceivable.
5- Performance Assessment: This means monitoring all major IoT touchpoints to ensure all interactions are mutually beneficial. This means assessing the business's success with respect to stakeholders other than customers. This method detects and resolves all customer and stakeholder issues.

In line with Grammatikis et al. (2019), both Kumar et al. (2016) and HaddadPajouh & Parizi (2019) focused on IoT challenges at the level layer. Method and solution for each layer have presented in Table 7.

Table 7: Method and Solution for each layer

Layer	Method	Solution
Application Layer	DSM	They offer five factors for the establishment of security metrics, all of which deal with security analysis and policies in general.
	Game Theory	A technique for assaulting systems to improve security methods.
	Preference Based Privacy Protection Method	Before connecting the device to the Internet of Things, a third-party entity evaluates the user's security and privacy choices and reports them to the service provider, who assigns the user an appropriate security level based on the perceived preferences.
	CCM	Security is quantified in their model in terms of event and asset loss.
	SMSC	Scalable security enhancement system for distributed resources based on the SMC concept.
	ASTM	Adaptive learning technique based on changing internal parameters and dynamic changes to the security system's architecture.
	Insecure interfaces	Verification of password strength, secure code (SQLi and XSS), and installation of application gateway firewalls.
Application layer, and Network layer	Insecure Firmware/OS	Secure software/firmware upgrades regularly, the usage of file signatures, and encryption with validation.
	CoAP security with internet	DTLS, secure application proxy, and resource directory are all used.
Application layer, Transport layer, and Network layer	Middleware security	Secure communication channel with authentication, policy definition, key management and distribution, installation of secure gateways and M2M components, and lightweight encryption solutions.
Edge layer	Frequency Jamming adversaries	Signal strength measurement, packet delivery ratio computation, packet encoding with error-correcting codes, and frequency and position changes.
	Spoofing Attack	Signal strength readings and estimation of the channel.
	Insecure initialization and configuration	Data transmission speeds between nodes are adjusted, and artificial noise is introduced.
	Insecure interface	TPM modules that are hardware-based, and avoid the use of testing/debugging software.
Edge layer and Network layer	Sleep deprivation attack	Intrusion detection system based on multiple layers.
Network Layer	Identity Management Framework Method	Configure the devices using an Identity Manager and a Service Manager.
	ITS Security Methods and Standards for Efficiency – Risk Analysis	Public key infrastructure is employed in that certificate authentication (CA) servers are used to manage and monitor security credentials for network nodes on ITS to devices to prevent data from being disrupted.
	Authentication and Control	When a user seeks authentication to access a device, the device requests permission to do so from a "Registration Authority," the RA authorizes the device to send a question to the user, and if the response is acceptable, the user is granted access to the device.
	Security Middleware	Secure communication between devices is accomplished by the use of entity identification, secure storage, security auditing, data encryption/decryption, and digital signature/verification.
	Replay Attack	For packet verification, define a timestamp and an authentication parameter, as well as a checksum using a hash value.
	Insecure nearest node discovery	Authentication through the use of encrypted (ECC) signatures.
	Buffer Overflow attack	Deploying threat hunting modules such as an intrusion detection system (IDS).
	RPL routing attack	Authentication using a lightweight encryption mechanism, as well as device monitoring.

Layer	Method	Solution
Network layer	Sinkhole and Wormhole attacks	Verification using hash systems, management of trust levels, analysis of device communication, detection of anomalies via IDS, use of encrypted key management, and signal strength monitoring.
	Sybil attacks	Analyzing graphs, analyzing user interactions, and implementing an access control list.
	Authentication and secure communication	Using symmetric and asymmetric encryption systems for encrypting packet payload dispatch type values with, and collecting logs.
	end-to-end security	IPSec is installed, and advanced encryption technology is used for authentication and authorization.
	Session Hijacking	Using a secret key to maintain a session for an extended period, a lightweight encryption scheme.
Perception Layer	AAL	Keep In Touch (KIT) is accomplished through the use of smart objects and technologies such as NFC, RFID, and Closed Loop Hierarchy.
	Cyber Sensors	Cyber sensors that collect data from physical things can be used to perform activities or to respond to real-time events.
	PKI – Product Key Infrastructure	When a node is safely transmitted, it is authenticated by an "offspring node" that delivers a decryption key. The offspring node is still being enhanced and developed.
	SMC	A model of SMCs (Self-Managed Cells) comprising of policy, discovery, and role services.
	ASM	ASM entails four steps: continuous monitoring, analytics and prediction functions, decision-making, and metrics-based adaptive security models. Sensor data is analyzed to learn about the device's surroundings and environment. Very effective in hospitals.
Physical Layer	RFID Tags (Radio Frequency ID)	RFID tags can be incorporated into smart items to enable wireless communication between them.

4 Conclusion

Massive opportunities have opened up as a result of the Internet-of-things. Along with influencing everyone's social and economic behavior, the internet of things has influenced their way of life and thought. While the Internet of Things has benefited economic and social outcomes, it has also introduced a slew of security concerns. This article examines a variety of security features and issues in the IoT environment from the perspectives of privacy protection, application layer, network layer, perception layer, physical layer, and edge layer. In addition, it includes challenges in big data analytics, person, process, intelligent object, technological ecosystem, trust, identification/access control, reliability, safety, auto-immunity, and responsibility. Additionally, this article discusses the internet of things challenges and opportunities for forensics, as well as the Industrial Internet of Things. It also discusses preventive measures for these problems. These research contributions can be found both theoretically and practically. Theoretically, this study focuses on the most common challenges in a variety of areas, which can assist scholars in gaining a comprehensive understanding of these challenges and testing the validity of solutions' methods. To solve these problems, this study includes previously identified solutions. In practice, these solutions would be useful to decision-makers in a variety of industries, including healthcare, manufacturing, education, marketing, and others. Although some progress has been made, there is still much more work to be done to protect IoT security and privacy. To effectively address IoT security issues, technological solutions must be integrated with appropriate laws and legislation.

5 Availability of Data and Material

Data can be made available by contacting the corresponding author.

6 References

Anderson, C. M., & Long, E. S. (2002). Use of a structured descriptive assessment methodology to identify variables affecting problem behavior. *Journal of Applied Behavior Analysis*, *35*(2), 137-154.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*, 180-187. DOI: 10.1109/ISCC.2015.7405513

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, *78*, 544-546. DOI: 10.1016/j.future.2017.07.060

Dai, H.-N., Wang, H., Xu, G., Wan, J., & Imran, M. (2020). Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies. *Enterprise Information Systems*, *14*(9-10), 1279-1303.

De Cremer, D., Nguyen, B., & Simkin, L. (2017). The integrity challenge of the Internet-of-Things (IoT): on understanding its dark side. *Journal of Marketing Management*, *33*(1-2), 145-158.

Grammatikis, R. P. I., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. *Internet of Things*, *5*, 41-70. DOI: 10.1016/j.iot.2018.11.003

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294-1312. DOI: 10.1109/COMST.2015.2388550

Gupta, K., & Shukla, S. (2016). Internet of Things: Security challenges for next generation networks. *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, 315-318. DOI: 10.1109/ICICCS.2016.7542301

HaddadPajouh, H., & Parizi, R. (2019). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, 100129. DOI: 10.1016/j.iot.2019.100129

Kumar, S. A., Vealey, T., & Srivastava, H. (2016). Security in Internet of Things: Challenges, Solutions and Future Directions. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5772-5781. DOI: 10.1109/HICSS.2016.714

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440. DOI: 10.1016/j.bushor.2015.03.008

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, *4*(5), 1125-1142. DOI: 10.1109/JIOT.2017.2683200

Mosenia, A., & Jha, N. K. (2017). A Comprehensive Study of Security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing*, *5*(4), 586-602. DOI: 10.1109/TETC.2016.2606384

Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ait Ouahman, A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, *112*, 237-262. DOI: 10.1016/j.comnet.2016.11.007

Sain, M., Kang, Y. J., & Lee, H. J. (2017). Survey on security in Internet of Things: State of the art and challenges. *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 699-704. DOI: 10.23919/ICACT.2017.7890183

Saunders, M., Lewis, P., & Thornhill, A. (2003). *Research methods for business students*. Essex: Prentice Hall: Financial Times.

Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks*, *4*(2), 118-137. DOI: 10.1016/j.dcan.2017.04.003

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. DOI: 10.1016/j.comnet.2014.11.008

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE Transactions on Industrial Informatics*, *14*(11), 4724-4734. DOI: 10.1109/TII.2018.2852491

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of Things: A Review. *2012 International Conference on Computer Science and Electronics Engineering*, *3*, 648-651. DOI: 10.1109/ICCSEE.2012.373

Brig. Gen. Adel Ali B. Al – Zahrani is Chief of the Safety & Risk Management Dept. WR, King Abdulaziz Medical City, Health Affairs, Ministry of National Guard, KSA. He has a Bachelor's degree in Medical Sciences from Umm Alqura University, Makkah, KSA, and a Master's degree in Public Administration from King Abdulaziz University, Jeddah, KSA.

Abdullah Safhi is associated with King Abdulaziz University, Jeddah, SAUDI ARABIA.

Brig. Gen. Engr. Mohammed Al-Hebbi is Manager, Healthcare Technology Management Services PHC WR, King Abdulaziz Medical City, Ministry Of National Guard Health Affairs. He holds a Bachelor's degree in Biomedical Engineering, from King Saud University, Riyadh KSA, and a Master's degree in Public Administration from King Abdulaziz University, Jeddah KSA.