JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 08 Issue 01
2024

Research Article
https://doi.org/10.56979/801/2024

A Comprehensive Survey of IoT Threats Assessment and Mitigation Strategies

Salman Mushtaq Qureshi[1*], Syed Muhammad Sajjad[2], Faisal Fiaz[2], Komal Batool[3], Muhammad Kaleem[4], Sayyid Kamran Hussain[5], and Sadaqat Ali Ramay[5]

[1]Department of Risk Management, Sauid Credit Bureau, Riyadh, Saudi Arabia.
[2]Department of Cyber Security, Air University, Kharian, Pakistan.
[3]Faculty of Computing, Riphah University, Islamabad, Pakistan.
[4]Department of IT , Faculty of Computing & IT , University of Sargodha, Pakistan.
[5]Department of Computer Science, Faculty of Science and Technology, TIMES Institute, Multan, Pakistan.
[*]Corresponding Author: Salman Mushtaq Qureshi. Email: mushtaqsalman@gmail.com

Received: May 20, 2024 **Accepted:** September 22, 2024

Abstract: As the quantity of gadgets linked to the internet rises, cybersecurity has emerged to be an essential topic especially with the emergence of the IoT. It is crucial to shield IoT systems from numerous threats to avoid possible vulnerabilities and preserve the users' security. This survey aims at revealing the sphere of influence of the IoT which is a technique that makes it possible for messages to be sent across different physical items.. Used massively in industrial and social contexts, IoT improves ease of life while posing significant risks to security. As IoT devices feature an autonomous functionality and rather limited human intervention, they require smart and secure design. further more, through paper explains the security risks associated with IoT and gives relative attention about different layers and need for effective solution. Through pointing out the issues of portability, resource limitation, and open environments, this work is intended to help researchers and manufacturers strengthen the IoT devices against possible attacks and contribute to the proper, secure, and productive IoT development.

Keywords: IoT Security; Internet of Things; Security Threats; Mitigation Strategies; Autonomous Devices; Connected Devices; Cybersecurity; Vulnerabilities.

1. Introduction

As of now, it's projected that there are about 14 billion connected IoT devices. It is projected that this figure rise to approximately 29. 42 billion by 2030.Here are 5 standout IoT stats for 2023 [1]. It is estimated that there are well over 15 billion connected IoT devices out there now. IoT projections extends with active devices increasing to 2 billion by 2030. Internet of Things/IoT Devices in Greater China is well over 5 billion devices. About 65 percent of devices are Internet of Things enabled. This is because according to a 2020 forecast, IoT devices are more in number in the world than the non IoT devices. Global statistics proclaim that by 2025 the number of (IoT) devices will considerably outweigh the quantity of non-IoT devices.

With every IoT ecology or context, there are 4 fundamental levels [2]. The first level integrates a number of sensors and actuators to collect the facts as well as implement multiple tasks. After that, another layer used the communication network for conveying the collected data. Finally, in the current context of dynamism in the IoT applications, there is a popular enhancement of the third layer, called the middleware layer, which acts as a link between the network and the applications. The last or the fourth layer also includes various end-to-end IoT applications including smart grid, smart transport, and smart factories among others. Each layer has its security concerns as will be discussed in detail below. Further, several gateways link these layers thus providing a means for data transfer and at the same time presenting certain security risks. The security threats and the available counter measures that are relevant in the context of the IoT are discussed in this paper in a comprehensive manner.

2. Critical Security Application Domains in IoT

Security is a concern of significant concern in most of the IoT applications that have been deployed or are in the process of deployment. The growth of the IoT and the applications are on the rise, and it's being implemented in near all the industries available today. Although these IoT applications are provided by operators leveraging on current networking technologies, none of such applications demands more security than can be provided by the used networking technologies.

2.1. Sources of IoT Security Risks

However, each of these layers in an IoT application has different technologies; it also has numbers of issues and security threats. Some technologies, devices and applications at the four layers are shown in the figure 1. This section discusses various forms of security threats in as much as the four mentioned layers in IoT applications.

2.1.1. Sensing Layer Issue

The sensing layer is principally involved with the IoT physical sensing devices and the physical IoT actuators. Sensors are getting hold of the physical event that transpires in the vicinity of the sensors. Here, under this context, actuators re-emphasize a special action on the operational phase of the physical world built out of sensed data [3]. There are also numerous types of sensors by the type of data that is being captured: there is the ultrasonic sensors, the camera sensors, the smoke detection sensors for the physical environment sensing and the temperature and humidity sensors are also cultivated and they can be mechanical, electrical, electronic and even the chemical based.

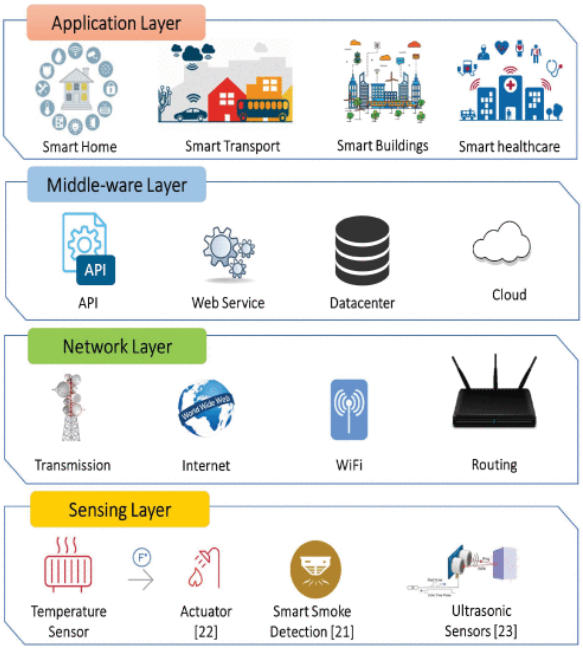

Figure 1. Layers in IoT system.

Figure 2 obviously illustrate the potential threats on these four layers. Special security concerns with the gateways that interface these layers are also reviewed in this section.

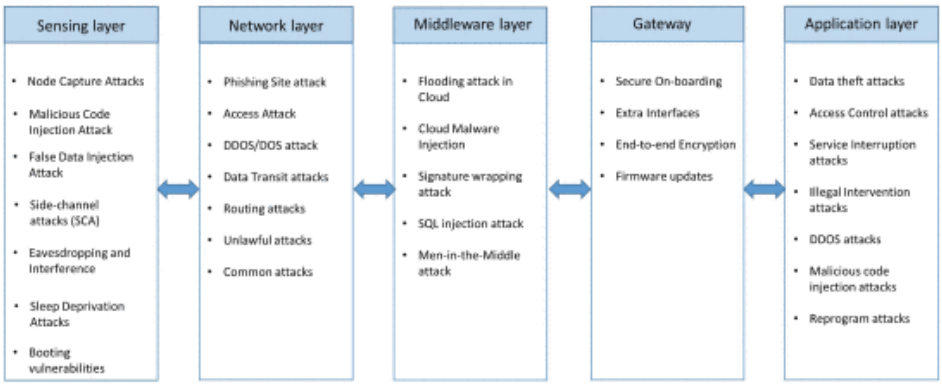

Figure 2. Possible attacks on four layers.

2.1.2. Network Layer Issue

The job of network layer is to send the data that the sensing layer has collected to the computing unit [4].

Major security issues that are experienced at the Network layer are as follows.

- Access Attack
- Phishing Attack
- Data Transit Attacks
- Denial of Service
- Routing Attacks

2.1.3. Middleware Layer Issues

Middleware in IoT is tasked with the responsibility of building a layer of the network between the application layer and the network layer. Middleware can also offer computing and storage capacities as well [5]. This layer offers API to meet the requirements of the application layer. Another layer that comes in the middle of the processes is middleware layer such as brokers, data store management systems, queuing systems, machine learning and so on. While it is important in order to make the IoT application completely reliable and robust, the middleware layer is also exposed to multiple attacks. These attacks can even compromise the middleware and therefore take full control of the whole IoT application. Another two key security issue in the middleware layer is the database security and cloud security.

2.1.4. Gateways Security Issues

This layer is wide as the one that can be Smartphone or a car or an inhabitant of the area or a cloud service. Gateways are also useful in providing the solutions with regard to the hardware and software of the IoT devices. Gateways are employed in deciphering and encoding information from/to IoT devices along with translating the protocols required for the different layers of technology [6].

Today's IoT systems are heterogeneous encompassing LoraWan, ZigBee, Z-Wave and even TCP/IP stacks with multiple gateways in between.

2.1.5. Application-Layer Issues

Thus is the only layer that communicates and deals with the end users and provides the services. Smart home applications, smart meters, smart cities, smart grids, and so on, fall under this layer of IoT applications. As they pointed out this layer has its own security issues such as theft of data and has no privacy as seen in other layers [8].

As with most of the security issues that arise at this layer, they are also specific to the application in question. Quite many IoT applications also incorporate an extra layer between the network layer and application layer which is termed as the application support layer or the middleware layer. The support layer offers access to number of business services and in overall resource management and computation [9]. Given below are some of the major security threats related to the application layer.

3. Mitigations of IoT Attacks

In the previous section, we pointed out some of the security threats that affect IoT applications, in this section we are going to describe some of the approaches that can be used to protect IoT applications and the environment.

• Within this framework, IoT security using the Fog computing paradigm can be understood as the implementation of security measures at the boundary of the IoT system.

• IoT Security leveraging Machine Learning

• An analysis of the state of IoT security: Applying this concept in edge computing

• Blockchain to Security Internet of Things.

3.1. Fog Computing IoT issues

Fog computing is a distributed computing concept that is positioned in-between the edge computing and cloud computing layer and deals with data processing, computation, storage as well as services. Hence, similar to fog computing, edge computing is a model that extends the benefit and strength of cloud closer to the source of data origin and usage [11]. With reference to the attacks elucidated in Section III, below is the solution that fog computing provides or could provide to solve such security issues.

Man-in-the-middle attack: Fog layer acts like a veil to the end-user from the cloud or the IoT system. All the threats or attacks to the IoT systems are those that are obliged to pass through the fog layer in the

middle and the layer is able to detect all the undesired activities to prevent or remove them before they get to the system.

Data transit attacks: The general handling and storing of data are much enhanced in case they are done in the secure fog nodes instead of in the IoT device. If stored on the fog nodes then the data will be more secured than to be stored on the end user devices. Other tasks that are performed by the fog nodes include also making the user data more available [11].

Eavesdropping: In a way of data transmission, it is only between the end-user and a specific fog node without the influences of the other nodes. As it is; it becomes challenging for an adversary to stage an eavesdropping exercise because overall traffic on the network is comparatively smaller.

Resource-constraint issues: This is so because most IoT devices are constrained in terms of resources and the at-tackers have leveraged on this. They try to compromise the edge devices and include the latter as the weak links to be used to infiltrate the system. The fog nodes can help the edge devices and also can remove effects of such attacks to the devices. All security related operations other than simple encryption and decryption can be performed by a neighboring fog node [12].

Incident response services: Such fog nodes can be created to meet on-demand incident response services at a particular time. Notably, it is desirable for fog nodes to generate a flag to the IoT system or the end users each time they receive any form of nasty data or a request. What one gets from fog computing is the ability in the detection of the malware and the solving of the issues that may be present during transit. This makes it possible to manage the malware incidences because it becomes very hard or nearly impossible in most of the crucial applications to fOR instance close the whole system [13].

Such resolutions can be useful with the fog nodes while the system is still active.The fog nodes can be useful in any of such resolutions while the system is on.

3.2. IoT Security Using Machine Learning

- The field of ML has attracted much attention over the recent years. As it is seen, ML is used in many domains for their developments and IoT security is one among that. From the literature, it appears that ML can protect IoT devices from cyber-attacks since ML provided a different perspective in terms of security against the attacks compared to traditional mechanisms [14].
- Relating to the attacks discussed in Section III with regards to the security threats described, the following solutions provided by ML to counter overcome these security risks are as follows.
- **DoS Attack:** DoS attacks which are targeted at IoT devices or those originated from IoT devices are something that should not be taken lightly. For that reason, it is possible to defend the networks against such attacks using the protocol established on Multi-Layer Perceptron (MLP). ML approaches were helpful in improving the deduced accuracy and at the same time preventing IoT devices that are vulnerable to DoS attacks.
- **Eavesdropping:** While passing on messages, the attackers can be very wise in order to eavesdrop as the messages are being passed. To prevent such attacks, several ML tactics, which are Q-learning based offloading strategy and nonparametric Bayesian among others, can be used [15]. There other ML techniques that may also be used to guard de-vices against eavesdropping and these are the schemes like Q-learning and Dyna-Q.
- **Spoofing:** The given techniques can be used to counter spoofing attacks and these are Q- Learning with Dyna- Q, SVM, DNN model, Incremental Aggregated Gradient (IAG), and distributed Frank Wolfe (dFW). In addition, these techniques also effectively improve the detection accuracy and classification accuracy, average error rate and false alarm rate is relatively low.
- Privacy Leakage: For instance, receiving health data, location, or photos the personal data of the user comes under threat. Ensuring that the Privacy Leakage is avoided should be done using the privacy-preserving scientific computations or the PPSC. Another approach that has been advocated for the establishment of IoT application trust is a commodity integrity detection algorithm which uses CRT.
- **Digital Fingerprinting:** Digital fingerprinting is one of the innovative and effective approaches to secure IoT system, as well as to achieve the desired level of trust for the end users in the relevant applications. Fingerprints are now used to unlock smart phones payment authentication, unlock cars and homes etc. As mentioned by [16].
- Though studied for their effectiveness, digital fingerprinting is already proving to be economical, reliable, and practicable and highly secure; it is gradually emerging as the most preferred method of

the biometric identification. Apart from the advantages of the digital fingerprinting, there are several limitations on how this technique to be used efficiently and effectively in IoT, namely: the fingerprint classification, the image enhancement, the feature matching, etc.

3.3. IoT Security Using Edge Computing

Thus, in an edge computing framework the compute and analysis power is available precisely at the edge itself. The devices in an application can be interconnected and then the single devices in an interconnection can process the data. Therefore, a large amount of data can be protected from being transmitted out of the device, to the cloud or to the fog nodes and this in turn enhances the security of the particular IoT application.

I have elaborated below in relation to the attacks discussed in Section III the solutions that can be provided by edge computing or could be potential solutions.

Data Breaches: In edge computing all the information relating to a specific device or an organization is stored and managed at the edge. As for data transfer there is only transfer of data from the data originator to the processor. This ensures the data is not in transit and thus ensures there are no data thefts and breaches of data [17].

In fog computing, there is information downloading from a device to the fog layer and this is where an adversary may capitalize on.

Data Compliance Issues: In this case most countries have set the legal provisions that regulate transfer of data across their territories for example European Union has set GDPR (General Data Protection Regulation). Some of the features that are included –; The data can remain within the organization's premises through edge computing, and addresses the issue of data sovereignty compliance.

Safety Issues: Security and safety are assumed as inherent aspects with the progress of the integration of cyber-physical systems. But if there is even a little delay in the responses, then that may cause physical security complications. For instance, if sensors of a car are showing that an accident is imminent then the air bags need to be inflated immediately.

Bandwidth Issues: IoT application generate data in the form of streams at a very fast rate and in large amount. Slightly over half of that information is initial information and, as a rule, it can be referred to low analytics. This also means that the transfer of all data to the cloud is expensive in terms of bandwidth costs as well as security of the data transfer [18].

If edge computing is used then much of data cleansing and data aggregation can be done in distributed edge nodes and only the summarized data if required can be sent to the cloud.

3.4. IoT Security Using Block chain techniques

In the context of IoT and the use of block chain technology, the most important progress has been made in security. In its simplest form Blockchain is an account book that contains all the transactions where it records the transaction as a hash.

As it has been seen, there are many advantages in terms of IoT applications while using the blockchain technology.

Blockchain can store data coming from IoT devices: This concern involves a huge number of applications that involves multiple different devices connected under IoT. These other devices are extended and managed and connected to these devices. This setup is then connected to cloud so as to enable IoT applications to be executed from any point of location. That is why there are many opportunities in data movement, and therefore blockchain is suitable for storing data and preventing their misuse. Therefore, no matter in which layer of an IoT application one interacts, blockchain can be a right way to store and transfer data.

Blockchain has the nature through which data storage is secure: As in the case with the decentralized architecture of the block chain the problem of being a single point of failure like in the case of different IoT applications based on the cloud can be avoided. Therefore, irrespective of where the devices are, the data generated thereon can be secured on the blockchain.

Data encryption using the hash key and verified by miners: Even at the central hub in blockchain implementation, the actual data can't be stored instead only the 256-bit hash key of the data only can be stored. This is because if there is any change in the pieces of data then there hash will change in some way means that the pieces of data have been changed. It also assist in making the data secure / personalized. It

will also be appropriate to point that the size of block chain will not be of any concern when it comes to size of data since all that is stored in block chain is the hash value [19].

Avoidance from spoofing attacks/ data loss: For instance, in spoofing attacks on IoT applications, a new adverse node will try and infiltrate into the IoT network and then mimic a node in the real network. In spoofing, the adversary can actually get a chance to capture, monitor or even forward data through the network. The latter works as a practical solution to avert hackers as the blockchain does. Every legal user or device is registered in blockchain and the devices are able to identify each other and authenticate each other without any intermediary, or certification center. Since most of the IoT devices are low power devices hence they potentially have data loss [20].

It could be a reality that due to some factors in the external environment even the recipient has a possibility of losing the data sent or received. This does away with such losses as soon as the block has been incorporated within the chain, the block cannot be expunged.

Blockchain to prevent unauthorized access: IoT is rich of applications and many of these applications have a lot of long-lived sessions that include sending a large number of messages between different nodes. The exchange or transaction in blockchain is through Public and Private keys hence only the particular member or nod can see the data. However, in the case that the unintended party gets hold of the data, he or she will not be in a position to understand the contents of the data since the data is encrypted using keys. Therefore, blockchain data structure tries to solve several security concerns that exist with IoT applications.

Despite the fact that blockchain technology provides many securities for the distributed environment, IoT has a specific issue of scarcity of resources. IoT devices are extremely limited in terms of resources, and this in turn implies that large ledgers cannot be stored on the devices. That is why, there are some studies in this regard to enable the implementation of blockchain in IoT. Among the promising possible solutions that can be used to implement blockchain for IoT devices, there is a proxy-based architecture. Here, one needs mention the fact that proxy server can also be incorporated into the network.

4. Taxonomy

Table 1. Taxonomy

Category	Sub Category	Key Concept	Paper	Contribution	Limitations
IoT Security	IoT Security Datasets	Datasets for IoT security Dataset creation and evaluation Dataset characteristics and diversity	A Reviewof Machine Learning (ML)-based IoT Security in Healthcare: A Dataset Perspective Generating Datasets for Anomaly-Based Intrusion Detection Systems in IoT and Industrial IoT Networks	Provides a comprehensive survey of available datasets specific to IoT security. Highlights the importance of dataset diversity for effective security measures.	Existing datasets may lack realism or fail to cover all attack vectors. Dataset generation can be costly and time-consuming.

	IoT Security Taxonomy	Taxonomy ofIoT threats and attacks Layer-wise security challenges Categorization of IoT attacks`	State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions Landscape of IoT security	Offers a structured categorization of IoT threats and security challenges. - Assists in identifying and mitigating security issues across different IoT layers.	Static taxonomies may not adapt well to emerging threats. Might overlook novel or unforeseen attack methods.
Machine Learning in IoT	ML Algorithm for IoT Security	Application of ML algorithms in IoT Anomaly detection techniques Performance evaluation metrics	Advancing IoT Security: A Systematic Review of Machine Learning Approaches for the Detection of IoT Botnets AI, Machine Learning, and Deep Learning: A Security Perspective.	Demonstrates the effectiveness of ML techniques in detecting and mitigating IoT threats. Provides a comparative analysis of different ML approaches for IoT security.	ML models may be resource-intensive, which can be a limitation in IoT environments. Requires large representative data sets for effective tranning.
	Anomaly Detection using ML	Intrusion detection systems Anomaly detection in IoT Attack scenarios and	Detection of Security Attacks in Industrial IoT Networks Enhancing IoT Device Security through Network Attack Data Analysis Using Machine Learning Algorithms	Enhances the accuracy and efficiency of detecting anomalies in IoT networks. Provides robust solutions for detecting a variety of IoT-specific attacks.	High false positive rates can be a challenge. Dependence on high-quality datasets may limit generalizability. Proposed solutions might not be applicable to all IoT environments. Security and performance

	IoT Security Challenges	detection accuracy	Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence Security at the Edge for Resource-Limited IoT Devices	Addresses the challenges of securing resource-constrained IoT devices. Proposes lightweight and decentralized security solutions.	trade-offs may be necessary.
Challenges in IoT		Resource constraints in IoT Lightweight security solutions Securing resource-limited devices			Current datasets may not fully capture the complexity of real-world IoT environments. - Benchmarking across diverse datasets can be challenging.
	Dataset Availability and Benchmarking	Lack of benchmark datasets Need for realistic datasets Heterogeneity in datasets	A Survey on Performance Evaluation of Artificial Intelligence Algorithms for Improving IoT Security Systems Generating Datasets for Anomaly-Based Intrusion Detection Systems in IoT and Industrial IoT Networks	Identifies the need for standardized and comprehensive IoT datasets. Encourages the development of benchmark datasets to improve security research.	Integration may be complex and costly. Risks such as bias and lack of transparency in AI decisions remain a challenge.
	Integration of AI with IoT			Highlights the role of AI in addressing IoT security challenges. Discusses integration challenges and offers adaptive	

	A Survey on Performance Evaluation of Artificial Intelligence Algorithms for Improving IoT Security Systems	solutions for AI-IoT systems.
AI-IoT integration challenges Security, compatibility, and complexity Need for adaptive architectures	Cyber Threat Intelligence for IoT Using Machine Learning	

5. Conclusions

In this survey paper, we have elaborated on the security threats to the IoT devices concerning different IoT layers e.g. physical, software, and network & encryption layers. Also we discussed how to mitigate these threats using different available platforms like Edge computing, Blockchain, Fog computing and Machine learning. To sum up, there is no silver bullet to security challenges, it will always be a combination of different combination of people, process, and technology.

References

1. Alex, Christin, Giselle Creado, WesamAlmobaideen, Orieb Abu Alghanam, and Maha Saadeh. "A comprehensive survey for IoT security datasets taxonomy, classification and machine learning mechanisms." Computers Security 132 (2023): 103283.
2. Harahsheh, Khawlah M., and Chung-Hao Chen. "A survey of using machine learning in IoT security and the challenges faced by researchers." Informatica 47, no. 6 (2023).
3. De Keersmaeker, Franc¸ois, Yinan Cao, Gorby Kabasele Ndonda, and Ramin Sadre. "A survey of public IoT datasets for network security research." IEEE Communications Surveys Tutorials 25, no. 3 (2023): 1808-1840.
4. Chawla, Diksha, and Pawan Singh Mehra. "A survey on quantum computing for internet of things security." Procedia Computer Science 218 (2023): 2191-2200.
5. Javanmardi, Saeed, Mohammad Shojafar, Reza Mohammadi, Mamoun Alazab, and Antonio M. Caruso. "An SDN perspective IoT-Fog security: A survey." Computer Networks 229 (2023): 109732.
6. Kaur, Barjinder, Sajjad Dadkhah, Farzaneh Shoeleh, Euclides Carlos Pinto Neto, Pulei Xiong, Shahrear Iqbal, Philippe Lamontagne, Suprio Ray, and Ali A. Ghorbani. "Internet of things (IoT) security dataset evolution: Challenges and future directions." Internet of Things 22 (2023): 100780.
7. Sarker, Iqbal H., Asif Irshad Khan, Yoosef B. Abushark, and Fawaz Alsolami. "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions." Mobile Networks and Applications 28, no. 1 (2023): 296-312.
8. Najmi, Kholoud Y., Mohammed A. AlZain, Mehedi Masud, N. Z. Jhanjhi, Jehad Al-Amri, and Mohammed Baz. "A survey on security threats and countermeasures in IoT to achieve users confidentiality and reliability." Materials Today: Proceedings 81 (2023): 377-382.
9. Thabit, Fursan, Ozgu Can, Asia Othman Aljahdali, Ghaleb H. AlGaphari, and Hoda A. Alkhzaimi. "Cryptography algorithms for enhancing IoT security." Internet of Things 22 (2023): 100759.
10. Mahamat, Michael,¨ Ghada Jaber, and Abdelmadjid Bouabdallah. "Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges." Wireless Networks 29, no. 2 (2023): 787-808.
11. Falayi, Ayodeji, Qianlong Wang, Weixian Liao, and Wei Yu. "Survey of distributed and decentralized IoT securities: approaches using deep learning and blockchain technology." Future Internet 15, no. 5 (2023): 178.
12. Alwahedi, Fatima, Alyazia Aldhaheri, Mohamed Amine Ferrag, Ammar Battah, and Norbert Tihanyi. "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models." Internet of Things and Cyber-Physical Systems (2024).
13. Siwakoti, Yuba Raj, Manish Bhurtel, Danda B. Rawat, Adam Oest, and R. C. Johnson. "Advances in IoT security: Vulnerabilities, enabled criminal services, attacks, and countermeasures." IEEE Internet of Things Journal 10, no. 13 (2023): 11224-11239.
14. Alqarawi, Ghaida, Bashayer Alkhalifah, Najla Alharbi, and Salim El Khediri. "Internet-of-things security and vulnerabilities: case study." Journal of Applied Security Research 18, no. 3 (2023): 559-575.
15. Mazhar, Tehseen, Dhani Bux Talpur, Tamara Al Shloul, Yazeed Yasin Ghadi, Inayatul Haq, Inam Ullah, Khmaies Ouahada, and Habib Hamam. "Analysis of IoT security challenges and its solutions using artificial intelligence." Brain Sciences 13, no. 4 (2023): 683.
16. Zohourian, Alireza, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Hassan Mahdikhani, Priscilla Kyei Danso, Heather Molyneaux, and Ali A. Ghorbani. "IoT Zigbee device security: A comprehensive review." Internet of Things 22 (2023): 100791.
17. Shirvani, Mirsaeid Hosseini, and Mohammad Masdari. "A survey study on trust-based security in Internet of Things: Challenges and issues." Internet of Things 21 (2023): 100640.
18. Jahangeer, Asma, Sibghat Ullah Bazai, Saad Aslam, Shah Marjan, Muhammad Anas, and Sayed Habibullah Hashemi. "A review on the security of IoT networks: From network layer's perspective." IEEE Access 11 (2023): 71073-71087.
19. Mathur, Shikha, Anshuman Kalla, Gurkan G¨ ur, Manoj Kumar Bohra,¨ and Madhusanka Liyanage. "A survey on role of blockchain for iot: Applications and technical aspects." Computer Networks 227 (2023): 109726.
20. Ni, Chunchun, and Shan Cang Li. "Machine learning enabled industrial iot security: Challenges, trends and solutions." Journal of Industrial Information Integration (2024): 100549.