International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

Analysis on Security Vulnerabilities of the Modern Internet of Things (IOT) Systems

Dr. Srinivas A Vaddadi,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. Vsad93@gmail.com

Dr. Rohith Vallabhaneni,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. rohit.vallabhaneni.2222@gmail.com

Dr. Abhilash Maroju,

Ph.D. Research Graduate, Department of Information Technology, University of the Cumberlands , USA. doctorabhilashmaroju@gmail.com

Sravanthi Dontu,

PhD Research Student, Department of Information Technology, University of the Cumberlands, USA. sravanthi.dontu13@gmail.com

ABSTRACT

The IoT, or Internet of Things, has quickly grown in popularity as a means to collect data in real-time from any and all linked devices. These networked physical objects can exchange data with one another via their respective sensor technologies and have their own unique identifiers. Insightful data analytics applied to the obtained information also presents a substantial possibility for many organisations. Embedded devices, authentication, and trust management are all areas where the Internet of Things has shown a significant security hole. This study delves into the problems with the Internet of Things (IoT), covering topics such as its privacy and security, its vulnerability, its analytics at the moment, the impending ownership threat, trust management, IoT models, its roadmap, and its security issues. It then offers solutions to these problems.

1. INTRODUCTION

In this era of ubiquitous wireless communication and global interconnection, the field of computer networking has witnessed tremendous technological growth. It was in 1999 that Kevin Ashton initially used the term "Internet of Things (IoT)" [1]. The Internet of Things (IoT) is a relatively new platform that allows for the creation of networks linking different objects in the physical and virtual worlds [2]. The Internet of Things (IoT) enables autonomous sensing and action by connecting disparate physical items, ranging in size from small wearables to large pieces of machinery, through the use of actuators and sensors [3,4].

As more industries begin to employ IoT apps, the quantity of these apps and related devices will grow. One company that offers wearable technology is one that makes gadgets to track and exchange health data and a person's habits. In the healthcare sector, patients are increasingly having access to Internet of Things (IoT) apps and devices [5]. At this time, there are a variety of "smart house" Internet of Things (IoT) devices on the market, such as intelligent refrigerators, heating systems, gardens, video doorbells, light assistants, coffee machines, and locks. Internet of Things (IoT) devices and applications have been created for "smart city" purposes, such as smart parking, smart street lights, and smart waste management [6].

The academic community is very interested in the topic of Internet of Things security. Academics have been discussing the security of Internet of Things devices in length [7]. Data transmission, data gathering, and data security are the three primary issues with the Internet of Things (IoT),

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

despite its many benefits. There are a plethora of tracking apps designed to gather information from Internet of Things devices. Several protocols have been created and modified to allow IoT devices to communicate with existing networks and share data. Nevertheless, these protocols are not given the necessary attention. Therefore, many current and past security issues, such as identification, data protection, permission, etc., are directly associated with the IoT. There are a variety of login vulnerabilities that can lead to attacks such as replay attacks, Denning-Sacco attacks, password guessing attacks, and denial of service. However, authenticating IoT devices across interconnected and diverse networks is a formidable challenge. Issues with energy consumption, limited memory space, and computational power, as well as the constraints of IoT devices, should be taken into account by these protocols [8].

An unauthorised disclosure assault exposes private user or company information. By using it, malicious actors can gain access to sensitive data regarding people's identities, routines, and preferences. Lastly, this section provides a high-level overview of security attacks based on the Internet of Things (IoT), before going on to more in-depth analyses of individual subjects. Researchers have recently achieved great strides in automating the process of anomaly detection in sensor networks through the use of machine learning techniques [9]. But there hasn't been much effort to date in tailoring anomaly detection methods for cybersecurity applications that use interconnected sensors. As an example, [10] suggests a Bayesian classifier-based approach for smart grid anomaly detection. Also, in [11], the authors offer a way to evaluate smart grid networks' security. Researchers have also begun to analyse and categorise security attacks that target the Internet of Things [12]. There are other dangers under each of the three major categories they identified: denial of service (DoS), data tampering, and data exposure. Several requirements must be satisfied before an assault on an IoT device can be carried out successfully. The ability to identify vulnerable devices is a prerequisite. As a second point, those gadgets should have security holes that could be exploited. Thirdly, for malware to be able to speak with them, issue commands, or steal data, they need to connect via unprotected communication channels or protocols. It is crucial to remember that IoT devices can be exploited in attacks against other devices or entities, in addition to assaults against devices directly. An assault model for wireless implantable medical devices is suggested, for example, in [13]. Methods for evaluating the safety of M2M/IoT communications are laid forth in [14]. Similarly, studies analysing and categorising security attacks based on the Internet of Things have only recently begun. They classified attacks as either data modification or disclosure or denial of service (DoS). Within each group, there are distinct dangers.

In order to address the issue of denial-of-service and distributed denial-of-service assaults, the author [15] suggested a straightforward and energy-efficient attack, offered a reliable defence against nonce values, and demonstrated its efficacy through an example. With an emphasis on first-phase security detection and target identification, the writers provide a thorough overview of the literature on several authentication approaches that enhance security levels through theoretical analysis.[16-17] The importance of secure key management in ensuring long-term service support is also highlighted. Both parts of DDoS attack detection methods have seen a flurry of recent academic writing.

2. CLASSIFICATION OF IOT-BASED SECURITY ATTACKS

This research aimed to categorise the many cyber threats to the IoT according to the danger vector, target, and attack mechanism. Any illegal act done using a computer with the goal to do harm is called a cyberattack. Included in this category are instances of identity theft and denial of service attacks. The Internet of Things (IoT) refers to "smart" physical things that include software and hardware, can communicate with one another and other devices through networks, and perform tasks similar to computing. Spoofing attacks, in which an assailant pretends to be a trusted device, and denial of service (DoS) attacks are the two most prevalent types of security breaches in the Internet of Things (IoT). From intermediate gateways to end devices, spoofing attacks can target any portion of a network.

In the context of the Internet of Things, these go-betweens are typically smart hubs that link faraway objects to nearby networks. When communicating with end devices, these gateways often skip the authentication step. Consequently, further Internet of Things (IoT) endpoints linked to an intermediary device can be compromised if an attacker is able to spoof that device or devices. A man in the middle (MITM) attack is a typical term for this type of attack. In a similar vein, a malicious actor could attempt to exploit the software or hardware of a trustworthy IoT endpoint in order to pose as it. Because they enable the attacker to get around all current security mechanisms for the Internet of Things and gain direct access to data stored on the network, these assaults can have a disastrous effect. In addition, MITM attacks are difficult for Internet of Things (IoT) endpoints to identify due to their typically low power and processing capabilities. Consequently, developers should think carefully about how their products will deal with MITMs when they construct IoT

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

systems. Using rogue access points to eavesdrop is another form of spoofing attack. Typically, these malicious access points (APs) are set up in public areas where user-app authentication is not necessary. Figure 1 is the flow diagram, and specific assaults are detailed below.

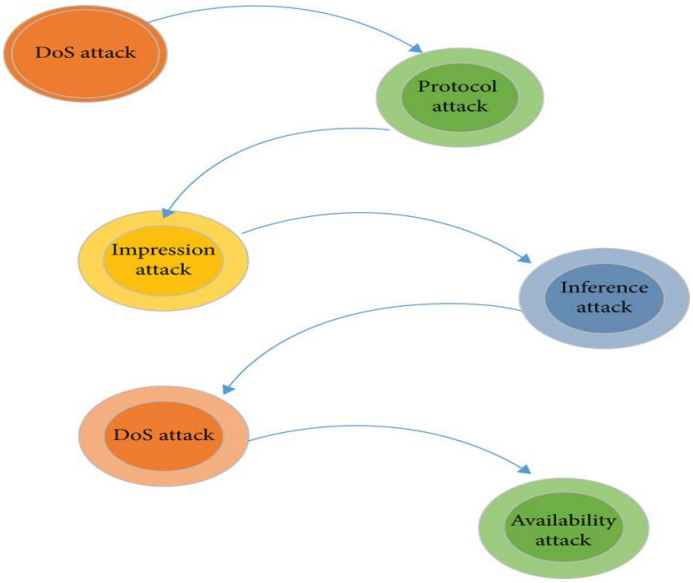

Figure 1 Classification of IoT-based security attacks.

2.1. DoS Attack

A system that allows devices to communicate wirelessly with one another or with a control system is known as the Internet of Things (IoT). If one gadget has a question, it can ask any other device for help. So, we can control the data sent and received by various Internet of Things devices. Too many connections trying to access the same device at once or an infinite stream of requests made using its insecure code can lead them to fail. In a denial-of-service (DoS) assault, an attacker floods a target device with requests until it crashes. No device can withstand this on its own. Researchers in the field of security must thus devise a means of thwarting these assaults. Additionally, they need to figure out how to keep an eye out for and identify these types of assaults. In order to gather data packets transmitted across a network, the researchers employed a number of tools, one of which being Wireshark, an open-source programme for analysing network protocols. We can examine traffic patterns and users can observe what data is being transported across networks with its help. We also make use of packet sniffers, although these cannot decode encrypted data packets that are acquired from networks. Live capture lets users record data as it travels across local area networks (LANs) or other types of computer networks in real time, while file access lets users store captured data in files for further study at a later time. Researchers were able to watch protocols being executed by various Internet-connected devices with the help of Wireshark. The next step would be to look for security holes in those protocols that would be easy for hackers to exploit. The IDA Pro Disassembler Software programme, which is part of the Hex-Rays family of products, was also utilised by the researchers. In order to identify common vulnerabilities among all sorts of IoT devices, researchers disassembled the executable scripts and examined them individually.

3. THE METHODS TO ENSURE THE SECURITY FOR IOT SOLUTIONS

Any company serious about adhering to privacy standards should use a comprehensive framework. So, as illustrated in Figure 2, the National Institute of Standards and Technology (NIST) established a cybersecurity framework based on five essential activities. With this plan, you can "Identify" potential cybersecurity threats and then "Protect" yourself by taking the necessary measures. In the "detect" phase, the cybersecurity events that have already taken place can be identified, and the "respond" phase can then implement the necessary response. With the "Recover" state, services can get restored to their original form following cybersecurity incidents.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

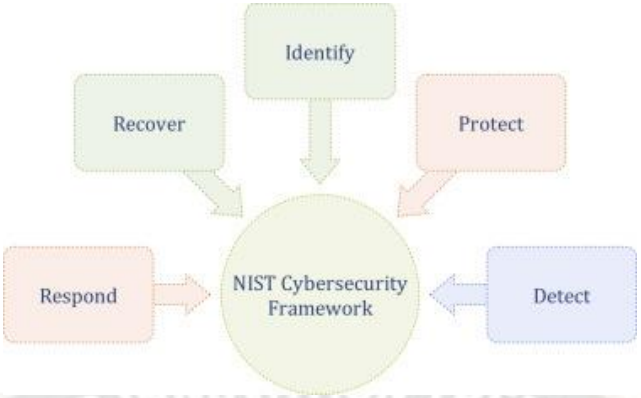

Fig. 2. The defined cybersecurity framework by NIST.

3.1. Information assurance (IA)

Information assurance (IA) is defined by the National Security Agency (NSA) as a set of rules that guarantee the data's availability, integrity, authenticity, secrecy, and non-repudiation in order to offer data security. Security services, security countermeasures, and information states are the three primary components of IA, with time serving as the fourth parameter. To aid security professionals working on Internet of Things (IoT) applications, Fig. 3 shows the primary effective parameters of the IA model.

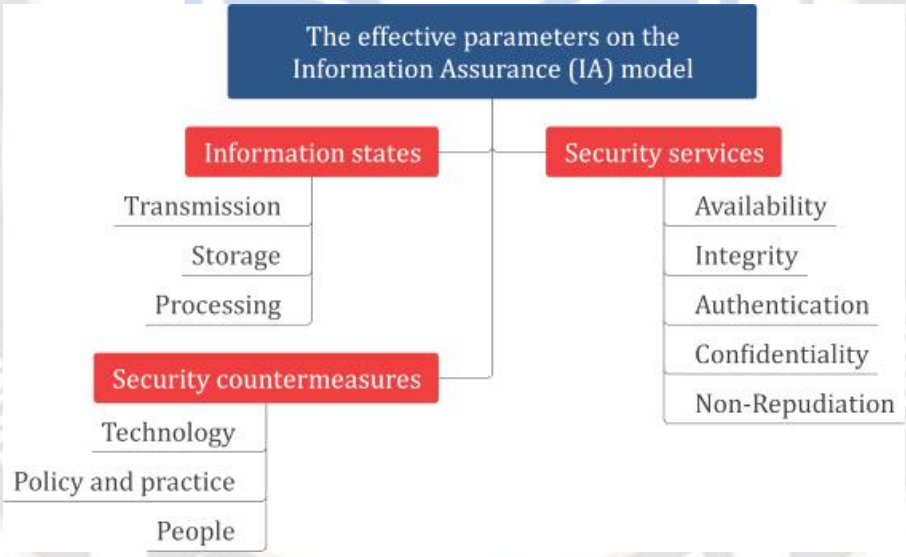

Fig. 3. A schematic of the main effective parameters in the information assurance model.

3.1.1. Security services

Fig. 3 shows that there are five primary characteristics that security services can be categorised into: non-repudiation, authenticity, availability, integrity, and confidentiality. Notably, the first three elements are known as the CIA trinity, and they deal with keeping information accessible, preventing unauthorised addition, modification, or deletion of data, and managing access to or exposure of information, respectively.

Confidentiality

This option regulates and safeguards sensitive information from outside parties. The information is more vulnerable than it would be in a wired network because wireless data transmission is the primary means of data transfer in IoT applications. An effective strategy for protecting the privacy of information is the cryptography methodology. Here, cryptographic techniques including data encryption, authentication, and access control can be employed. By

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

encoding data in an encryption way and verifying access requests using a AAA framework in an authentication and access control method, all cryptography techniques restrict unauthorised users from accessing the data.

Availability

The term "availability" refers to the prompt and dependable access that authorised parties have to data or services. Data availability is interrupted in IoT applications due to cybersecurity events, which prevents access to IoT devices. System redundancy, backups, better resilience, equipment maintenance, up-to-date software, and procedures to recover swiftly from unanticipated disasters can all contribute to making sure the information is available. High availability, defined as an agreed-upon degree of operational performance that minimises system unavailability, is crucial in IoT applications. Here, it's important to employ hot stand-by devices, redundant components, and multiple pathways to eliminate a single point of failure; provide reliable crossover with power supplies and redundant backups; and detect failures as they happen with a robust monitoring system. This will improve performance and reduce downtime.

Integrity

In every operational step, including data capture, storage, retrieval, updating, and transfer, integrity checks the data to make sure it is accurate, relevant, consistent, and reliable. Data integrity is influenced by the amount of use in an organisation and the type of information that is collected. Low, medium, high, and critical are the four primary categories of data integrity. One example of the crucial level would be the financial and healthcare records. In order to guarantee the data's reliability, it is validated, tested, and checked at this stage. Data in these organisations' databases is validated and checked to ensure reliability, so you can trust them. The employment of mid-level integrity with little verification is prevalent in online sales and search engines. Information gathered from publicly available forms makes the data unreliable at this stage. For the low level, we are also looking at personal posting sites and blogs, where the data might not be checked and where trust in the content is poor.

Authentication

The purpose of authentication is to verify that the sender, message, or individual has the right to receive specific kinds of data. Some examples of authentication mechanisms include biometric logins and passwords. Identifying and eliminating any potential authentication system constraints is essential for IA authentication.

Non-Repudiation

Sender and receiver will both receive delivery confirmation and identity verification notifications using this service. Sender will also obtain proof of delivery. To conduct error-free analysis of data transfers, IA necessitates setting up a network architecture.

4. RESULS AND DISCUSSION

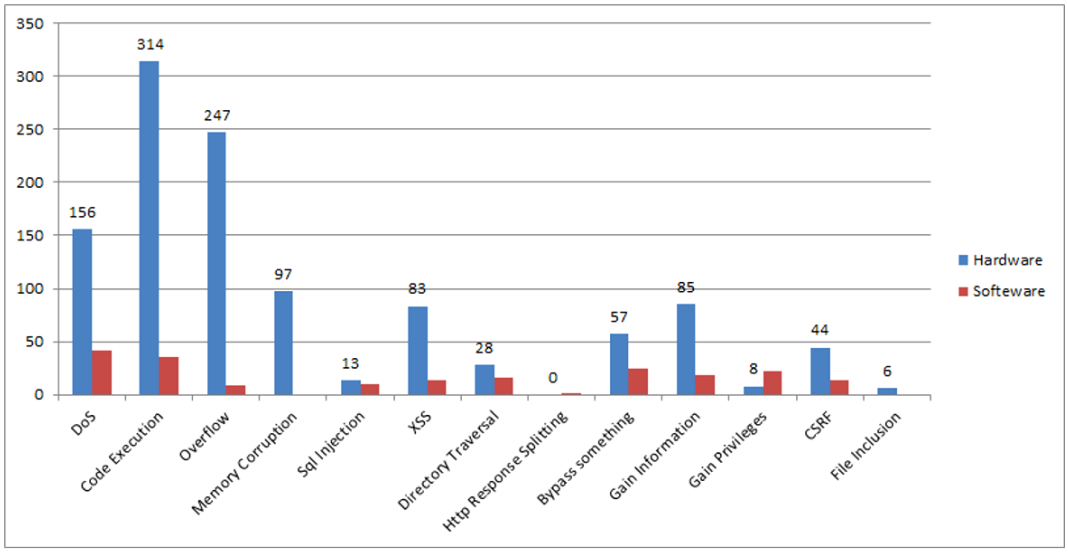

Fig 4: Number of H/W and S/W vulnerabilities of IoT devices.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

Table 1.Ratio of H/W and S/W vulnerabilities of IoT devices

	Total	**IoT device vulnerabilities**	**HW vulnerability**	**SW vulnerability**
Number of vulnerabilities	12,174	1,342	1,138 (84.8)	204 (15.2)
DoS	919	198	156 (78.8)	42 (21.2)
Code execution	2,277	349	314 (90)	35 (10)
Overflow	1,247	256	247 (96.5)	9 (3.5)
Memory corruption	296	97	97 (100)	0 (0)
SQL injection	410	23	13 (56.5)	10 (43.5)
XSS	1,593	96	83 (86.5)	13 (13.5)
Directory traversal	280	44	28 (63.6)	16 (36.4)
Http response splitting	4	1	0 (0)	1 (100)
Bypass something	495	82	57 (69.5)	25 (30.5)
Gain information	900	103	85 (82.5)	18 (17.5)
Gain privileges	129	30	8 (26.7)	22 (73.3)
CSRF	398	57	44 (77.2)	13 (22.8)
File inclusion	40	6	6 (100)	0 (0)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

After combining the two analyses of the percentage of vulnerabilities for each type of IoT device and the ratio of vulnerabilities for each type to the overall number of vulnerabilities in the IoT, we find that DoS, overflow, and memory corruption are the most often occurring vulnerabilities (Table 1, Fig. 4). One could argue that these are weaknesses that require extreme caution.

Category (Class)	# of vulnerabilities	DoS	Code execution	Overflow	Memory corruption	SQL injection	XSS	Directory traversal	HTTP response splitting	Bypass something	Gain information	Gain privileges	CSRF	File inclusion
H (home)	223(17%)	33(17%)	71(20%)	34(13%)	11(11%)	0(0%)	14(15%)	12(27%)	0(0%)	17(21%)	17(17%)	0(0%)	12(21%)	2(33%)
S (Scada)	279(21%)	37(19%)	101(29%)	72(28%)	5(5%)	0(0%)	17(18%)	6(14%)	0(0%)	9(11%)	19(18%)	4(13%)	7(12%)	2(33%)
E (enterprise)	530(39%)	104(53%)	148(42%)	49(19%)	7(7%)	17(74%)	54(56%)	20(45%)	1(100%)	33(40%)	38(37%)	21(70%)	36(63%)	2(33%)
M (mobile)	192(14%)	12(6%)	11(3%)	81(32%)	50(52%)	1(4%)	3(3%)	2(5%)	0(0%)	14(17%)	16(16%)	2(7%)	0(0%)	0(0%)
P (pc)	40(3%)	4(2%)	2(1%)	0(0%)	24(25%)	1(4%)	1(1%)	1(2%)	0(0%)	1(1%)	5(5%)	1(3%)	0(0%)	0(0%)
A (other)	78(6%)	8(4%)	16(5%)	20(8%)	0(0%)	4(17%)	7(7%)	3(7%)	0(0%)	8(10%)	8(8%)	2(7%)	2(4%)	0(0%)
Total	1342(100%)	198(100%)	349(100%)	256(100%)	97(100%)	23(100%)	96(100%)	44(100%)	1(100%)	82(100%)	103(100%)	30(100%)	57(100%)	6(100%)

1st place 2nd place

Fig 5: Frequency table by class vs. vulnerability (number of vulnerabilities by class/sum by vulnerability).

There were a total of 198 (100%) DoS vulnerabilities found, with 104 (53%) in E-class equipment and 37 (19%) in S-class rated first and second, respectively, according to Fig. 5. Out of the 349 code execution vulnerabilities, 148 (or 42% of the total) were found in E-class equipment, while 101 (or 29% of the total) were found in S-class equipment.

CONCLUSION

The importance of identifying and describing the key cybersecurity assaults in IoT devices was highlighted in the given review paper, which aimed to provide a complete source for assuring the security of IoT systems. Data stored on Internet of Things devices and their availability, confidentiality, and integrity are all jeopardised by these assaults. To that end, we mapped out every potential weak spot in the IoT reference model and provided solutions to shore up the security of connected devices and the infrastructure supporting them. It was proposed that organisations can successfully secure sensitive information, prevent cybersecurity threats, and preserve stakeholder trust in today's digital ecosystem by following the NIST framework and applying IA mechanisms to guarantee the security of the IoT solution. Blockchain technology was also proposed as an innovative area for further research and development in the field of Internet of Things (IoT) cybersecurity. Blockchain technology can cut costs, offer a resilient and transparent system, and do away with middlemen by connecting digital data using cryptographic principles and distributing them over numerous computers.

REFERENCES

1. Amin, F.; Abbasi, R.; Rehman, A.; Choi, G.S. An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks. *Sensors* **2019**, *19*, 2007. [**Google Scholar**] [**CrossRef**] [**PubMed**]
2. Patel, K.K.; Patel, S.M.; Scholar, P. Internet of things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges. *Int. J. Eng. Sci. Comput.* **2016**, *6*, 6122–6131. [**Google Scholar**]
3. Hammoudi, S.; Aliouat, Z.; Harous, S. Challenges and research directions for Internet of Things. *Telecommun. Syst.* **2018**, *67*, 367–385. [**Google Scholar**] [**CrossRef**]
4. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [**Google Scholar**] [**CrossRef**]
5. Taherdoost, H. Blockchain-Based Internet of Medical Things. *Appl. Sci.* **2023**, *13*, 1287. [**Google Scholar**] [**CrossRef**]
6. Chaudhary, S.; Johari, R.; Bhatia, R.; Gupta, K.; Bhatnagar, A. CRAIoT: Concept, review and application (s) of IoT. In Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and

Usages (IoT-SIU), Ghaziabad, India, 18–19 April 2019; pp. 1–4. [**Google Scholar**]

7. Thakor, V.A.; Razzaque, M.A.; Khandaker, M.R.A. Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access* **2021**, *9*, 28177–28193.
8. Narayanan, U.; Paul, V.; Joseph, S. Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec. *J. Ambient Intell. Humaniz. Comput.* **2021**, *13*, 769–787.
9. A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan, and M. S. Haghighi, "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4291–4300, 2021.View at: Publisher Site | Google Scholar
10. S. Shukla, S. Thakur, and J. G. Breslin, "Anomaly detection in smart grid network using FC-based blockchain model and linear SVM," *International Conference on Machine Learning, Optimization, and Data Science*, Springer, Cham, pp. 157–171, 2021.View at: Publisher Site | Google Scholar
11. A. Chehri, I. Fofana, and X. Yang, "Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence," *Sustainability*, vol. 13, no. 6, article 3196, 2021.View at: Publisher Site | Google Scholar
12. V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava, "Federated-learning-based anomaly detection for IoT security attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545–2554, 2022.View at: Publisher Site | Google Scholar
13. A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "Improving Internet of Things (IoT) security with software-defined networking (SDN)," *Computers*, vol. 9, no. 1, 2020.
14. WireShark, "Trace traffic WireShark," 2015.View at: Google Scholar
15. J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: an experimental approach," *Sensors*, vol. 20, no. 3, 2020.
16. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)
17. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D. Dissertation.University of South Alabama