Migration Letters

Volume: 21, No: 11 (202), pp. 1416-1427

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Security Attacks And Proposed Solutions In Internet Of Things (Iot)

Minahil Irfan[1], Irshad Ahmed Sumra[2*], Ijaz Ahmad Awan[3], Khalid Mahmood[4], Muhammad Aaqib Javed[5], Muhammad Akram Mujahid[6], Naheed Akhtar[7]

Abstract

IoT is one of the key areas of future research due to its real time applications for industry. IoT Applications take more attention from industry and different projects are in progress for safety of end user in smart future. Security is one of hot research area in future applications of IoT and security and privacy playing a key role for implementation of applications in real time environment and ensure the end user privacy. In this paper, we will discuss the importance of security in different types of IoT applications and discussed the security on different levels like security issues on sensing layer, on network layer, middleware layer and application layer and then provide the best solution according to the recent research of different researchers IoT security using Blockchain and security on different Attacks. Smart Home and Smart City are two major applications of IoT and end users are more concern about their privacy of data and successful implementation of IoT applications require to develop the user trust in IoT applications.

Index Terms: Security, Privacy, Trust, Applications, Blockchain, End user.

1. Introduction

[1]The Internet is connected computer networks globally with standard protocols like: (TCP/IP) to provide trillions of users around the world. As it is a network of networks that contain billions of publics, private, business, academic and government networks for both locally and globally they relate to the broad range of electronics, wireless and networking technology [1]. There is a wide range of connectivity applications in M2M like: smart cities, smart retail, smart environment, smart grid, and smart farming [2]. The Fig 1 represents the past, present and future of IoT architecture. In future, the devices cannot only connect with the internet, but can also the devices can communicate with each other through internet. Here we have the concept of SIoT is a social networking in which the user can connected with the devices and the users to share the devices along the internet [3]. The wide range of IoT application also have security and privacy issue like management issue, privacy issue, authentication issue and security issue etc. to secure the IoT environment is more challenging than to secure the IT devices.

[1,2]Department of Computer Science, Lahore Garrison University. irshadahmed@lgu.edu.pk
[3]Department of Civil Engineering, University of Engineering and Technology, Lahore, Pakistan; ijazuet@gmail.com.
[4]Department of the Information Sciences· University of Education, Lahore, Pakistan, khalid@ue.edu.pk
[5]Department of Computer Science, University of Alabama at Birmingham, Birmingham AL 35294, USA. mjaved2@uab.edu
[6]Department of the Information Sciences· University of Education, Lahore, Pakistan, akram.mujahid@ue.edu.pk
[7]Department of the Information Sciences, University of Education, Lahore, Pakistan· naheedswl@ue.edu.pk
Corresponding Author: Irshad Ahmed Sumra Email: irshadahmed@lgu.edu.pk

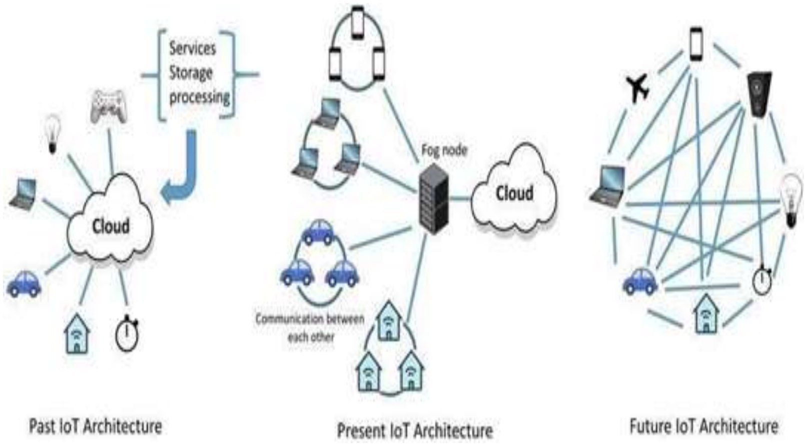

Figure 1: Present and Future of IoT [4]

Table 1: Security Comparison of IT devices and IoT devices [4]

IT Devices	IOT Devices
• Wide range of IT security. • Wide range of IT devices which are rich in resources need more care. • Wide range of IT is dependent on devices which are rich on resources • For the wide range of security and lower capabilities more complex algorithm can be implemented. • High security is maintained by homogenous technology	• Widespread of IoT security. • IoT devices can be installed with security issues. • IoT systems consists of devices that have some limitations in terms of hardware and software. • Only lightweight algorithm is considered. • Heterogenous technology with IoT can produce a large amount of heterogenous data that can increase the surface attack.

Due to all these kinds of IoT issues have different kind of cyber threats. As there is already many security and privacy attacks on the implemented IoT applications worldwide. In the last quarter of 2016, the Mirai attack was almost infected around 2.5 million devices that are connected to the internet through (DDoS) attack. After the Mirai attack the Hajimi and Reaper are another big botnet attacks against vast range of IoT devices [5]. The domain if IoT is expanded to things and objects. The successful implementation of IoT devices on human body to monitor the live the organs in human body [6]. Cyber Physical System (CPS) is a very beneficial growth of IoT that is can based on physical objects that can monitor real time environment and take decisions according to physical change. It has their own unique characteristics. In any IoT environment there are four important layers. The first layer includes the sensors and actuators that can receive the information and perform the task. The second layer consists of network to transmit data. IoT applications are considered in third layer which is middleware layer that can act as a bridge in between network and application. At last, it has the IoT based end-to-end applications like smart factories and smart transport etc. All layers consist of their own security issues and their own gateway in the data transmissions.

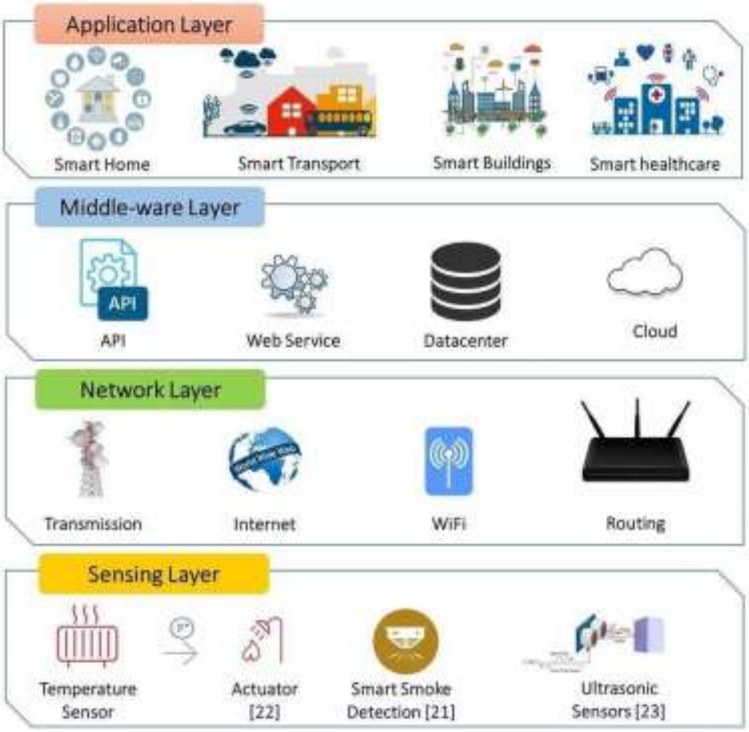

Figure 2: Layers in IoT System [4]

This paper addresses the most important procedure which to recognize and understand the type of security threats to the trust information and designing a trust management system in IoT. The Section 2, will discuss about the security threats in IoT applications with different layers' structures. The Section 3, will provide the detail analysis about the IoT Security using Blockchain technology. The proposed solutions of IoT attacks from literature will discuss in section 4 and section 5 conclude the paper.

2. Security Threats in IoT Applications

IoT applications are divided into four different layers [4]:

A. Sensing layer
B. Network layer
C. Middle ware layer
D. Application layer

Each layer has their own security issues that can be discuss as below:

A. Security Issues at Sensing Layer

This layer deals with the sensor and the actuators. Sensors can sense the environment and actuator can perform certain actions. Sensors like camera sensor, ultrasonic sensor, temperature and humidity [7]-[9]. Various layer can use various IoT technologies Like: RFID, RSNs, WSNs, GPS. Main security threats that can experience at the sensing layer are the following:

1. Node Capturing
2. Malicious Code Injection Attack
3. Wrong Data Injection Attack
4. Side-Channel Attacks (SCA)

5. Eavesdropping and Interference
6. Sleep Deviation Attack
7. Booting Attacks

B. Security Issues at Network Layer

The main function of network layer is to send the information that can be received form the sensing layer to CPU. The main security issues that can be occurred in the network layer are as follow:

1. Phishing Site Attack
2. Access Attack
3. DDoS/DoS Attack
4. Data Transmit Attack
5. Routing Attacks

C. Security Issues at the Middleware Layer

The main function of middle ware in IoT is to create an abstraction in between network layer and application layer. It can also provide storage capabilities [10]. The following attacks can take control the entire IoT application when infected the middle ware layer. Database and cloud security are the other main issue occurred in the middleware layer. The following are the attacks:

1. Man-in-the-Middle Attack
2. SQL Injection Attack
3. Signature Wrapping Attack
4. Cloud Malware Attack
5. Flooding Attack in Cloud

Security Issues at Gateway

The Gateway is a very board layer that plays an important role to connect device, things, people, and services of cloud. Gateway is very helpful that it can provide solutions of hardware and software in IoT devices. It can also use for encrypting and decrypting IoT data and translate protocols for the communication in between different layers [11]. The security issues of Gateway are as follow:

1. Secure On-Boarding
2. Extra Interface
3. End-to-End Encryption
4. Firmware Updates

D. Security Issues at Application Layer

The Application Layer deals and provide services to the user. The applications like smart grid. Smart cities, smart home etc. These smart things are specific to this layer. This layer has their own security issues that is not in any other layer like theft of data and privacy issues. The following are the security issues of application layer.

1. Data Theft
2. Access Control Attacks
3. Service Interruption Attacks
4. Malicious Code Injection Code
5. Sniffing Attacks
6. Reprogram Attacks

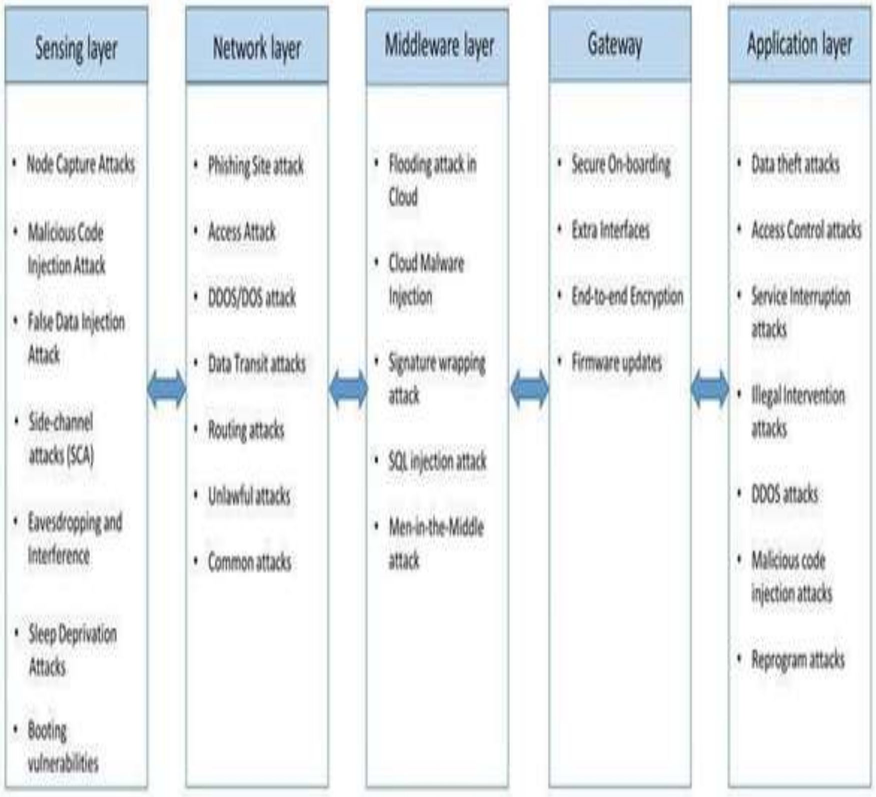

Figure 3: Types of Attacks on IoT [4]

The most challenging field before any research in study is to identify the related recent study and proposed the new idea for need in that research [65]. Table 3 represents the related research by different authors.

Table 2: Survey on Security Aspects of IoT

Research Paper	Trust	Security Requirements	Privacy	Methodology
Atzori et al [24]		Integrity And authentication	□	
Weber [25]		Resilience to attack, authentication	□	Legislation based
Heer et al [26]			□	Bootstrapping and operational phase through IP-based security
Miorandi et al [27]	□	The Confidentiality	□	
Roman et al [28]	□	Access control, identity, and authentication	□	
Riahi et al [29,30]	□	Authentication and identification	□	Based on systematic approach
Yan et al [31]	□			8 taxonomies based on trust management
Sadeghi et al [32]		CIA		

Granjal et al [33]		Nonrepudiation and CIA		Communication based
Farooq et al [34]		Authentication and CIA	□	4 architectural layers based
Sicari et al [35]	□	Confidentiality, authentication, and AC	□	
Nguyen et al [36]		Integrity, authorization, Confidentiality, authentication, and freshness	□	Security based on life of bootstrapping phase
Alaba et al [37]	□	Exhaustion of resources, authentication and authorization	□	Application based
Yang et al [38]		Access control and authentication	□	4 architectural layers based
Fremantle and Scott [39]	□	Access control, Authentication and CIA	□	3 aspects based (hardware, network, cloud/server)
Mosenia and JHA [40]			□	Vulnerabilities on (edge computing, communication, and edge nodes)
Lin et al [41]	□		□	3 layers based
Mendez et al [42]	□	CIA, authentication, and access control	□	3 layers based
Zarpelo et al [43]			□	Taxonomies in intrusion detection
Ferrang et al [44]	□	Authentication	□	4 environment authentications (IoS, IoV, M2M and IoE)
Ammar et al [45]		Access control, authentication, and secure communication		Frameworks for each IoT
Kouicem et al [46]	□	Availability, CIA, and non-repudiation	□	Each based on application
Sfar et al [47]	□	Access control and identification	□	
Hassija et al [48]			□	Security like: (ML, fog, edge and blockchain)
Farris et al [49]		Authorization and authentication	□	Security like: (NFV and SDN)

3. IoT Using Blockchain Technology

As Blockchain and IoT has a great impact on Its industry. IoT is focused on how sensors can work and Blockchain can focus on the security of data by using distributed, ledger shared and decentralization [12]. The idea behind Blockchain is a distributed ledger (also known as duplicated log files). The data in Blockchain is time-stamped and chronological. Each entry relates to the previous using cryptographic Hash Algorithms. A Merkle tree can store single transaction and in blockchain the root hash tree is stored. New hash root is generated as the hash child nodes are concatenated with it. The resultant root hash is stored on blockchain (e.g., H1 and H2.). The hash root can verify that the securely transaction can be held. Whole side will be affected or changed even if the individual transaction is change. The ledger that can maintain the minor verification can maintain the log files and transaction and can generate a unique key that enables a last transaction to be the part of ledger. Through this process the data is present in the nodes of the network. Presence of cryptographic hash keys in every block, it is difficult and time-consuming to tamper each block [13].

Benefits of Blockchain in IoT

The use of Blockchain has many benefits in IoT applications. The following are the benefits blockchain.

1. Data coming from IoT devices can be stored in Blockchain
2. Distributed nature of blockchain allowing secure data storage
3. Data encryption using the hash key and verified by miners
4. Prevention from data loss and spoofing attacks
5. Blockchain to prevent unauthorized access
6. Proxy based architecture in blockchain for resource constrained devices
7. Elimination of centralized cloud servers

Table.3 shows the challenges and the possible solution in blockchain.

Table 3: Challenges in IoT and Possible Blockchain Solution [4]

Challenges towards IoT	**Specification**	**Possible Blockchain Solution**
Privacy in IoTdevices	IoT devices are vulnerable to expose the private data of user	To address a challenge, give solution using Permissioned Blockchain that is secure to IoT devices [14-16].
Traffic and Cost	It can handle exponential growth in IoT devices	Decentralization in blockchain, the devices can automatically connect and communicate each other with other devices [2][17][18].
Service insufficiency on cloud service due to heavy load	Unavailability of cloud services due to attacks, errors in software and many other problems	The record of data must be saved at the different nodes of network. So, at the time of failure the data will not affected [19][20].
Defective Architecture	Some part of IoT devices have point of failure that affect the whole device	Validation is necessary in blockchain. So, that it may confirm that the data will be send from only one source [21].
Data Manipulation	The data that can be manipulated from the IoT devices used in very inappropriate way after manipulation.	In blockchain, the devices are interconnected. If one device wants to update the data. The system should not allow it and also reject it [22][23].

4. Attacks and Their Proposed Solutions

Today most vastly spreading the field is Internet of Things (IoT). Many researchers want to look forward the future through Internet of Things (IoT). Now many advancements have been made in this field but there are some attacks that can harm your system and as some severe effects on it. Now many counter measures have been taken to prevent your system from these types of attacks before implementation commercially [66]. The number of technologies that is used today made the device in risk. In this paper we have discussed different technology with their required proposed solution by different researchers [67]. In 2006 Peng et al [50] discussed the routing attack and provide the solution accordingly like to prevent the Routing Attack: Ad hoc On-demand Distance Vector (AODC) and Dynamic Source Routing (DSR). In 2011 Simmons et al [51] discussed the Booting Attack and provide the solution accordingly like to prevent the Booting Attack: Loop-Amnesia's countermeasure of an attack and A register-based architecture. In 2014 Latif et al [52] discussed the Flooding Attack and provide the solution accordingly like to prevent the Flooding Attack: In cloud system all the servers are organized to form a group of fleets of the servers. In Patil et al [53] discussed DoS Attack and provide the solution accordingly like to prevent the DoS: Real time Intrusion detection model and Fuzzy logic can be used to identify the reason of an attack. In 2016 Aweke et al [54] discussed Malicious Code Injection Attack and provide the solution accordingly like to prevent the Malicious Code Injection Attack: ANVIL detect all row hammer attack by tracking the location of DRAM rows. In 2019 Maunero et al [55] discussed Service Interruption Attack and provide the solution accordingly like to prevent the Service Interruption Attack: To analysis the Control Flow Integrity, they focus on the dichotomy that show the unexpected behavior. In 2020 Ahmad et al [56] discussed Man in the Middle Attack and provide the solution accordingly like to prevent the Man in the Middle Attack: MARINE a trusted model is implemented between connected devices that Identifies the suspicious nodes. In Jemal et al [57] discussed SQL Injection Attack and provide the solution accordingly like to prevent the SQL Injection Attack different methods can be used: Ontology based SQLI, Machine Learning based and Query model. Many other attacks with their provided solution have been discussed in Table 4.

Table 4: Attacks and Their Solutions

Year	**Authors**	**Attacks**	**Proposed Solution**
2006	Peng et al [50]	Routing Attack	To prevent the Routing Attack: • Ad hoc On-demand Distance Vector (AODC) and Dynamic Source Routing (DSR)
2011	Simmons et al [51]	Booting Attack	To prevent the Booting Attack: • Loop-Amnesia's countermeasure of an attack • A register-based architecture
2014	Latif et al [52]	Flooding Attack	To prevent the Flooding Attack: • In cloud system all the servers are organized to form a group of fleets of the servers.
2016	Patil et al [53]	DOS Attack	To prevent the DoS: • Real time Intrusion detection model • Fuzzy logic can be used to identify the reason of an attack.
2016	Aweke et al [54]	Malicious Code Injection	To prevent the Malicious Code Injection Attack:

		Attack	• ANVIL detect all row hammer attack by tracking the location of DRAM rows.
2019	Maunero et al [55]	Service Interruption Attack	To prevent the Service Interruption Attack: • To analysis the Control Flow Integrity, they focus on the dichotomy that show the unexpected behavior
2020	Ahmad et al [56]	Man in the Middle Attack	To prevent the Man in the Middle Attack: • MARINE a trusted model is implemented between connected devices • Identifies the suspicious nodes
2020	Jemal et al [57]	SQL Injection Attack	To prevent the SQL Injection Attack different methods can be used: • Ontology based SQLI • Machine Learning based • Query model
2020	Geetha et al [58]	Cloud Malware Attack	To prevent the Cloud Malware Attack: • Network level security • Host level security
2020	Schwenk et al [59]	End-to-end Encryption	To prevent the End-to-end Encryption: • Thunderbird and Eni Gmail can be used for the decryption of the text
2021	Shankaranarayanan H et al [60]	Eavesdropping and Interference	To prevent the Eavesdropping and Interference • Adaptive Fuzzy logic Controller (AFLC) used in Field Programmable Gate Array (FPGA) for implementation and designing
2021	Turhanlar et al [61]	Phishing Attack	To prevent the Phishing Attack • Natural Language Processing (NLP) can be used for the detection of the phishing attack
2021	Modak et al [62]	Signature Wrapping Attack	To prevent the Signature Wrapping Attack: • Xpath expression • ID referencing
2021	Angappan et al [63]	Reprogrammable Attack	To prevent the Reprogrammable Attack: • Noval Sybil Attack detection protocol (NoSad)
2022	Ng et al [64]	Side Channel Attacks	To prevent the side channel attacks: • Field Programmable Gate Array FPGA based Advanced Encryption Standard AES accelerator • Most effective design for security.

5. Conclusion

On edge devices of cloud computing there is more theft of attack. The gateway must be secure in any network as it is an entry and exit point of any network. End -to end encryption is needed for the safety of data. The current architecture of blockchain is limited to some specific number of computers. In this survey paper, we discussed about different layers on IoT security that is sensing layer, network layer, middleware layer, gateway layer and application layer and discussed the proposed solutions of different IoT attacks from the best solutions given by different authors. It is necessary for successful implementation of IoT applications to develop end user Trust and data privacy in real environment.

References

[1] Nunberg, G. (2012) The Advent of the Internet: 12th April, Courses. reference/ReferencesPapers.aspx?ReferenceID=14 82944

[2] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," IEEE Access, vol. 6, pp. 32 979–33 001, 2018.

[3] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the iot world: present and future challenges," IEEE Internet of Things Journal, vol. 5, no. 4 pp. 2483– 2495, 2018.

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

[5] Flashpoint, "Mirai Botnet Linked to Dyn DNS DDoS Attacks," December. 18 ,2018.

[6] G. Yang, M. Jiang, W. Ouyang, G. Ji, H. Xie, A.M. Rahmani, P. Liljeberg, and H. Tenhunen, "Iot- based remote pain monitoring system: From device to cloud platform," https://ieeexplore.ieee.org/document/8118086 IEEE journal of biomedical and health informatics, vol. 22, no. 6, pp. 1711–1719, 2018.

[7] Bridgera, "IoT System | Sensors and Actuators," online;accessed 09 February 2019.

[8] Smarthomeblog, "How to make your smoke detector smarter,", online;accessed 10 Feburary 2019.

[9] Tictecbell, "Sensor d'ultrasons,", online;accessed 11 Feburary 2019.

[10] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "A survey of middleware for internet of things," in Recent trends in wireless and mobile networks. Springer, 2011, pp. 288–296.

[11] C. Fife, "Securing the IoT Gateway,", online; accessed 09 Feburary 2019.

[12] H. Orman, "Blockchain: The emperors new pki?" IEEE Internet Computing,vol. 22, no. 2, pp. 23– 28, 2018.

[13] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," IEEE Internet of Things Journal, vol. 5, no. 2, pp.1184– 1195, April 2018.

[14] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," IEEE Internet of Things Journal, vol. 5, no. 2, pp.1184– 1195, April 2018.

[15] P. Lv, L. Wang, H. Zhu, W. Deng, and L. Gu, "An iot-oriented privacy preserving publish/subscribe model over blockchains," IEEE Access, vol. 7, pp. 41 309–41 314, Jan 2019.

[16] U. Javaid, M. N. Aman, and B. Sikdar, "Blockpro: Blockchain based data provenance and integrity for secure iot environments," in Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. ACM, 2018, pp. 13–18.

[17] K. Valtanen, J. Backman, and S. Yrjölä, "Blockchain-powered value creation in the 5g and smart grid use cases," IEEE Access, vol. 7, pp. 25 690–25 707, Feb 2019.

[18] [102] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, "Mitigating lot device based ddos attacks using blockchain," in Proceedings of the 1stWorkshop on Cryptocurrencies and Blockchains for Distributed Systems. ACM, 2018, pp. 71–76.

[19] K. R. Ozyilmaz and A. Yurdakul, "Designing a blockchain-based iot with ethereum, swarm, and lora: The software solution to create high availability with minimal security risks," IEEE Consumer Electronics Magazine, vol. 8, no. 2, pp. 28–34, March 2019.

[20] [104] V. Sharma, "An energy-efficient transaction model for the blockchainenabled internet of vehicles (iov)," IEEE Communications Letters, vol. 23, no. 2, pp. 246–249, Feb 2019.

[21] P. K. Sharma, M. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," IEEE Access, vol. 6, pp. 115–124, Mar 2018.

[22] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain- based solutions to security and privacy issues in internet of things: a survey. Comput. Network. 54 (15), 2787–2805, [Online]. Available.

[23] Weber, R.H., 2010. Internet of thingsnew security and privacy challenges. Comput. Law Secur. Rep. 26 (1), 23–30.

[24] Heer, T., Morchon, O.G., Hummen, R., Keoh, S.L., Kumar, S.S., Wehrle, K., 2011. Security challenges in the ip-based internet of things. Wireless Pers. Commun. 61 (3), 527–542, [Online]. Available.

[25] Miorandi, D., Sicari, S., Pellegrini, F.D., Chlamtac, I., 2012. Internet of things: vision, applications and research challenges. Ad Hoc Netw. 10 (7), 1497–1516 [Online]. Available.

[26] Roman, R., Zhou, J., Lpez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Comput. Network. 57 (10), 2266–2279, [Online]. Available.

[27] Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., Bouabdallah, A., 2013. A systemic approach for iot security. In: IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS 2013, Cambridge, MA, USA, May 20-23, 2013, pp. 351–355, [Online]. Available.

[28] Riahi, A., Natalizio, E., Challal, Y., Mitton, N., Iera, A., 2014. A systemic and cognitive approach for iot security. In: International Conference on Computing, Networking and Communications, ICNC 2014, Honolulu, HI, USA, February 3-6, 2014, pp. 183–188, [Online]. Available.

[29] Yan, Z., Zhang, P., Vasilakos, A.V., 2014. A survey on trust management for internet of things. J. Netw. Comput. Appl. 42, 120–134, [Online]. Available.

[30] Sadeghi, A., Wachsmann, C., Waidner, M., 2015. Security and privacy challenges in industrial internet of things. pp. 54:154:6. In: Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, June 7-11, 2015 [Online]. Available.

[31] 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 and Tutorials 17 (3), 1294–1312, [Online]. Available.

[32] Farooq, M.U., Waseem, M., Khairi, A., Mazhar, S., 2015. A critical analysis on the security concerns of internet of things (iot). In: the internet of things," IEEE Wireless Communications, vol. 25, no. 6, pp. 12–18, December 2018.

[33] U. Javaid, M. N. Aman, and B. Sikdar, "Drivman: Driving trust management and data sharing in vanets with blockchain and smart contracts," in Proceedings of IEEE Vehicular Technology Conference. IEEE, 2019, pp. 1–6.

[34] Atzori, L., Iera, A., Morabito, G., 2010. The International Journal of Computer Applications, vol. 111, no. 7.

[35] Sicari, S., Rizzardi, A., Grieco, L.A., Coen- Porisini, A., 2015. Security, privacy and trust in internet of things: the road ahead. Comput. Network. 76, 146–164, [Online]. Available.

[36] Nguyen, K.T., Laurent, M., Oualha, N., 2015. Survey on secure communication protocol for the internet of things. Ad Hoc Netw. 32, 17–31, [Online]. Available.

[37] Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F., 2017. Internet of things security: a survey. J. Netw. Comput. Appl. 88, 10–28, [Online]. Available.

[38] Yang, Y., Wu, L., Yin, G., Li, L., Zhao, H., 2017. A survey on security and privacy issues in internet- of-things. IEEE Internet of Things J. 4 (5), 1250– 1258, [Online]. Available.

[39] Fremantle, P., Scott, P., 2017. A survey of secure middleware for the internet of things. PeerJ Comp. Sci. 3, e114, [Online]. Available.

[40] Mosenia, A., Jha, N.K., 2017. A comprehensive study of security of internet-of-things.IEEE Trans. Emerg. Top. Comput. 5 (4), 586–602, [Online]. Available.

[41] 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 J. 4 (5), 1125–1142, [Online]. Available.

[42] Mendez, D.M., Papapanagiotou, I., Yang, B., 2017. Internet of things: survey on security and privacy. vol. abs/1707.01879 CoRR. [Online]. Available

[43] Zarpelo, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C., 2017. A survey of intrusion detection in internet of things. J. Netw. Comput. Appl. 84, 25–37,[Online]. Available.

[44] Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L., 2017. Authentication protocols for internet of things: a comprehensive survey. pp. 6562953:16562953 Secur. Commun. Network. 2017 (41), [Online]. Available.

[45] Ammar, M., Russello, G., Crispo, B., 2018. Internet of things: a survey on the security of iot frameworks. J. Inf. Sec. Appl. 38, 8–27, [Online]. Available.

[46] Kouicem, D.E., Bouabdallah, A., Lakhlef, H., 2018. Internet of things security: a top-down survey. Comput. Network. 141, 199–221, [Online]. Available.

[47] Sfar, A.R., Natalizio, E., Challal, Y., Chtourou, Z., 2018. A roadmap for security challenges in the internet of things. Digit. Commun. Netw. 4 (2), 118–137.

[48] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B., 2019. A survey on iot security: application areas, security threats, and solution architectures. IEEE Access7, 82721– 82743, [Online]Available.

[49] Farris, I., Taleb, T., Khettab, Y., Song, J., 2019. A survey on emerging SDN and NFV security mechanisms for iot systems. IEEE Communications Surveys and Tutorials 21 (1), 812–837, [Online]. Available.

[50] Peng, G., & Chuanyun, Z. (2006, November). Routing attacks and solutions in mobile ad hoc networks. In 2006 International Conference on Communication Technology (pp. 1-4). IEEE.

[51] Simmons, P. (2011, December). Security through amnesia: a software-based solution to the cold boot attack on disk encryption. In Proceedings of the 27th Annual Computer Security Applications Conference (pp. 73-82).

[52] Latif, R., Abbas, H., & Assar, S. (2014). Distributed denial of service (DDoS) attack in cloud-assisted wireless body area networks: a systematic literature review. Journal of medical systems, 38(11), 1-10.

[53] Patil, S., & Chaudhari, S. (2016). DoS attack prevention technique in wireless sensor networks. Procedia Computer Science, 79, 715- 721.

[54] Aweke, Z. B., Yitbarek, S. F., Qiao, R., Das, R., Hicks, M., Oren, Y., & Austin, T. (2016). ANVIL: Software-based protection against next-generation rowhammer attacks. ACM SIGPLAN Notices, 51(4), 743-755.

[55] Maunero, N., Prinetto, P., & Roascio, G. (2019, September). Cfi: Control flow integrity or control flow interruption? In 2019 IEEE East-West Design & Test Symposium (EWDTS) (pp. 1-6). IEEE.

[56] Ahmad, F., Kurugollu, F., Adnane, A., Hussain, R., & Hussain, F. (2020). MARINE: Man-in-the- middle attack resistant trust model in connected vehicles. IEEE Internet of Things Journal, 7(4), 3310-3322.

[57] Jemal, I., Cheikhrouhou, O., Hamam, H., & Mahfoudhi, A. (2020). Sql injection attack detection and prevention techniques using machine learning. International Journal of Applied Engineering Research, 15(6), 569-580.

[58] Geetha, R., Suntheya, A. K., & Srikanth, G. U. (2020). Cloud integrated IoT enabled sensor network security: research issues and solutions. Wireless Personal Communications, 113(2), 747-771.

[59] Schwenk, J., Brinkmann, M., Poddebniak, D., Müller, J., Somorovsky, J., & Schinzel, S. (2020, October). Mitigation of attacks on email end-to- end encryption. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (pp. 1647-1664).

[60] Shankaranarayanan, H. (2021, July). Digital Design of Fuzzy Logic Controller for Optical Beam Steering in Free Space Optical Communication. In 2021 International Conference on System, Computation, Automation and Networking (ICSCAN) (pp. 1-5). IEEE.

[61] Turhanlar, M., & Acartürk, C. (2021). Detecting Turkish Phishing Attack with Machine Learning Algorithm.

[62] Modak, S., Majumder, K., & De, D. (2021). Vulnerability of Cloud: Analysis of XML Signature Wrapping Attack and Countermeasures. In Proceedings of International Conference on Frontiers in Computing and Systems (pp. 755- 765). Springer, Singapore.

[63] Angappan, A., Saravanabava, T. P., Sakthivel, P., & Vishvaksenan, K. S. (2021). Novel Sybil attack detection using RSSI and neighbour information to ensure secure communication in WSN. Journal of Ambient Intelligence and Humanized Computing, 12(6), 6567-6578.

[64] Ng, J. S., Chen, J., Chong, K. S., Chang, J. S., & Gwee, B. H. (2022). A Highly Secure FPGA- Based Dual-Hiding Asynchronous-Logic AES Accelerator Against Side-Channel Attacks. IEEE Transactions on Very Large Scale Integration (VLSI) Systems.

[65] S. Marcos-Pablos, A. Garc´ıa-Holgado, and F. J. Garc´ıa-Peñalvo, Guidelines for Performing Systematic Research Projects Reviews, 2020.

[66] Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: A survey. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 32-37). IEEE.

[67] Liang, X., & Kim, Y. (2021, January). A survey on security attacks and solutions in the IoT network. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0853-0859). IEEE.