Research Article

A Comprehensive Survey of Internet of Things Security Challenges and possible Solutions

Shouq M. Alnemari[1], Mohammed A. AlZain[1], Mehedi Masud[1,*], NZ Jhanjhi[2], Jehad Al-Amri[1], Mohammed Baz[1]

[1]College of Computers and Information Technology, Taif University,
P.O. Box 11099, Al-Hawiya-Taif, 21944, Saudi Arabia
[2]School of Computer Science and Engineering, SCE, Taylor's University, 47500, Malaysia

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract

The Internet of Things (IoT) is considered as one of the greatest significant fields of future technology. It is aimed to join anyone with anything at anywhere. IoT will play a critical role and will change our ways of life, aspirations, and business models. It is vulnerable to numerous security threats. IoT security should move towards in perceiving threats and reacting to attacks.

In this research we intent to surveys recent research in the field of IoT security. Another goal of this work is to promote IoT security solutions to reduce security risks that affect IoT users.

Keywords: Internet of things, Security, Dos, Attacks, Applications.

1. Introduction

IoT consider a group of several interconnected objects, services, humans and devices that can interact, exchange information in various areas and applications to achieve a common purpose [1]. IoT makes a major contribution to improving our everyday lives through a lot of applications in many sectors, like smart cities, smart grids, smart homes, healthcare, industrial manufacturing and so on. The issue of protection and privacy comes with all this vast spectrum of IoT applications. IoT technologies cannot achieve high demand and can lose all their potential without a trusted ecosystem[2],[3]. Since the IoT consists of various network- connected devices the responsibility of protecting data privacy also handling security issues like MITM attacks, spoofing attacks, (DoS) attacks, jamming, eavesdropping and malware. This paper focuses on the issues related to the data security domains of IoT with the discussion of security solutions to reduce security risks that affect IoT users.

The rest of this paper is structured as follows. Section 2 represents the related work. Section 3 presents IoT applications. Section 4 denotes IoT attacks. Section 5 discusses IoT solutions. Section 6 analyses IoT technologies. Section 7 presents conclusion of this research.

2. Background

IoT security objectives for information and information systems, such as privacy[4], authentication, non-repudiation, accessibility, and privacy, will be addressed. IoT is a technology that is currently being built at a different stage and needs further upgrades. IoT architecture is represented in detail in [5]. They define three IoT architecture layers. Although it adds another layer in papers i.e., the layer of middleware whose jobs are service control, data stored in the database from the network layer, etc. Changing the layer and its flaws do not allow much improvement in IoT technology [5]. Various flaws and potential IoT attacks are clarified in [1]. Assaults are divided into four classes depending on the flaw used in the attack by the opponent. Describes potential attacks on an OSI layer. Concentrate on IoT device security challenges; much of these documents, however, only discuss categories of risks based on specific security targets. Categories of risks based on specific security targets. There are no such rigorous approaches suggested that can address most IoT security problems. In last few years, a little paper represents the numerous problems with common IoT solutions [6].

The IoT is seen as the world's future. Several IoT-based technologies, such as building structural protection, waste control, air quality, noise detection, traffic pollution, urban energy use, smart lighting, etc. have been suggested. The paper [7] related to a list of IoT technologies [8] and their contributions to society. Sees applications can help to utilize capital quickly and easily.

3. IoT Applications

This section will discuss the IoT applications for instance healthcare, smart grids, smart cities, smart homes, and industrial applications.

3.1 Smart Homes

Domotics or Home automation using a centralized hub a smart phone to control various things as discussed in [9], things such as air conditioner, smart television, lights, etc.

3.2 Smart Cities

A multidisciplinary concept not only information technologies infrastructure Smart City clarify the management of information and resources to achieve improvement of people lives. As [10] say the technology consider the main key factor in Smart City, presenting many operations such as sensor, control, monitor and communication in services such as environment control, emergencies, social, crime control, electricity etc.

3.3 Healthcare

Healthcare in IOT or (H-IOT) all devices used in bedsides monitoring, fitness tracker, smartwatches etc. Every object send data, monitor, control, or communicate in healthcare[11],[12] field using sensor depend on IOT consider a (H-IOT).

4. Attacks of IoT

Normally, IoT devices are connected through wireless networks where an attacker would be able to expose private information. In this section will discuss IoT attacks[13],[14],[15] which cause weaknesses in a system and exerts a negative impact on it [16]. As show in Fig. 1.

4.1 Physical Attacks

This type of attacks focuses on Perception Layer aim to physically breach the network and divide into seven types:

- Tampering

Modifying network components such as modify RFID (Radio Frequency Identification) or Alter communication links [5].

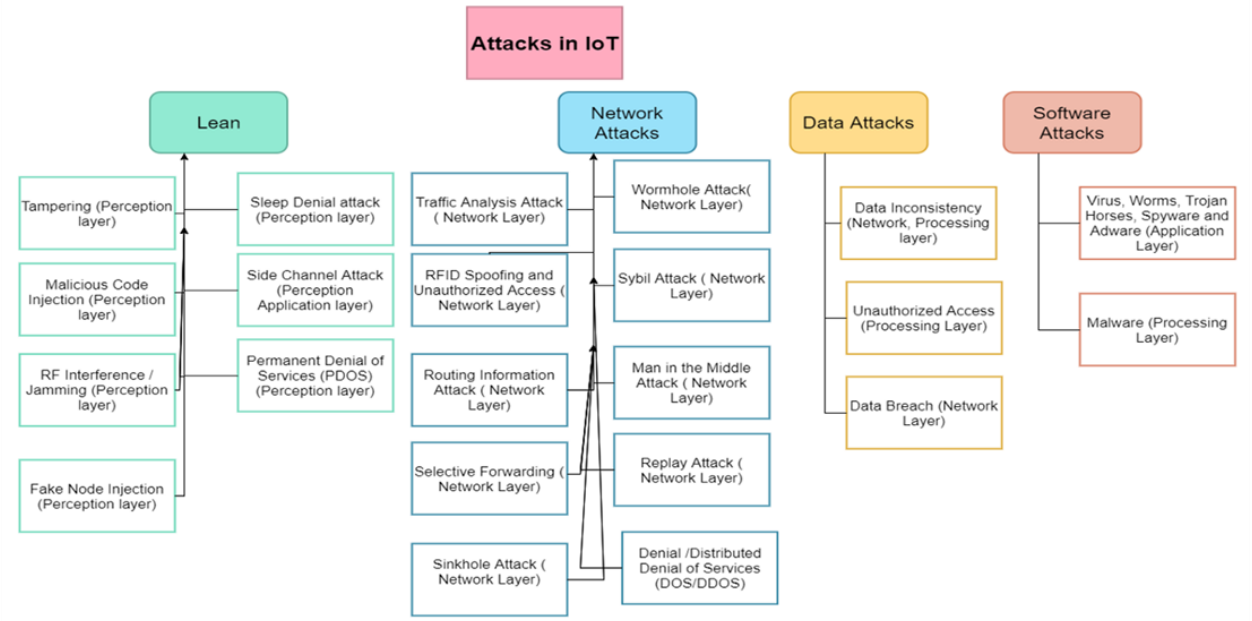

Fig. 1 Attacks in IoT

- Malicious Code Injection

Inserting Malicious code physically by alter the existing code in node to compromise other nodes.

- RF Interference /Jamming

Sending noise signal over RF/WSN to achieve DOS attack in RFID to prevent legal communications [17].

- Fake Node Injection

Drop fake node in network to gain unauthorized monitoring [17].

- Sleep Denial Attack

In this attack, attacker feed wrong value in battery power to keep it work to exhaust and caused shutdown [17].

- Side Channel Attack

This attack done by collecting encryption keys by applying fault attack, timing and power modification to breach the confidentiality by knowing the keys to encrypt/decrypt data [5].

- Permanent Denial of Services (PDOS)

Consider a DOS attack, but in this attack, attacker aim to damage IOT devices by launching the devices duo to destroying it firmware or using malware and upload it to corrupt devices BIOS [1].

4.2 Networks Attacks

This type of attack takes place in the network layer where the attacker aims to manipulate to cause damage. In this type, attacks happened far from existing close to the network in another word no need for physical interfered.

- Traffic Analysis Attack

The attacker aims to sniff the data to breach confidentiality or disclosed data. There is not any need to being closed to the network [16].

- RFID Spoofing and Unauthorized Access

In this attack, the attacker spoof RFID signal by using the original tag ID, then posing modified data as valid data [17].

- RFID Unauthorized Access

The ability of the attacker to breach data exist in RFID node duo to the lake in authentication mechanism [5].

- Routing Information Attack

Spoofing or altering routing information by the attacker by direct modify routing information. This type of attack presented in activities like routing loop or sending error messages.

- Selective Forwarding

Modify node maliciously by drop, alter, or selectively to forward malicious messages to interfered information and depraved information from reaching the destination [18].

- Sinkhole Attack

This attack exploits the attacker with a narrow node in sink node and modifies it so that the sink node is imitated by network traffic [18].

- Wormhole Attack

A low-latency attacker establishes a tunnel packet connection [18].

- Sybil Attack

Malicious node claims multiple identifies to locate itself in multi-location causing huge resource allocation [17].

- Man in the Middle Attack

Eavesdrop the communication by mimic a legitimate party between to nodes [16].

- Replay Attack

Another face of DOS, where the attacker captures a signed packet and resend it multiple time to keep the network busy [17].

- Denial/Distributed Denial of Service (DOS/DDOS) Attack

The same as Dos Attack, in this attack the attacker aim to slow down the system or crash it [16].

4.3 Software Attacks

This type of attack happened in application, perception layers. Meaning in software vulnerabilities or system limitations.

- Virus, Worm, Trojan Horses, Spyware, and Adware

Using this malicious software by the attacker aims to manipulating data, data (information) stealing, or even causing DOS attack [18].

- Malware

  Malware, which may contaminate the server or commercial records center, can influence data present in IoT devices.

4.4 Data Attacks

Each attack aims to modify data called Data Attack, these types of attack exist in network, processing layers

- Data Inconsistency

In IoT, Data Inconsistency is referred to as the intrusion on integrity the reason behind that is the inconsistency of data during the transmission process or storing data in a central database.

- Unauthorized Access

Access control means giving authorized users access and denying unauthorized user's access. This means malicious intent may have the ability to gain ownership rights over data or breach sensitivity.

- Data Breach

Infringement of data or memory leakage defined as the unauthorized withdrawal of private, sensitive and personal data [16].

5. IoT Security Solution

Security subject is one problem in IoT. To date, a variety of proposals aimed at resolve IoT security issues have been made. In this section, will discuss some security solutions and technologies in IoT. As shown in Table 1 we classify the Attacks and its Effects on the IoT network, then we mention the perfect countermeasures to handle each attack.

Table 1 Countermeasures, Effects, and Attacks

Name of Attack	Effects	Proposed techniques	Researchers	Type of Attack
Malicious Code Injection and Tampering	Breach sensitivity and gain access (DOS)	Physical Unclonable Function based Authentication	Muhammad and el at[19]	Physics Attacks
RF Interference/Jamming	Jam Communication (DOS)	Cute Mote	Tiago and el at[20]	Physics Attacks
Fake Node Injection	Control data flow	PAuthKey	Porambage and el at[21]	Physics Attacks
Sleep Denial	Shutdown node	Cute Mote and Support Vector Machine	Tiago and el at[20]	Physics Attacks
Side Channel Attacks	Disclose Encryption key	Making Technique; Authentication using PUF	Muhammad and el at[19]	Physics Attacks
Permanent Denial of Services (PDOS)	Destroy Resources	NOS Middleware	Sicari et al. [22]	Physics Attacks
Traffic Analysis Attack	Data Leakage (Breach Network Information)	Obfuscation framework	Liu et al. [23]	Network Attacks
RFID Spoofing and Unauthorized Access	Modification of Data (Read, Delete, Write)	SRAM based on PUF	Guin et al. [24]	Network Attacks
Routing Information Attacks	An Infinity Routing Loops	Hash Chain Authentication	Glissa et al. [25]	Network Attacks
Selective Forwarding	Message Destruction	Hash Chain Authentication	Glissa et al. [25]	Network Attacks
Sinkhole Attack	Leakage in data or alter	Hash Chain Authentication	Glissa et al. [25]	Network Attacks
Wormhole Attack	Tunneling packet	Intrusion Detection clustering	Prachi Shukla [26]	Network Attacks
Sybil attack	Redundancy and exhausting resources	Trust aware Protocol	Prachi Shukla[26]	Network Attacks
Man in the Middle	Privacy violation	Secure MQIT	Singh et al. [27]	Network Attacks

Replay Attack	DOS, Network Congestion	Signcryption	Ashibani et al. [28]	Network Attacks
DOS/DDOS attack	Crash and flood network	SDN based IoT framework	Park et al. [29]	Network Attacks
Inconsistency Data	Data Inconsistency	Blockchain architecture	Adat et al. [30]	Data Attack
Unauthorized Access	Privacy Violation	Blockchain- based ABE	Adat et al. [30]	Data Attack
Data Breach	Data Breach	Two factor Authentication	Adat et al. [30]	Data Attack
Worm, Spyware, Trojan Horse, Virus, Adware	Destroy Resources	Lightweight framework	Konigsmark et al. [31]	Software Attack
Malware	Data infected	Malware Image Classification	Naeem et al. [32]	Software Attack

6. IOT technologies

6.1 SDN

A modern architecture for network connectivity options and opportunities for Software-Defined Networking (SDN). Duo to possibility of programming network, SDN provide User ability to alter user-specific network behaviour. That means SDN not a solution by itself, it a frame of work (tool) improve network management. By other words SDN consider an architecture to simplest and customize user preferable.

- Home networking:

Managing devices resource in home network consider a big challenge. Many of the solutions proposed in this, such as the implementation of an Open Flow-based monitoring and management framework based on the use limit or restricting data for each user or computer. The framework offers user-based, community, computer, program, or time-of-day visibility of network resources and access control and allows for the ability to share data capability with another user. The nice Kermit GUI is used for the control and network management system. The management of capacity the network policies and policies are focused on the language of response[33].

- Security:

The network's global vision will boost the protection of structures. It is not possible to base this defense on Server such defenses are ineffective only in the host protection when it is corrupted by the host. The Pedigree method in it is viewed as an alternative to offering traffic control.

Moving into an organizational network. Cantered on this Open Flow the device makes it possible for the controller to interpret and authorize the Connections and the distribution of traffic on the network.

- Virtualization:

With the separation of the SDN data-control, the possibilities for the development of modern integrated virtual networks are exciting. For example, this is an OpenFlow initiative. This helps you to create slices according to several criteria, including the bandwidth TCP ports (src/dst, src/dst and IP) or the loading of your CPU switch [33]. Any single slice is independent, which ensures that the traffic of the other slices does not influence it. In addition, to construct hierarchical structures, it is possible to subdivide slices. Migrating virtual networks is a network service that takes advantage of virtualizing network capabilities. A framework involving the transmission of the switch set-up to another network device without disrupting the active traffic in the network is proposed. It copies the flow tables setup from the before the present transfer configuration, that switches the routes automatically. This service requires a network machine to be substituted for an Escape interference or packet loss. It could be this advantage dynamic alteration of the services used in the network (Networks in green). In other words, you should toggle off the network. Unnecessary devices (nights or weekends) and unnecessary devices (nights or weekends) or uninstall them.

- Mobile Network:

In the networks, the machines related constraints exist on mobile carrier networks, as networks for computers. The carrier networks, likewise, the Seventh, for example, implements guidelines and protocols the 3GPP (Generation Collaboration Project) as well as implementations with private vendors. The SDN at this stage you should extend the paradigm and its flow-based model to this kind of infrastructure offers stronger instruments. Software—Products SDMN is an architecture for a Given Mobile Network (SDMN). This allows for clarity, creativity, and programmability. Operators, without relying on proprietary suppliers or exclusive vendors over the largest (OTT) suppliers of services. This model is made of the MobileFlow Forwarding Engine (MFFE) consists of two elements the MFC (MobileFlow Controller) and MFFE is a simple type of balanced and high-performance

data aircraft. It features a lot of complicated structure than an Overflow switch, as a result of it must support extra carrier functions, equivalent to layer three tunneling (i.e., GRE and GTP-U), nodes functions of access network, and versatile charging [33],[34].

- Multimedia:

The numerous immersive web platforms, real time transmissions, for example, require elevated levels of the quality of the network service and its availability. IP video traffic, according to studies provided by CISCO, it will rise to 73 percent by 2017 from 60 percent in 2012. Furthermore, in recent years, the Consistency of expertise (Toe) definition of distinctive no heritable power. That seeks to redefine (QoS) that considers the client level admission to a specialized multimedia system application or service. Thus, SDN makes it possible to customize the multimedia Tasks in Administration. For example, the QoEE is enhanced Experience by optimization of the route. The QoS Matching and Optimization Function (QMOF), which crosses and defines the required setup to the distinctive mixed media boundary and the Path Assignment Function (PAF), continuously improves the geography of the enterprise [33]. The framework dynamically modifies the route parameters in the event of a decline in the condition of the connections, considering the Customers' tendencies. In comparison, the QOE Fairness Scheme (QFF) OpenFlow-Helped venture explores the transport of organizations and characterizes mixed broadcasts for terminal gadgets and organization [33].

6.2 Blockchain

Industry and analysis have foreseen Blockchain technologies[35]. Culture as a disruptive technology that is prepared to be disrupted in overseeing, monitoring, and most importantly, playing a major role protecting IoT devices. This segment explains how it is possible for the blockchain to crucial enabling technologies for the delivery of viable defense solutions challenging IoT security challenges today.

Research work on IoT protection and blockchain is minimal in the literature, with the bulk of work concentrating on using blockchain technologies to generally support the IoT. Blockchain use cases have been classified, four of which are IoT cases. The four formats of IoT include an immutable case archive and data access control administration, the trading of IoT data gathered and IoT device symmetrical and asymmetrical key management. The challenges to IoT identification have been set bare. Such problems specifically involve relatio nships of ownership and identification, authentication and permission, data governance and privacy.

In addition, recent research reveals a significant number of IoT based security attacks based studies [36-37]. These studies considered different attack types, including ransomware, cybersecurity-related challenges to IoT and Big Data application. Authors considered the pandemic time and ranked the most popular cybersecurity attack in [38]. Furthermore, a detailed systematic study and a comporehensive related to the security attacks and threats have been presented in [39-40].

7. Conclusion

Since the advent of IoT, the research community has drawn attention to many security flaws, from mobile attacks to bus data attacks. Moreover, it has been made a distinct analysis area by the comprehensive use of IoT in industries.

In this research we intended to surveys recent research in the field of IoT security. Another goal of this work is to promote IoT security solutions to reduce security risks that affect IoT users. This survey offered interesting open areas of analysis on IoT security problems for both conventional and blockchain-based solutions that are still less investigated.

8. References:

1. Mahmoud, R., et al. Internet of things (IoT) security: Current status, challenges and prospective measures. in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). 2015: IEEE.
2. AlZain, M.A., et al. Cloud computing security: from single to multi-clouds. in 2012 45th Hawaii International Conference on System Sciences. 2012: IEEE.
3. AlZain, M.A., B. Soh, and E. Pardede. Mcdb: using multi-clouds to ensure security in cloud computing. in 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. 2011: IEEE.
4. Alzain, M.A. and E. Pardede. Using multi shares for ensuring privacy in database-as-a-service. in 2011 44th Hawaii International Conference on System Sciences. 2011: IEEE.
5. Andrea, I., C. Chrysostomou, and G. Hadjichristofi. Internet of Things: Security vulnerabilities and challenges. in 2015 IEEE Symposium on Computers and Communication (ISCC). 2015: IEEE.

6. Kaur, D. and P. Singh, Various OSI layer attacks and countermeasure to enhance the performance of WSNs during wormhole attack. International Journal on Network Security, 2014. **5**(1): p. 62.
7. Zanella, A., et al., Internet of things for smart cities. IEEE Internet of Things journal, 2014. **1**(1): p. 22-32.
8. Alshambri, H., et al., Cybersecurity attacks on wireless sensor networks in smart cities: an exposition. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 2020. **8**(1).
9. wikipedia, Home Automation. 2018.
10. Ramaprasad, A., A. Sánchez-Ortiz, and T. Syn. A unified definition of a smart city. in International Conference on Electronic Government. 2017: Springer.
11. Samra, H.E., et al., A Conceptual Model for Cloud-Based E-Training in Nursing Education, in Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth. 2019, IGI Global. p. 295-310.
12. Samra, H., et al., Utilisation of hospital information systems for medical research in Saudi Arabia: A mixed-method exploration of the views of healthcare and IT professionals involved in hospital database management systems. Health Information Management Journal, 2019. **49**(2-3): p. 117-126.
13. Alqurashi, R.K., et al., Cyber Attacks and Impacts: A Case Study in Saudi Arabia. International Journal of Advanced Trends in Computer Science and Engineering, 2020. **9**(1).
14. Alhathally, L., et al., Cyber security Attacks: Exploiting weaknesses. International Journal of Recent Technology and Engineering 2020. **8**(5).
15. Altwairqi, A.F., et al., Four Most Famous Cyber Attacks for Financial Gains. International Journal of Engineering and Advanced Technology, 2019. **9**(2).
16. Sengupta, J., S. Ruj, and S.D. Bit, A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 2020. **149**: p. 102481.
17. Ahemd, M.M., M.A. Shah, and A. Wahid. IoT security: A layered approach for attacks & defenses. in 2017 international conference on Communication Technologies (ComTech). 2017: IEEE.
18. Varga, P., et al. Security threats and issues in automation IoT. in 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). 2017: IEEE.
19. Aman, M.N., K.C. Chua, and B. Sikdar. A light-weight mutual authentication protocol for iot systems. in GLOBECOM 2017-2017 IEEE Global Communications Conference. 2017: IEEE.
20. Masud, M. and Hossain, M. S., Secure data-exchange protocol in a cloud-based collaborative health care environment. Multimedia Tools and Applications, vol. 77, no. 9, pp. 11121-11135, 2018.
21. Porambage, P., et al., PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications. International Journal of Distributed Sensor Networks, 2014. **10**(7): p. 357430.
22. Sicari, S., et al., REATO: REActing TO Denial of Service attacks in the Internet of Things. Computer Networks, 2018. **137**: p. 37-48.
23. Liu, J., C. Zhang, and Y. Fang, Epic: A differential privacy framework to defend smart homes against internet traffic analysis. IEEE Internet of Things Journal, 2018. **5**(2): p. 1206-1217.
24. Guin, U., et al. A secure low-cost edge device authentication scheme for the internet of things. in 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID). 2018: IEEE.
25. Glissa, G., A. Rachedi, and A. Meddeb. A secure routing protocol based on RPL for Internet of Things. in 2016 IEEE Global Communications Conference (GLOBECOM). 2016: IEEE.
26. Shukla, P. Ml-ids: A machine learning approach to detect wormhole attacks in internet of things. in 2017 Intelligent Systems Conference (IntelliSys). 2017: IEEE.
27. Singh, M., et al. Secure mqtt for internet of things (iot). in 2015 Fifth International Conference on Communication Systems and Network Technologies. 2015: IEEE.
28. Ashibani, Y. and Q.H. Mahmoud. An efficient and secure scheme for smart home communication using identity-based signcryption. in 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC). 2017: IEEE.
29. Park, N. and N. Kang, Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. Sensors, 2016. **16**(1): p. 20.
30. Adat, V. and B. Gupta. A DDoS attack mitigation framework for internet of things. in 2017 international conference on communication and signal processing (ICCSP). 2017: IEEE.
31. Konigsmark, S.C., D. Chen, and M.D. Wong. Information dispersion for trojan defense through high-level synthesis. in Proceedings of the 53rd Annual Design Automation Conference. 2016.
32. Naeem, H., B. Guo, and M.R. Naeem. A light-weight malware static visual analysis for IoT infrastructure. in 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD). 2018: IEEE.
33. Valdivieso Caraguay, Á.L., et al., SDN: evolution and opportunities in the development IoT applications. International Journal of Distributed Sensor Networks, 2014. **10**(5): p. 735142.
34. Li, H., P. Li, and S. Guo. MoRule: Optimized rule placement for mobile users in SDN-enabled access

networks. in 2014 IEEE Global Communications Conference: IEEE.

35. Alabdali, N.A., et al., BITCOIN AND DOUBLE-SPENDING: HOW PAVING THE WAY FOR BETTERMENT LEADS TO EXPLOITATION. Indian Journal of Computer Science and Engineering, 2020. **11**(1).
36. S. Saeed, N. Z. Jhanjhi, M. Naqvi, M. Humayun and S. Ahmed, "Ransomware: A Framework for Security Challenges in Internet of Things," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2020, pp. 1-6, doi: 10.1109/ICCIS49240.2020.9257660.
37. D. K. Alferidah and N. Jhanjhi, "Cybersecurity Impact over Bigdata and IoT Growth," 2020 International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 2020, pp. 103-108, doi: 10.1109/ICCI51257.2020.9247722.
38. Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1
39. Alferidah, D. K., & Jhanjhi, N. Z. (2020). A Review on Security and Privacy Issues and Challenges in Internet of Things. International Journal of Computer Science and Network Security IJCSNS, 20(4), 263-286.
40. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cybersecurity threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45(4), 3171-3189.