Wireless Sensor Networks: Security, Threats, and Solutions

Usman Inayat
Dept. of Informatics and Systems
University of Management and Technology
Lahore, Pakistan
usman.inayat@umt.edu.pk

Fahad Ali
Dept. of Informatics and Systems
University of Management and Technology
Lahore, Pakistan
fahad.ali@umt.edu.pk

Hafiz Muhammad Ashja Khan
Dept. of Informatics and Systems
University of Management and Technology
Lahore, Pakistan
ashja.khan@umt.edu.pk

Syed Moshin Ali
Dept. of Informatics and Systems
University of Management and Technology
Lahore, Pakistan
syed.moshin@umt.edu.pk

Kiran Ilyas
Dept. of Informatics and Systems
University of Management and Technology
Lahore, Pakistan
kiran.ilyas@umt.edu.pk

Habiba Habib
Dept. of Informatics and Systems
University of Management and Technology
Lahore, Pakistan
habibahabibullah207@gmail.com

2021 International Conference on Innovative Computing (ICIC) | 978-1-6654-0091-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICIC53490.2021.9693021

***Abstract*— Wireless sensor network (WSNs) is a rapidly growing technology that could be utilized in almost all applications like in healthcare environment, smart homes, smart building, analysis of habitat, global application, and so on. However, the development and huge deployment of WSN in different applications also raises the concerns of worst security threats, which make WSNs vulnerable to many security attacks and system failures. Usually, sensor nodes arrangement cause problems like arrangement in the deserted environment cause the WSNs to become weaker against the complicated threats or destruction, sensor nodes internal storage limitations also cause the classical arrangement of the system useless. Therefore, this papers discusses the major security goals, vulnerabilities, and threats that are associated with the layers of WSNs along with their countermeasures.**

Keywords*— *Wireless sensor network, sensor nodes, Security goals, security vulnerabilities, security measures.

I. INTRODUCTION

The wireless sensor network (WSNs) is a network that extends wireless technologies to the embedded network and it is also described as a domain-specific wireless system. Each node is linked with various other sensor nodes and every node is known as a sensor node in a wireless sensor. It is a diverse group of sensors. The sensors in WSN are usually inexpensive and also utilize a very low amount of energy. They have low bandwidth for connectivity and are also small in scale [1]. They are ad hoc in nature. To collect data from the real world is the key purpose of WSNs. They track physical and environmental conditions like sound, pressure, temperature, and relay data accurately across the network. In such types of networks, the sensors are included and they combine information, process the information, and transfer via the central node. The wireless sensor nodes assist in the monitoring of sensor operations are usually bi-directional. To work they do not require any infrastructure. The utilized sensors in this technology are not currently available, at the micro- and nano-stages. Researchers are working on it that for the utilization of network anywhere how sensor size could be utilized [2]. They are helpful in conditions where wires are not ideal. They could be underwater, underground, and terrestrial.

Adding to their network popularity they could be utilized in any area. This offers inexpensive alternatives to real-world challenges. They are utilized in various areas just because of the various benefits of WS security, like military, environmental areas like forest fire identification, earthquakes, medical field and in business applications, and others [3] – [6]. WSN consists of several low-priced sensors with limited properties such as low memory, limited battery supply, low bandwidth, and low processing units [7]. The different applications of WSNs are also presented in Fig. 1. However, it causes new security risks (Sybil, false node, malicious data, sinkhole, wormhole, and information gathering) [8]. The risk profile for defense is changed by this. It has different security problems because of its design, storage, and energy constraints. The attacker will leave the network susceptible to multiple forms of threats via utilizing these security susceptibilities. So, security is one of the main criteria for every network. The general security remains the same as for standard networks priorities like availability, data confidentiality, and authentication [9, 10]. Wireless sensor networks follow the protocol framework of the OSI layer which has seven layers. The security vulnerabilities with these protocol layers are covered separately at every layer. Protocols of each layers are provided in Table I. This fulfills the security criteria like authentication, confidentiality, integrity, encryption, latency, complexity, and availability. Using cryptographic algorithm we can protect the confidentiality of data by preventing the unauthorized used access [11]. Cryptography enhance the data confidentiality but needs more power and increase the latency, because more time is required in data encryption and decryption. WSNs, to ensure data integrity utilizes different authentication techniques. These approaches are like MAC layer authorization [12], transport layer authorization [13], and network layer authorization [14]. The network layer utilizes a WPA and WPA2 to ensure authorization, while the transport layer utilizes the SSL and TSL protocols.

TABLE I. SECURITY REQUIREMENTS AND THEIR PURPOSES

OSI layers	Wireless Protocols
Application	FTP, HTTP, and SMTP
Network	IP and ICMP
Transport	UDP and TCP
MAC layer	CSMA/CA and CDMA
Physical	Coding, transmission medium, and modulation

The normal mechanism of WSNs mainly consists of the mode of transmission of sensor data towards the center via multiple-hop transmission. This transmission should be speedy and secure. The one node is called the sink node that connects with the base station. The sensor node is responsible for the processing of the sensed information and the neighbor node is transmitted. After that, the information is transfer to the sink node and forward to the center through the base station.

In wired system, a physical connection is established in between communicating nodes through cables. Because of the broadcasting nature of the wireless network, the WSNs are susceptible to many security attacks like denial-of-service (DoS), eavesdropping, man-in-the-middle, spoofing, and false message attack and so on. In a wireless network, the unauthorized nodes could cause interruption which disrupts information transmission between legal users [15].

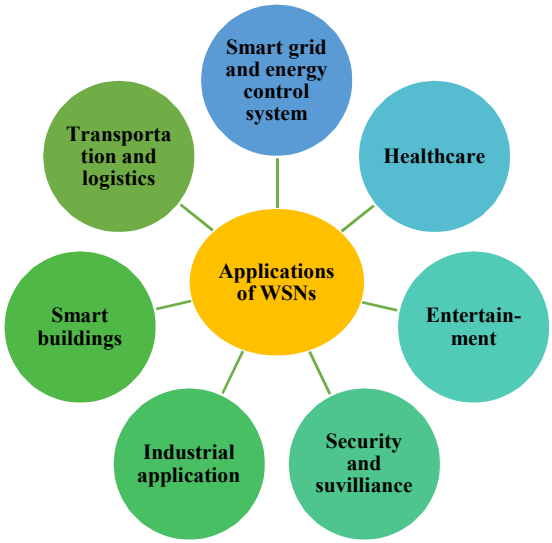

Fig. 1. Wireless sensor network applications

In this paper, the major threats associated with the different layers of WSN has been discussed. Section II describes the security goals of WSNs. Section III describes the challenges of security in WSNs. Section IV describes some threats in WSNs. Section V describes some countermeasure against threats and finally section VI conclude this paper.

II. SECURITY GOALS IN WSNS

Several safety criteria have been defined to secure wireless communication from threats like node compromise, eavesdropping, and denial of service [16]. The various types of security specifications for wireless sensor network are provided in Table II and also discussed as follow.

A. *Confidentiality*

The confidential data could not be access by unauthorized persons that's why this mechanism includes the security of confidential data. Confidentiality encrypts the sharing of data in the sensor environment when packets are transported among the base station and in sensor nodes. From eavesdropping, it stops threats. The greatest confidentiality danger is the presence of infected nodes since the attacker could be able to hack nodes to access sensitive information, like cryptographic keys [17].

B. *Authentication*

For the identity checking of the users and notifies the fraudulent participants and authentic or legal users this approach is important. Each base station and sensor node could be able to distinguish either an intruder node or a legal node is transferring the received packet for the wireless sensor network [18].

C. *Integrity*

This causes the data in the sensor network from becoming changed during the transferring process of information usually prevent this. Integrity loss is a significant concern because the utilization of false or incorrect data could lead to devastating endings.

D. *Protected management*

The management of various nodes in the whole network is crucial to handle confidential data. In WSNs, protected management at the base station level is needed because the connectivity at the base station from the sensor nodes ends.

TABLE I. SECURITY REQUIREMENTS AND THEIR PURPOSES

Security goals	Purpose
Confidentiality	Allow only authentic users to access the data.
Integrity	Improve data accuracy and restrict falsification.
Authenticity	Make difference between authentic and unauthorized users.
Availability	Ensure the network availability to the legitimate node.

III. CHALLENGES OF SECURITY IN WSNS

Because of its free wireless media and broadcast nature, wireless sensor network has various security susceptibilities. The fraudulent attackers to perform many types of attacks utilized these current network susceptibilities, like wormhole, DoS, sinkhole, and flood among others [18]. Many other susceptibilities are listed below.

A. *Medium of broadcast nature*

Only by placing wireless media access with the radio spectrum of the sensor network node, the wireless media access is easily available to all, the fraudulent users could access network permission. Thus, an attacker will intercept, repeat, and change or eavesdrop on the network packets.

B. *Resource limited sensor nodes*

The WSNs have limited computing, energy, computational capacity, storage, and bandwidth in a sensor network. This limits the capabilities of sensor networks like prevention approaches like cryptography and data aggregation.

C. Limitation of physical safeguards

The sensor networks are deployed in a hostile situation. They could be physically affected, seized, and disrupted in such types of conditions through attackers. On military battlefields capturing machines could cause serious consequences.

D. Diverse network topologies

Wireless sensor network has a diverse topology of the network and since the SNs could leave and join the network at any time, therefore have no statically fixed boundaries or configuration. Security systems which could fight like high network dynamism are also crucial.

E. Immense scale

As compared to the small-scale networks, intrusion detection is complicated in networks including thousands of SNs.

IV. Threats in Wireless Sensor Network

Threats could be divided into active and passive threats in wireless sensor networks. The main purpose of an attacker is to get transferred data without being notified in a passive threat. The attacker accumulates a huge volume of information and performs data processing to retrieve any sensitive data. The active and passive attacks in WSNs are presented in Fig. 2. In active attacks, the malicious user performs multiple threats like insertion, replay, and packet alteration by leveraging security attacks susceptibilities in the wireless protocol stack.

Relative to active attack the passive attack is less serious, but as it is often difficult to detect this passive attack because an intruder is disguised and does not leave any evidence. In a wireless sensor network, it is also possible to divide attacks into internal and external attacks. In an external attack malicious user could be able to insert attacks from outside and it has minimal effect. While in internal the malicious user obtains authentication to enter in the network and inflict collateral harm via installing attacker nodes and even accessing the secrets of legal nodes. Security problems are present in every layer and challenges in the reference model OSI. Numerous susceptibilities are thus shown because different layers are dependent on different protocols [18, 19]. Various security risks and their solutions are summarized in different layers of OSI in Table II.

In wireless sensor networks, there are various types of threats or risks that cause the loss of information, with the help of sensor node cause loss of connectivity, insert delay by slowing down the service [19].

A. Changed, retransferred, and spoofed routing data.

An adversary could be able to modify the routing data among nodes, make routing loops, produce fake texts, and also increase delay from one point of the network to another.

B. Selective forwarding

Any fraudulent node which was escaped from the network cause destruction of the incoming data. It usually causes the block of the data flow and it is identical to the black hole. If any malicious user is using the flow path, then it will cause the destruction of every data packet and behave like a black hole, also cause a denial of service, because of changes in messages from legal nodes. The attacker on the flow path induced jamming and collision for every transferred packet.

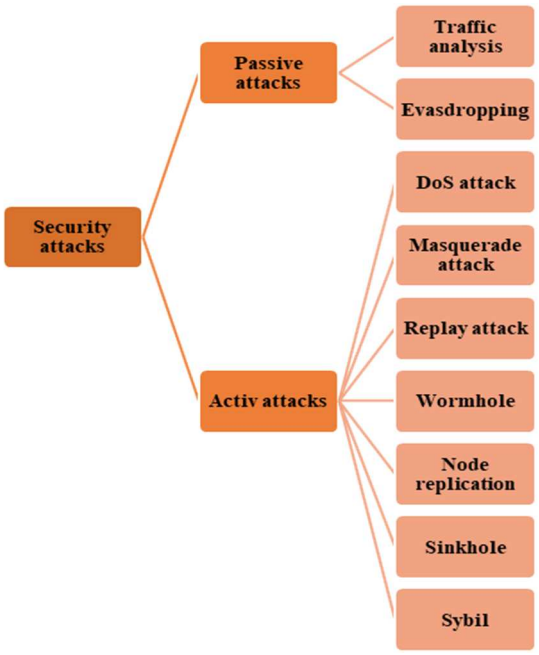

Fig. 2. Active and passive attacks in WSNs

C. Sinkhole attack

It is just like a selective forwarding threat. A node that loses the network behaves like a sink node, attracts all packets of information towards itself. There is a great danger associated with traffic in this threat. A sinkhole threat could be able to generate the forwarding threat to tamper the flow of the packet path. It produces the attraction in malicious nodes for its neighboring nodes. It also gives a supportive environment to wormhole threats.

D. Sybil attack

This threat minimizes the capacity of the error detecting system. However, the node could be provided with different IDs, data related to location could also be modified. It also put an effect on effective mechanisms like authentication, and topology maintenance. After ensuring the misbehavior of nodes it starts the selective forwarding threats.

E. Wormhole attack

In this message over low-latency connectivity are received by the malicious user who gets access into the part of any network and also can repeat these messages via a tunnel. This threat consists of two nodes that want to minimize the distance between them through repetition. The malicious users make two distant nodes neighbor of each other. With this attack, the sinkhole threat could also be able to activate. Usually, it sends packets more speedily from one point of any network to another. In short, it creates smart cuts in any network. Two nodes are malicious, one is inserted into the network and the other is neighbor with the targeted node.

F. Hello flood attack

This attacker behaves as it is a neighbor of any node. Fraudulent data then transfer with great transmission power. Different nodes that pretend neighbors of other nodes need a hello packet. When this hello message is received by the node then it assumes that the sender node is also in the radio range. This attack slow-down the transmission process by producing confusion in the network.

TABLE II. SUMMARY OF VARIOUS ATTACKS IN WSN LAYERS

Attacks	Threats	Solution
Physical layer		
Jamming attack [21]	In the sensor network, the attacker interacts with radio-frequency communication. The attacker arbitrarily choose jamming nodes and implement jamming	To stop this, various types of spread spectrum could be utilized. One of the most common is frequency hopping. But the price is too much.
Tampering [22]	In this, the network nodes are equipped with tamper-resistant hardware.	Whenever sensor networks nodes are physically accessed, they combust their data to stop the loss of data.
Sybil attack [23], [24]	This attack aligns the legal node to get new identities or maybe through fraud.	This could be fixed at a higher level stack by setting all the SN in the network.
Link layer		
Collision [25]	In this, the collision in a small area is needed by the attacker. The insignificant alternation in data packets could cause checksum error.	Error checking nodes could be utilized but it consumes a large amount of energy
Exhaustion [26]	When communication is altered various time then this cause retransmission of data.	When counts of sensor nodes cross threshold value then it clarifies itself in attack and goes to sleep mode.
Interrogation attack	In such type of attack, the request for packets is normally sent by fraudulent nodes, without considering the control to send.	Nodes must not accept any request from the neighbor node.
Sybil attack [23], [24]	Produced negative results. And attackers estimate the outcomes.	Radio resource testing cause over connectivity.
Network layer		
Misdirection [26]	Fraudulent nodes misguide the packets and make their destination unreachable.	A node can transfer itself to sleep mode if it finds an incorrect path.
Neglect and Greed	In this node leave the packet in between the path and allow random priorities to pass through the packets.	Utilization of multiple routing ways.
Blackhole attack [27]	Fraudulent nodes show cost zero for various paths and make an impact on routing protocol and select the fraudulent node as a legitimate node.	Can be solved by when only a legal node can send a reply about the route.
Sybil attack [23], [24]	Malicious nodes impersonate the routing protocol by showing different paths. It impacts the geographical protocols.	There is no accurate mechanism against this attack.
Wormhole attack [28]	The attacker makes a wormhole to destroy the routing path.	Check out the bi-directionality of the link.
Altering and spoofing attack [29]	This attacker makes the path shorter or longer, attracts or repels the traffic in the network.	Authentication and encryption mechanisms are effective.
Transport layer		
Flooding [30], [31]	The attacker keeps on sending connection requests, cause network flooding.	Employ a limited number of connections for any node.
De-synchronization	It causes the energy loss of nodes.	An effective mechanism is helpful for the security of all exchanged packets.
Application Layer		
SQL injection [32]	Have an unauthorized access to the multiple websites	Anti-viruses and firewalls
SMTP attack [33], [34]	Password sniffing and email spoofing	Anti-viruses and firewalls
Malware attack	Disturb or block the authorized data	Anti-viruses and firewalls

G. *Acknowledgment spoofed*

It shows that the dead node is not dead and still alive and the connection is strong. In this way, it could be able to seize packets that were sent to the dead node. The attacker could also be able to predict which node is dead or not by listening to the packets.

H. *Denial of Service attack*

In this attacker put false traffic to destroy the targeted server then the maximum operating limit of that server. This attack is usually carried out to fill the aimed node with false requests to put the load on the system and try to stop giving the response to the legal nodes. The general mechanism of SNs makes them vulnerable to the DoS threat.

I. *Masquerade threat*

In this threat, the attacker uses the false personality to find access to any person's private data illegally. The malicious user utilizes an unauthorized system to get the data or maybe to get extra permissions than the previous one. This attack includes the other type of active threat. For instance, an authenticated arrangement could be carried out, and after that legal person could get rights to get all the sensitive data in an unauthorized way [35].

J. *Replication of node*

In this threat, the attacker made specific manageable nodes and present these nodes as authorized nodes to the whole network to make them accommodated in the network. Only with the help of centralized monitoring, it could be detectable otherwise not.

K. *Rushing attack*

A new threat that causes DoS threat while using for competition against all routing practices of the network. The adversary divides the fraudulent data speedily to genuine data which later reaches. Several security threats have been proposed and elaborated in [36-51].

V. COUNTERMEASURES AGAINST WSNS ATTACKS

Countermeasures used for security in WSNs are various techniques and tools depend on the situation in which the attacker inserts an attack. To ensure security in SNs, keep in mind the various attributes of WSNs. Some of the following techniques are described in the following which are used as a countermeasure [35].

A. Multi-parent routing mechanism.

Information partitioning is effective to stop the leakage of information from wireless sensor networks. As the name indicates that main aim is to divide the information into portions. If the node wants to send an information, then it needs to transfer this into packets of static size. And packets are transferred over various routes. After this base received them, who accumulate all the data to generate the original data. To prevent this, the malicious user gets all the packets to rebuild the legal message.

B. Cryptographic algorithm

WSNs could not be able to utilize complicated and efficient cryptographic algorithms due to their limitations. However, they need costly and energetic sensors for the processing of power autonomy. That's why usually symmetric algorithms are given importance. Key sharing is of four kinds which are utilized; individual key, global key, shared key via pair of nodes, shared key via the group of nodes.

C. Key management protocol

In the key generation process, this solution was presented. A new produced key is created and also send via a base station to the whole network. In the whole network, this new key is utilized to authenticate every node. Just legal nodes are allowed to access the network.

D. Location identification protocol

For the identification of fraudulent nodes, a mechanism mainly consists of the utilization of the geolocation data. In this mechanism, beacon nodes coordinates are already configured in the devices, they have their positions.

E. Reputation depends on the protocol

This solution mainly consists of a sensor network, there is a large number of nodes so that's why it is harder to detect the fraudulent ones. Every network node will keep an eye on its neighboring node for the identification of threats and also save the integrity of the network. It also accumulates the nodes' confidence index according to the activities of its neighboring nodes.

F. Anti-tamper mechanism

Through this method, physical compromise threats could be solved like self-destruction methods and micro-switches.

VI. Conclusion

Nowadays security of wireless networks is one of the major concerns, especially wireless network security. Therefore, it is one of the alarming problems these days. This paper has discussed security vulnerabilities, security goals, and threats which are associated with the wireless sensor network nodes. The threats associated with wireless sensor network nodes can be active and passive and these threats are further classified according to modeling layers. However, further research is required in this field for improving systems against security threats. Different protocols have also been associated with the wireless sensor networks, but they do not give satisfactory results. Moreover, the requirements for wireless sensor network nodes and their associated protocols make the wireless sensor network more complicated to have strong security practices.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer networks, vol. 38, no. 4, pp. 393-422, 2002.

[2] D. Estrin, L. Girod, G. Pottie and M. Srivastava, "Instrumenting the world with wireless sensor networks," 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. 2033-2036, 2001.

[3] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: an up-to-date survey," Applied System Innovation, vol. 3, no. 1, pp. 14, 2020.

[4] M. F. Zia, E. Elbouchikhi, M. Benbouzid and J. M. Guerrero, "Microgrid Transactive Energy Systems: A Perspective on Design, Technologies, and Energy Markets," IECON 2019 - 45th Annual Conference of the IEEE Industrial Electronics Society, pp. 5795-5800, 2019.

[5] M. Ali, M. F. Zia and M. W. Sundhu, "Demand side management proposed algorithm for cost and peak load optimization," 2016 4th International Istanbul Smart Grid Congress and Fair (ICSG), pp. 1-5m 2016.

[6] A. Zafar, A. Shafique, Z. Nazir and M. F. Zia, "A Comparison of Optimization Techniques for Energy Scheduling of Hybrid Power Generation System," 2018 IEEE 21st International Multi-Topic Conference (INMIC), pp. 1-6, 2018.

[7] A. Perrig, J. Stankovic and D. Wagner, "Security in wireless sensor networks," Communications of the ACM, vol. 47, no. 6, pp. 53-57, 2004.

[8] F. Shahzad, M. Pasha, and A. Ahmad, "A survey of active attacks on wireless sensor networks and their countermeasures," arXiv preprint arXiv:1702.07136, 2017.

[9] R. Jadhav and V. Vatsala, "Security issues and solutions in wireless sensor networks," International Journal of Computer Applications, vol. 162, no. 2, pp. 14-19, 2017.

[10] P. Sinha, V. K. Jha, A. K. Rai and B. Bhushan, "Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey," 2017 International Conference on Signal Processing and Communication (ICSPC), pp. 288-293, 2017.

[11] O. G. Aliu, A. Imran, M. A. Imran and B. Evans, "A Survey of Self Organisation in Future Cellular Networks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 336-361, 2013.

[12] K. H. M. Wong, Yuan Zheng, Jiannong Cao and Shengwei Wang, "A dynamic user authentication scheme for wireless sensor networks," IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 8, 2006.

[13] L. Venkatraman and D. P. Agrawal, "A novel authentication scheme for ad hoc networks," 2000 IEEE Wireless Communications and Networking Conference, Conference Record (Cat. No. 00TH8540), vol. 3, pp. 1268-1273, 2000.

[14] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," IEEE Personal Communications, vol. 1, no. 1, pp. 25-31, 1994.

[15] B. Bhushan, and G. Sahoo, "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks," Wireless Personal Communications, vol. 98, no. 2, pp. 2037-2077, 2018.

[16] A. Tyagi, J. Kushwah, and M. Bhalla, "Threats to security of wireless sensor networks," In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence, pp. 402-405, 2017.

[17] J. Shaheen, D. Ostry, V. Sivaraman and S. Jha, "Confidential and secure broadcast in wireless sensor networks," 2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1-5, 2007.

[18] Y. Jiang, C. Lin, X. Shen and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," IEEE Transactions on wireless communications, vol. 5, no. 9, pp. 2569-2577, 2006.

[19] T. Azzabi, H. Farhat, and N. Sahli, "A survey on wireless sensor networks security issues and military specificities," In 2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET), pp. 66-72, 2017.

[20] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," IEEE Communications Surveys & Tutorials, vol. 11, no. 4, pp. 42-56, 2009.

[21] D. W. Huang, W. Liu and J. Bi, "Data tampering attacks diagnosis in dynamic wireless sensor networks," Computer Communications, vol. 172, pp. 84-92, 2021.

[22] K. F. Ssu, W. T. Wang and W. C. Chang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," Computer Networks, vol. 53, no. 18, pp. 3042-3056, 2009.

[23] P. R. Vamsi and K. Kant, "Detecting sybil attacks in wireless sensor networks using sequential analysis," International journal on smart sensing and intelligent systems, vol. 9, no. 2, pp. 651-680, 2016.

[24] I. Ialam, M. Ouadou, D. Aboutajdine and O. Zytoune, "Energy based collision avoidance at the mac layer for wireless sensor network," 2017 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), pp. 1-5, 2017.

[25] M. Jo, L. Han, N. D. Tan and H. P. In, "A survey: energy exhausting attacks in MAC protocols in WBANs," Telecommunication Systems, vol. 58, no .2, pp. 153-164, 2015.

[26] R. S. Sachan, M. Wazid, D. P. Singh and R. H. Goudar, "A cluster based intrusion detection and prevention technique for misdirection attack inside WSN," 2013 International Conference on Communication and Signal Processing, pp. 795-801, 2013.

[27] M. Meghdadi, S. Ozdemir and I. Güler, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks," IETE technical review, vol. 28, no. 2, pp. 89-102, 2011.

[28] V. B. Srinivas and S. Umar, "Spoofing attacks in wireless sensor networks," International Journal of Science, Engineering and Computer Technology, vol. 3, no. 6, pp. 201, 2013.

[29] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram and D. Zamboni, "Analysis of a denial of service attack on TCP," In Proceedings 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097), pp. 208-223, 1997.

[30] R. K. Chang, "Defending against flooding-based distributed denial-of-service attacks: A tutorial," IEEE communications magazine, vol. 40, no. 10, pp. 42-51, 2002.

[31] A. Moosa, "Artificial neural network based web application firewall for SQL injection," International Journal of Computer and Information Engineering, vol. 4, no. 4, pp. 610-619, 2010.

[32] N. Zhang, B. Fang, L. Guo and Y. Jiang, "A new approach for detecting abnormal email traffic in backbone network," 2006 International Conference on Computational Intelligence and Security., vol. 1, pp. 586-591, 2006.

[33] S. Dharmapurikar, P. Krishnamurthy, T. Sproull and J. Lockwood, "Deep packet inspection using parallel bloom filters," 11th Symposium on High Performance Interconnects, pp. 44-51, 2003.

[34] A. Kieyzun, P. J. Guo, K. Jayaraman and M. D. Ernst, "Automatic creation of SQL injection and cross-site scripting attacks," 2009 IEEE 31st International Conference on Software Engineering, pp. 199-209, 2009.

[35] A. Karakaya and S. Akleylek, "A survey on security threats and authentication approaches in wireless sensor networks," In 2018 6th international symposium on digital forensic and security (ISDFS), pp. 1-4, 2018.

[36] Manzoor, A., Hussain, M., & Mehrban, S. (2020). Performance Analysis and Route Optimization: Redistribution between EIGRP, OSPF & BGP Routing Protocols. Computer Standards & Interfaces, 68, 103391.

[37] Mehrban, S., Nadeem, M. W., Hussain, M., Ahmed, M. M., Hakeem, O., Saqib, S., ... & Khan, M. A. (2020). Towards secure FinTech: A survey, taxonomy, and open research challenges. IEEE Access, 8, 23391-23406.

[38] Awan, M. J., Farooq, U., Babar, H. M. A., Yasin, A., Nobanee, H., Hussain, M., ... & Zain, A. M. (2021). Real-time DDoS attack detection system using big data approach. Sustainability, 13(19), 10743.

[39] Hussain M, Javed W, Hakeem O, Yousafzai A, Younas A, Awan MJ, Nobanee H, Zain AM. Blockchain-Based IoT Devices in Supply Chain Management: A Systematic Literature Review. Sustainability. 2021; 13(24):13646.

[40] Zainab, M., Usmani, A. R., Mehrban, S., & Hussain, M. (2019, November). Fpga based implementations of rnn and cnn: A brief analysis. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-8). IEEE.

[41] Hassan, M., Hussain, M., & Irfan, M. (2019, November). A Policy Recommendations Framework To Resolve Global Software Development Issues. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-10). IEEE.

[42] Abid, A., Manzoor, M. F., Farooq, M. S., Farooq, U., & Hussain, M. (2020). Challenges and Issues of Resource Allocation Techniques in Cloud Computing. KSII Transactions on Internet and Information Systems (TIIS), 14(7), 2815-2839.

[43] Faheem, M. R., Anees, T., & Hussain, M. (2019). The Web of Things: Findability Taxonomy and Challenges. IEEE Access, 7, 185028-185041.

[44] Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., & Albahri, A. S. (2018). Conceptual framework for the security of mobile health applications on android platform. Telematics and Informatics, 35(5), 1335-1354.

[45] Hussain, M., Al-Haiqi, A., Zaidan, A. A., Zaidan, B. B., Kiah, M., Iqbal, S., ... & Abdulnabi, M. (2018). A security framework for mHealth apps on Android platform. Computers & Security, 75, 191-217.

[46] Rehman, A. U., Hussain, M., Idress, M., Munawar, A., Attique, M., Anwar, F., & Ahmad, M. (2020). E-cultivation using the IoT with Adafruit cloud.

[47] Nadeem, M. W., Hussain, M., Khan, M. A., & Awan, S. M. (2019, July). Analysis of Smart Citizens: A Fuzzy Based Approach. In 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE) (pp. 1-5). IEEE.

[48] Nadeem, M. W., Hussain, M., Khan, M. A., Munir, M. U., & Mehrban, S. (2019, November). Fuzzy-Based Model to Evaluate City Centric Parameters for Smart City. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-7). IEEE.

[49] Khan, A. G., Zahid, A. H., Hussain, M., Farooq, M., Riaz, U., & Alam, T. M. (2019, November). A journey of WEB and Blockchain towards the Industry 4.0: An Overview. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-7). IEEE.

[50] Khan, A. G., Zahid, A. H., Hussain, M., & Riaz, U. (2019, November). Security Of Cryptocurrency Using Hardware Wallet And QR Code. In 2019 International Conference on Innovative Computing (ICIC) (pp. 1-10). IEEE.

[51] Nadeem, M. W., Goh, H. G., Hussain, M., Hussain, M., & Khan, M. A. (2021). Internet of Things for Green Building Management: A Survey. In Role of IoT in Green Energy Systems (pp. 156-170). IGI Global.