Security Enhancement Strategies in Wireless Sensor Networks - A Survey

S. Naga Chandra Sekhar[1], K. Sahadevaiah[2], B. Tarakeswara Rao[3]

[1]Research Scholar, Department of CSE, JNTU, Kakinada, Andhra Pradesh, India,
Email: schandu.bec@gmail.com
[2]Professor, Department of CSE, University College of Engineering, JNTU, Kakinada, Andhra Pradesh, India,
Email: ksd1868@gmail.com
[3]Professor, Department of CSE-AIDS, KHIT, Guntur, Andhra Pradesh, India, Email: tarak7199@gmail.com

Received: 07.04.2024 Revised: 18.05.2024 Accepted: 24.05.2024

ABSTRACT
The great qualities as well as fast data transfer through one location to the other using wireless technologies for communication is causing a rapid progress in this field. Security constitutes one of the biggest challenges in Wireless Sensor Networks [WSNs], relying mostly on applications deployed. There are many different security measures that have been suggested to protect the privacy of information in WSNs. With those strategies come disadvantages like security flaws. In this work, a security-related survey is undertaken. Because of their physical restrictions in terms of both size and power, WSN influence the adoption of security greatly. We also present the pro's and con's of several existing models with their implementation in WSN. The importance of QoS was also a very important one to know the performance of the various models in terms of security.

Keywords: Privacy, QoS, Security, Wireless Sensor Network.

1. INTRODUCTION

The wireless network is a type inside which nodes within the system are connected wirelessly. A wireless technology is a method for communication infrastructure to establish a connection among portable platforms without using cables and wires. Wireless refers to signal transmission that uses medium radio frequencies in place of cables. These networks are classified majorly into two different types. They are wireless ad-hoc and wireless sensor networks [1].

Wireless Sensor Networks (WSNs) have gained a lot of attention recently as a result of substantial developments in wireless and mobile communication technology as well as the wide expansion of useful applications. WSNs are however flexibly created from a number of power-constrained sensor network and a management node having lengthy power. WSNs were identity, autonomous systems made up of back-end data centers, management nodes, and standard sensors. Initially, the management nodes, which are intermediary collecting nodes, authentication technologies sensor information from a specified pervasive environment from the based on the suggestions [2]. The sensor information as from management nodes will then be delivered to the back-end data center for additional evaluation and processing. Obviously, wireless connectivity methods are used for all node-to-node interaction. Additionally, because wireless sensor networks are self-organized, independent of centralized infrastructure, and their topologies vary on a regular basis, broadcasts are the default communication technique in WSNs.

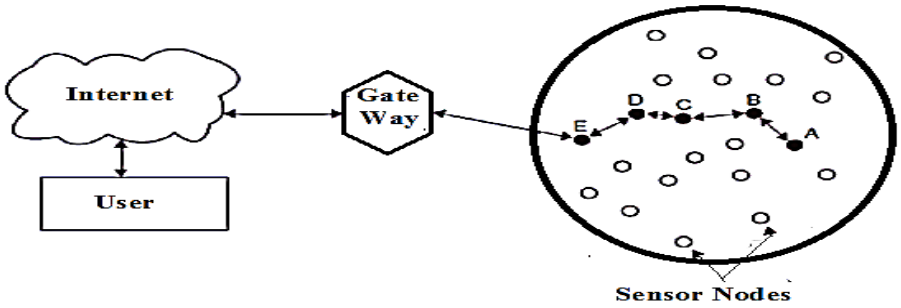

Figure 1. A simple Wireless Sensor Network architecture

Many implementations, like the surveillance of forest fires, the tracking of strategic targets, the fields of medicine or science, and sometimes even our daily lives, have made extensive use of wireless sensor networks. However, because wireless technologies are using a broadcast distribution medium and WSNs have physical protection, they are broken easily into by attackers [3]. A hacker could therefore listen to all conversations, send malware, replicate earlier messages, or take over a sensor network. Through practice, privacy protection as well as node authenticity is the two main security concerns that sensor networks are most concerned about. By achieving information security through protective measures, privacy enables secured network connectivity among sensors and the management platform. Additionally, a well-designed authentication method can guarantee that no authorized node may engage illegally and obtain sensitive data across WSNs [4]. In order to secure transactions in WSNs, a number of strategies have already been put forth. Depending on cryptographic, machine learning, as well as block chain methodologies, we divide things among three categories inside this article.
Following is the breakdown of the remaining chapters: We present the features and factors to be taken into account with WSNs in Section 2. We examine certain security issues and demands within WSNs in Section 3. Several security prevention and mitigation methods and their classification are covered in Section 4. Finally, we wrap things up a few current projects for such secure communication in WSNs.

2. Importance of Wireless Sensor Network

When designing WSNs, several characteristics as well as factors regarding sensor networks were examined and taken into account in comparison with traditional networks [5]. This section gives a brief overview of them.

Characteristics of Wireless Sensor Network

- Self-organized: Since WSNs constitute systems without infrastructures and without maintenance, they are described as such. By starting to operate with certain pre-defined layered protocols and decentralized methods, every sensor network was therefore fully formed independently. Following the completion of the construction of the sensor networks, the sense information would be gathered and sent to the rear system for subsequent processing using the systems that were developed.
- Multi-hop routing: Systems of wireless sensors employ a multihop networking method. Whenever connecting with those other nodes beyond its distribution area because of the restrictions of power transmission as well as the connection service range, each node requires the intermediary peers to be forward.
- Data-Centric Networks: It becomes clear that there's no required correlation seen between number of nodes as well as the node location since nodes are arbitrarily distributed as well as the system and node number association is hybrid evolutionary. The user explicitly informs the systems of both the subjects of interest; these systems then inform the individual of the data accessed within a given time frame. As a result, the WSN is a system that is focused on data.
- Dynamic topology: Consider that sensor networks are distributed at randomized in the majority of sensors communication networks, as well as the network structure will alter periodically because sensor nodes may be halted, breakdown, revive, or use mobile sensors.
- Quality of service: All homogeneous connected things equipment must improve the quality of service in terms of the intelligence provided to the sensor nodes. The burden can be distributed among the nodes that have access to the assets thanks to these heterogeneous systems. Due to fluctuating network setups and link properties, the QoS systems now used on the Internet still need to be improved.

Advantages of wireless sensor networks

The following are a few typical benefits of wireless networks:
Flexibility: Wireless sensor networks enable global network connectivity. Even distant connections outside of the structure are possible. WSNs offer greater flexibility throughout situations where an extra workspace is required, such as in an ad hoc scenario.
Low cost: Wireless sensor networks can communicate without wiring or cables thus require limited management. Consequently, its expense of implementation is low.
VoIP facility: VOIP or voice over internet protocol, is a service also offered by wireless sensor systems.
Scalability: This wireless router scalability allowed for the simple introduction of a new subscriber by utilizing a passcode and updating it via the domain controller.
Easy to setup: Network configurations are possible without any fixed infrastructure.

Disadvantages of wireless sensor networks

Security: A key concern with every data transmission involves security. In sensor networks, eavesdropper is a possibility. As a result, they employ authenticating as well as cryptography measures regarding security.

Reliability: Wireless sensor networks are highly influenced by their environment, which causes interference problems. Certain propagating factors also have an impact on it. The management finds it challenging to control such types of interruptions.

Speed of operation: A congested network slows down the pace of a sensor network, which really is slow by design in contrast to a wired system.

3. Security Concerns and Capabilities of Wireless sensor networks

Security issues and needs are crucial for such a variety of sensor system applications as well as towards the traits and factors already discussed. Numerous security concerns with WSNs have really been raised in recent times [6, 7]. We also discuss several security needs and dangers with WSNs inside this portion.

Active attacks : Active attacks may also be categorized into two parts: external attacks as well as internal attacks. Examples of these kind of attacks include node sybil attacks, replication attacks, compromised node attacks, and wormhole attacks. In external attacks (like wormhole attacks and sybil attacks), a node that isn't a member of the network system could first listen in here on data packet were sent and did receive by regular participating nodes with the intention of maliciously tampering, interrupting, guessing, or spamming the data before injecting incorrect packets to interfere with the network's operations [8].

Passive attacks : Eavesdroppers may passively observe the communications channel that connects two network entities in passive attacks (such as eavesdropping attacks) in order to gather and learn essential information without interfering only with interaction [9].

4. Literature Classifications of WSNs

Numerous studies have been conducted on the effective management applications that were previously mentioned. According to the various applications, we categorize wireless sensor networks strategies into many categories in this chapter, comprising of cryptography, game theory, machine learning, and block chain.

WSNs get a wide range of uses, such as organization and implementation in both defense and commercial contexts. As a result, implementing security measures seems to be crucial, and the foundation of network security is effective management methods. The literary comparison for secure communications networks is shown in Table 1.

Table 1

Classification	Approach	Remarks about the research work
Game Theory	Common game theory approaches [7]	Analysis of security in various aspects
	Intrusion detection system based on payoff matrix [10]	Identification of active DoS attacks
Cryptography	Symmetric and asymmetric cryptography [11]	Hybrid methodology for Wireless Sensor Networks using Vector Algebra
	Symmetric Key Cryptography[12]	Energy Efficiency
	Distributed key revocation [13]	Reduced storage cost and time
	3-Factor user authentication mechanism with elliptic curve scheme [14]	Reduce the overheads of communication and computation
Machine Learning	Cluster model in the LEACH protocol [15]	Improved DDOS attacks detection
	Adaptive chicken swarm optimization [16]	improved network lifetime combined with intrusion detection efficiency
	Combination of the MLP model and the Genetic Algorithm [17]	Improved intrusion detection
	Reinforcement learning or	Latest hybrid method for security enhancement

Classification	Approach	Remarks about the research work
	transfer learning [18]	
Block Chain	Block chain-based collocation storage architecture [19]	High output performance and security
	Cloud sensor [20]	Data delivery delay ratio decreases with the increase of the intergeneration time.
	Blockchain-based WSN with two routing protocols [21]	Network life time will increase
	Hybrid block chain model [22]	Better performance with comprehensive security

4.1 Game Theory in WSN

When WSN may be extensively utilized, WS security is a primary and crucial concern. In WSN safety, there are typically two intrusion prevention and detection systems. A mathematical approach for analyzing and simulating WSN security issues is provided by game theory since it takes into account situations in which numerous individuals with competing goals are present.

Conventional game theory tactics to improve WSN secure are categorised onto four areas utilising a taxonomy created by Shen et al. [9]: avoiding assaults, discovering intrusions, strengthening protection, and living with malevolent sensor nodes. They suggested a variety of potential domains for additional study in game model-based WSN safety, including Base Station trustworthiness, IDS efficacy, WSN mobility, WSN QoS, real-world applicability, energy consumption, sensor nodes learning, expanding game theory applications, and other games.

Both the defective endpoints and the IDS have access to the strategy space and payout matrix thanks to a game model created by Dong et al. [10] that can aid in the identification of active DoS attacks.

4.2 Cryptography in WSN

The use of WSN is growing in an extensive variety of uses, including automation of homes, environmental surveillance, vehicle tracking, and the impact of climate change. The WSN's security is a difficult task. Cryptography is one method of ensuring confidentiality. Security is provided using hash functions, symmetric key approaches, and asymmetric key mechanisms. Given that WSN are severely confined by means of compute, connection, and battery capacity, it calls for a compact encryption solution. The limitations of the node sensors in WSN make the choice of cryptographic approach essential.

Combining both asymmetrical and symmetric encryption can maximize the benefits of these two strategies. A recently proposed hybrid cryptographic technique using vector algebra [11] was suggested by Prof. Pugliese and Santucci in 2008 for the production of pair wise network architecture authenticated keys (TAK) in WSNs. Symmetric authentication is utilized for ciphering, whereas asymmetric key creation is employed.

The idea for Energy Efficiency of Symmetric Key Cryptographic Methods in Wireless Sensor Networks [12] was created by Xueying Zhang et. al. The overall energy performance of symmetric key cryptography methods used in wireless sensor networks (WSNs) was evaluated in the suggested study. By examining the quantity of CPU cycles needed for encryption, it determines the amount of computational energy cost of the ciphers under evaluation. It examined the energy performance of stream ciphers and block ciphers used on a noisy link in a WSN after assessing a variety of symmetric key ciphers. In upcoming research, examine the ciphers' properties and the impact of the link quality whenever used in WSNs.

The publication of A Scheme for Key Revocation in Wireless Sensor Networks [13] by Subhankar Chattopadhyay et al. Automated key revoking currently has one single point of failure. This paper addresses a decentralized key revoke technique that relies on a vote mechanism for key restoration.It demonstrated the ability to effectively revoke every of a corrupted node's keys across the whole network. A time and expense of storage associated with revoking a node that has been compromised may be further reduced in the future by using another method such as a voting approach. Future developments can also be developed to lower the expense of communication and computing.

In a different study (Burhanuddin et al.), the authors suggested a safety protocol for protecting communication across networks [14]. They suggested a 3-factor authorization technique using an elliptic curve approach. This plan's major goal is to lessen the burden on interaction and computing on the network's sensors. Additionally, the authors provide an in-depth evaluation of multiple characteristics and suggested an authentication system made up of two distinct authentication processes for two distinct registrations of nodes in connections; both authentication techniques in the suggested method proved to be a more effective security measure. The suggested algorithm is better suited for IoT-based components,

too. In comparison to DES along with other safety protocols, the technique suggested has a two-stage hybrid cryptographic method that is appropriate for substance and high-level services and offers security against multiple threats, adaptability, practicality, a lower memory usage, a shorter execution time, an extensive discovering curve, and an affordable cost.

4.3 Machine Learning in WSN

An effective method for lowering the cost of several security-related sectors is provided by ML technology. For instance, identifying anomalies produced great results when used in packet evaluation, monitoring, and DoS defense against all forms of hostile behavior. The ML technique is also used in the processes of increasing network accessibility, recognizing errors, and congestion due to traffic.It may be a good option in addition to the physical layer's procedures for authentication. In order to address several of these issues and offer enormous benefits in regards to adaptability and precision, ML approaches are being applied in WSNs.

In order to enhance DoS identification and reduce power usage in WSNs, authors in [15] presented a novel model. In addition, a brand-new cluster model for the LEACH protocol was suggested by the researchers in order for splitting relaying messages among WSN nodes. Following which, they enhanced DDoS recognition by using selecting features and a classification method. Another method for reducing the number of elements in a collection of data is through feature hiring, which involves choosing the most crucial characteristics to be trained and discarding the remainder. The authors also tried to calculate the power usage of their suggested method on WSN and discovered a 5% increase in the use of energy. The decision tree, which yields a 100% accurate answer, is one of the greatest machine learning strategies for defending wireless sensor networks from DoS, according to the authors.

A novel approach to increase the lifespan of networks paired with detection of breaches effectiveness was put forth by the authors in [16]. The researchers suggested an adaptive chicken swarm optimization methodology to reduce a WSN node's energy use, and they employed two tiers of the SVM technique for recognizing intrusions. The SVM is going to be utilized to examine packets at the next level after being used to identify the harmful node at the initial stage. Although the paper addressed the issue of extending WSN lifetime, the findings do not provide any justificationsfor the amount of energy that the suggested solution has saved.

A novel hybrid classification that blends deep learning with conventional machine learning methods has been suggested by the authors in [17]. To enhance the detection of intrusions in WSNs, the proposal combined the LTSM approach with a Gaussian Bayes model. The suggestion in contrast combined the Genetic Algorithm (GA) into the MLP model.

In addition, neither learning by reinforcement [18] nor transfer learning were discussed in any of the research examined in the domains of use of ML to assist with the safety of WSNs. Such methods are frequently used in the future of machine learning. Transferal learning is based on pre-trained models, whereas reinforcement learning involves experience-based learning rather than data-based training. Therefore, both approaches can be tried in open problems as well as SDN.

4.4 Blockchain in WSN

In comparison to the current WSN system that uses a trusted third party (TTP), the blockchain-based WSN (BWSN) system offers improved reliability and safety. A trustworthy distributed system for storing sensory data is offered by BWSN. As a result, there is no single-point-of-failure (SPF) issue.

Feng et al. [19] examined the security issue with the current WSN system and suggested a blockchain-based collocation storage architecture for the sensed data processing platform. The suggested structure comprises of an asymmetric signature scheme and a hierarchical Byzantine Fault Tolerant (BFT) consensus algorithm in the WSN-approved blockchain. Simulations and experimentation revealed that the recommended design and scheme produce outstanding quality with high security. They confirmed that the suggested plan enables blockchain to function as a service option for WSN's distributed storage system.

Youssef et al. suggested a network topology made up of a cloud of unmanned aerial vehicles (UAVs) and a cloud of sensors for the observation of dam sites. Sensing data is collected by the sensor cloud, and data delivery to the dam monitoring center (DMC) is handled by the UAV cloud. The solution that is being suggested is based on Blockchain technology, which offers storage of data, authorization, reliability of data, tracking, and payment of the entities used for sensing and delivering activities. A computational model is run and the information delivery delay ratio is calculated to assess the suggested system. The findings indicate that as the intergeneration time of alerts rises, the delay ratio falls and that as a result, less data is produced and the delivery delay lowers [20].

In order to avoid the concerns with the void hole and additional energy use, Mateen et al. proposed a blockchain-based WSN and two routing protocols, increasing the network lifetime. The recommended protocols are contrasted with the current protocols for evaluation. The systems that were suggested outperform comparable ones according to the simulation findings [21].
A multi-WSN security system for IoT based on blockchain was presented by Cui et al. . According to the variations in their capabilities, IoT nodes are categorized as cluster head nodes, regular nodes, and base stations that are used to create an ordered network. A hybrid blockchain approach with a local and public chain is created from various sorts of nodes. This hybrid approach implements mutual authentication of nodes in a variety of communication instances, while the identity authentication of cluster head nodes is implemented in a public blockchain and ordinary nodes are implemented in a local blockchain. The effectiveness of a safety system is assessed, and the results demonstrate that the proposed plan delivers superior performance with thorough security. [22].

Summary of the study on existing works

The combination of Machine Learning (ML) and Blockchain Technology offers significant advantages in Wireless Sensor Networks (WSNs), particularly in optimizing key Quality of Service (QoS) metrics such as delay, throughput, jitter, packet loss, and energy efficiency.
Reduced Delay through Optimization: Machine Learning can analyze network conditions in real-time and predict the most efficient paths for data transmission. This minimizes transmission delays by avoiding congested routes. Moreover, Blockchain consensus mechanisms (like Proof of Stake or Delegated Proof of Stake) can be optimized using ML to speed up block validation, further reducing delays.
Enhanced Throughput via Efficient Data Management: ML algorithms enhance throughput by optimizing the routing of data and balancing network loads, ensuring smoother and faster data flow. Blockchain complements this by securely validating and distributing data packets across the network, reducing disruptions and improving throughput consistency.
Reduced Jitter with Predictive Analytics: Jitter, or variations in packet arrival times, is minimized by ML's real-time network monitoring and adaptive routing strategies. Blockchain's synchronized ledger system helps maintain uniform data propagation across nodes, reducing fluctuations in transmission times.
Minimized Packet Loss through Anomaly Detection and Integrity Assurance: ML detects network anomalies, such as failures or attacks, that could lead to packet loss, allowing for immediate corrective actions like rerouting. Blockchain further ensures that data remains intact and untampered, providing a secure, immutable record that minimizes the risk of packet loss due to malicious interference.
Energy Efficiency through Optimization: Although ML and Blockchain can be energy-intensive, ML is used to optimize sensor operations by processing only essential data, reducing unnecessary energy consumption. Additionally, Blockchain can employ energy-efficient consensus mechanisms like Proof of Authority (PoA) or hybrid PoS, reducing the need for energy-heavy mining processes.
Combining Machine Learning and Blockchain in WSNs offers notable improvements across critical QoS metrics. ML optimizes network performance by reducing delay, jitter, and packet loss, while Blockchain ensures secure data management and adds energy-efficient consensus mechanisms. This powerful synergy results in a more secure, efficient, and reliable WSN.

CONCLUSION

The development of WSNs, which constantly sense the necessary parameters, has been facilitated by advances in the field of computer technology. Block chain-based WSN algorithms have recently attracted a lot of attention. The bandwidth, power, and resources of these networks are constrained during point-to-point communication. One brilliant solution to this issue is data collection. How to analyze vital data in a way that uses less energy is a major issue in sensor networks.As a result, different data consolidation algorithms were applied, which are discussed in this work, to reduce the power usage. In this study, the various data consolidation methodologies provided in earlier works are given after reviewing the existing works outlining the function of machine learning and block chain in WSN. The network's advanced security, higher QoS, and energy conservation are the main goals of data consolidation approaches.

REFERENCES

[1] Khan R A and Muhammad A T 2018 A Survey on Wired and Wireless Network Internationaljournal of communication network 5(7) 450-461.
[2] Patel A, Ghaghda S and Nagecha P 2014 Model for security in wired and wireless network for education International Conference on Computing for Sustainable Global Development(INDIACom) pp 699-704.

[3] Yick J, Mukherjee B, and Ghosal D 2008 Wireless sensor network survey Computer Networks52(12) 2292-2330
[4] Kaur N, Bedi R K, Gang,M. Welsh, D. Myung, M. Gaynor, and S. Moulton. "Resuscitation monitoring with a wireless sensor network," in Supplement to Circulation: Journal of the American Heart Association 2013.
[5] A.K. Pathan, H. Lee, C. S. Hong, "Security in Wireless Sensor Networks: Issues and Challenges", ICACT, pp: 1043 – 1048, 2006.
[6] D. Carman, P. Krus, and B. Matt. "Constraints and approaches for distributed sensor network security." Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood. Communications Magazine, pp. 102-114, 2010.
[7] Shen S., Yue G., Cao Q., Yu F. A survey of game theory in wireless sensor networks security. J. Netw. 2011;6:521–532.
[8] Yuan, H.-Y., Dai, J.-G., & Li, X.-L. (2007). An energy-efficient clustering algorithm in wireless sensor networks. Chinese Journal of Sensors Actuators, 20(12), 131–142.
[9] Mohamed, R.E., Saleh, A.I., Abdelrazzak, M. et al. Survey on Wireless Sensor Network Applications and Energy Efficient Routing Protocols. Wireless Pers Commun 101, 1019–1055.
[10] Dong R., Liu L., Liu J., Xu X. Intrusion detection system based on payoff matrix for wireless sensor networks. Proceedings of 2009 3rd International Conference on Genetic and Evolutionary Computing (WGEC 2009); Guilin, China. 14–16 October, 2009
[11] Pugliese M., Santucci F., Pair-wise Network Authenticated Hybrid Cryptographic Keys for Wireless Sensor Networks using Vector Algebra, 4th IEEE International Workshop on Wireless Sensor Networks Security (WSNS2008), Atlanta, Sep. 2008
[12] Xueying Zhang, Heys, H.M. ; Cheng Li ," Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks", Communications (QBSC), 25th Biennial Symposium.
[13] Subhankar Chattopadhyay et.al, "A Scheme for Key Revocation in Wireless Sensor Networks", International Journal on Advanced Computer Engineering and Communication Technology (IJACECT) in 2010.
[14] Burhanuddin M, Mohammed AA-J, Ismail R, Hameed ME, Kareem AN, Basiron H, A review on security challenges and features in wireless sensor networks: IoT perspective. J Telecommun Electron Comput Eng 10(1-7):17–21
[15] Ahmad R., Wazirali R., Bsoul Q., Abu-Ain T., Abu-Ain W. Feature-Selection and Mutual-Clustering Approaches to Improve DoS Detection and Maintain WSNs' Lifetime. Sensors. 2021;21:4821.
[16] Borkar G.M., Patil L.H., Dalgade D., Hutke A. A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: A data mining concept. Sustain. Comput. Inform. Syst. 2019;23:120–135.
[17] Wu D., Jiang Z., Xie X., Wei X., Yu W., Li R. LSTM Learning with Bayesian and Gaussian Processing for Anomaly Detection in Industrial IoT. IEEE Trans. Ind. Informat. 2020;**16**:5244–5253. doi: 10.1109/TII.2019.2952917.
[18] Tan C., Sun F., Kong T., Zhang W., Yang C., Liu C. International Conference on Artificial Neural Networks. Volume 11141. Springer; Cham, Switzerland: 2018. A Survey on Deep Transfer Learning; pp. 270–279.
[19] Feng, L., Zhang, H., Lou, L., & Chen, Y. A Blockchain-Based Collocation Storage Architecture for Data Security Process Platform of WSN. In 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design ((CSCWD)) (pp. 75-80). IEEE. (2018, May).
[20] Youssef, S. B. H., Rekhis, S., &Boudriga, N. A Blockchain based Secure IoT Solution for the Dam Surveillance. In 2019 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 1-6). IEEE. (2019, April).
[21] Mateen, A., Javaid, N., & Iqbal, S. (2019). Towards energy efficient routing in blockchain based underwater WSNs via recovering the void holes (Doctoral dissertation, MS thesis, COMSATS University Islamabad (CUI), Islamabad 44000, Pakistan).
[22] Cui, Z., Fei, X. U. E., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid BlockChain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing, 13(2), 241-251.