Systematic Analysis of Artificial Intelligence-Driven Trust-based Authentication Schemes for Wireless Sensor Networks

Rajesh. L[1*], *Girish Kumar.*D[2], *Pani* Rama Prasad. P[3], *Siddanna.* S R[4], and *Abhilash.* C N[5]

[1]Department of Information Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bengaluru, India
[2]Master of Computer Applications, Ballari Institute of Technology and Management, Ballari, India
[3]Department of Computer Science and Engineering, Ballari Institute of Technology and Management, Ballari, India
[4]Department of Information Science and Engineering, SJB Institute of Technology, Bengaluru, India
[5]Department of Artificial Intelligence and Machine Learning, SJB Institute of Technology, Bengaluru, India

Abstract. Wireless Sensor Network (WSN) is a system of distributed, autonomous sensors thatare used to monitor the environmental and physical conditions, like sound, pressure, and temperature, and share the information over a network to the sink nodes or a central location.As the data is exchanged over an insecure channel, they are vulnerable to various attacks or manipulations, and hence,network security plays a significant part in the WSN. Thus, a secure authentication protocol is essential to avoid security issues in WSNs. Moreover, the authentication process verifies and identifies devices, like users and nodes, before transmitting the data. This survey presents a review of the varioustrust-based authentication schemes in WSN. Further,the approaches are categorized as Deep Learning (DL) models, Cryptography frameworks, Multifactor authentication techniques, and other modelsare assessed to identify their ability to optimize network security. The articles analyze the papers published between 2018 and 2025, focusing on research methods, the efficiency of the proposed models, performance assessments, and publication years. Additionally, the assessment offers valuable insights for incorporating new techniques to enhance efficiency in trust-based authentication schemes for WSNs.

1 Introduction

WSN is made up of low-cost, autonomous, and low-energy sensor nodes, which collect information about the environment and later forward the sensed information to the centralized backend units known as sinks or base stations, which are mainly utilized for processing and sensing data. The foremost function of the WSN is gathering information, monitoring the fields, and sharing the information with the access points for preprocessing tasks [14]. Due to the ease of deployment, cost-effectiveness and compactness of the WSN, it is considered an efficient technique for several real-time applications. Depending on the high trust value, the Cluster Head (CH) selection is performed in the WSN to avoid attacks on the nodes. Hierarchical routing and clustering are significant for prolonging the WSNs' lifespan and conserving power [12].

Some of the attacks encountered by the WSN are the node capture attack, sinkhole Sybil attack, Denial-of-Service (DoS), hello flood attack, and selective forwarding attack [12]. The malicious nodes have to be isolated from the other nodes to minimize the tampering and illegal activities occurring in the network, in order to minimize the accuracy of the trust values [1]. The foremost technology utilized to address this problem is the utilization of the authentication systems, which represent the mutual authentication between the sensor and user, and to avoid illegal activities by third parties [7]. The process of trust analysis is an important task in the WSN, as the trust scores change due to different types of attacks occurring at various times in diverse paths. Trust value depends on the present and past behavior of the nodes. Additionally, the trust values can be enhanced by taking into account the trust value shared by the neighboring nodes and the estimated trust values. Meanwhile, a coordinator for communication, or a centralized trust controller, is essential to perform mutual authentication by encrypting the identities and validating them by generating keys.

This kind of authentication is based on dynamic trust modeling, and here the examination of present and past data is done to carry out the prediction of future behavior, consideration of neighbor opinions, and improved security by utilizing key sharing and verification. Distributed key management and centralized key management methods are exploited to achieve user authentication more efficiently. Various kinds of authentication mechanisms utilize user credentials, like Internet Protocol (IP) address, Captcha, user name, and password, for performing the initial steps in the authentication process [1].The Physical (PHY)layer authentication effectively handles the tradeoff between low latency and security needed in the WSN and attains lightweight authentication [2]. As authentication takes place over public channels, they are

*Corresponding author: rajesh-ise@dsatm.edu.in

vulnerable to eavesdropping and other methods that permit intruders to obtain the message exchanged during the communication [20]. Hence, the strong mutual authentication mechanisms address the security issues and validatethe individual received message. User authentication is implemented among all users and sensors before these session keys are exchanged. Next, these session keys are mostly exploited for encrypting sensitive data to avoid illegal access in the network [5].

This survey examines the various approaches exploited for trust-based authentication schemes for WSNs. The frameworks are divided into four categories: DL-based methods, Multifactor authentication-based models, Cryptography-based approaches, and other approaches. Moreover, this survey highlights the analysis of the current articles considering the implemented tools, publication, and performance metrics. This survey details the limitations in the prevailing models, recognizes the research gaps in articles, and offers directions for future developments in trust-based authentication schemes, particularly in the field of WSN.

The details of this survey is ordered as follows: the outline of the Trust-based Authentication Schemes in WSN is embodied in section 2, section 2.1 illustrates the various prevailing techniques exploited for Trust-based Authentication Schemes in WSN, Section 3 presents the detailed literature review of these approaches, and section 4 details the research gaps and limitation of the reviewed methodologies. Further, the examination of the research, including insights into evaluation metrics, employed datasets, tools applied, and accuracy of machine learning algorithms, is exemplified in section 5, and section 6 represents the conclusion part.

2 General outline of trust-based authentication schemes in WSN

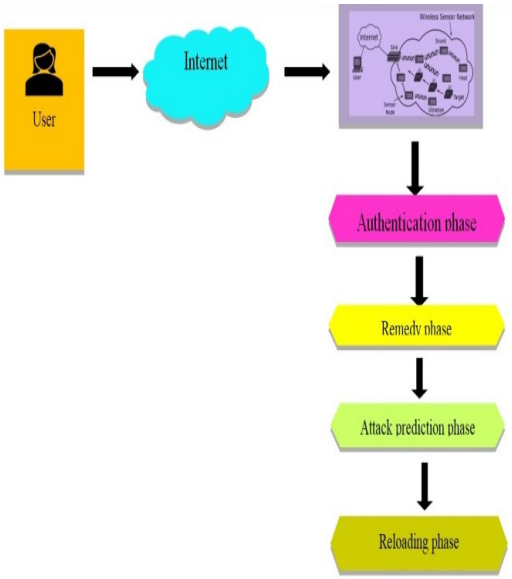

Fig. 1. A pictorial representation of the authentication schemes in WSN.

In WSN [16], authentication schemes serve as a security measure, in which the users cooperate with each other to introduce trust and authenticate data. The users play an essential part in the network operation and security, and the internet aids the users in establishing a path for data aggregation, external communication, control, and monitoring of WSN. The internet permits the incorporation of the WSN with other systems. Later, the data are uploaded to the cloud, where computing resources are used to optimize the security, scalability, and management of the WSN. The amalgamation of the WSN with cloud computing leads toa centralized platform, wherein the data gathered by using the sensor nodes can be later examined, processed, and saved. The sensor nodes have the ability to preprocess, sense, and communicate data to the Base Station (BS). Four distinct phases, namely the remedy phase, reloading phase, and attack prediction, are included in the authentication schemes in WSN. In the authentication phase, the devices present in the network detect the other nodes and permit them to exchange and communicate data. This phase helps to avoid malicious attacks like data injection and spoofing. Next, the remedy phase is exploited to enhance the security and integrity of the network after the identification of the illegal intrusion. In the attack authentication phase, the security threats or attacks occurring in the networks are detected, and preventive measures are taken to ensure that the WSN's integrity is maintained effectively. At last, the reloading phase is utilized for reinitializing the security systems and credentials in the network to secure the functionality and efficiency of the data. Figure 1 portrays the pictorial representation of the authentication schemes in WSN.

2.1 Categorization of trust-based authentication schemes in WSN

The Trust-based Authentication Schemes in WSN can be categorized into various kinds, including DL-based methods, Cryptography-based approaches, Multifactor authentication-based approaches, and other methods. Figure 2 displays the categorization of trust-based authentication schemes in WSN.

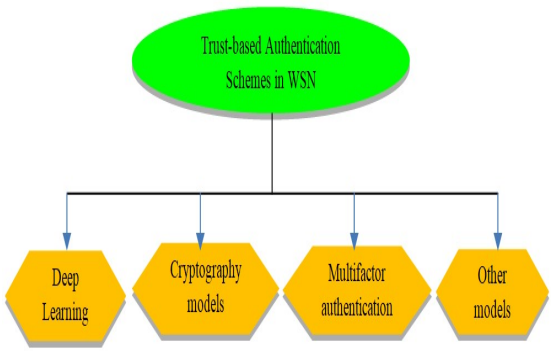

Fig. 2. Categorization of trust-based authentication schemes in WSN.

3 Literature survey

This section establishes distinct techniques exploited for performing trust-based authentication schemes in WSN. The methods reviewed in this article are categorized into

four groups, namely Multifactor authentication-based approaches, DL-based approaches, Cryptography-based methods, and other methods, which are elaborated in the upcoming sections.

3.1 Deep learning-based techniques

The DL is considered a branch of artificial intelligence (AI) and also a subset of Machine Learning (ML). DL uses Artificial Neural Networks (ANN) for efficient authentication with low resource consumption. The DL system is used for automatically capturing the features and patterns from the vast amount of data without developing any special programs for all tasks. In this section, the various DL frameworks applied for the examination of trust-based authentication schemes in WSN are explained.

Kalidoss, T., et.al.[1] presented the Energy Efficient Routing Protocol algorithm for enhancing energy utilization and improving the security of WSN. In this approach, the trust modeling utilized the authentication approach with a key-based security mechanism for enabling the trust scores. Further, the three different kinds of trust scores, indirect, direct, and overall trust scores, were measured to improve communication security. Then, the cluster-based secure routing algorithm was carried out to choose the CH based on trust scores and Quality of Services (QoS) metrics. In the end, the final path was chosen for efficiently securing the routing process based on hop count, path-trust, and energy. This approach efficiently enhanced the routing performance and minimized the energy consumption and delay.

Liao, R.F., et al. [2] proposed a DL-based physical (PHY) layer authentication framework to enhance the security of Industrial WSNs (IWSNs). The techniques were utilized to establish the proposed approach. Particularly the authentication of sensor nodes with the aid of Convolutional Neural Networks (CNN), Convolution Preprocessing Neural Networks (CPNN), and Deep Neural Networks (DNN) method of authentication. Among them, the enhanced CPNN-based method supported a lightweight multi-node PHY-layer authentication, incurred minimal latency, and demanded limited computational resources. This method provided a superior performance, efficiently solved the issue of high training time, and sped up the convergence.

Althubiti, S.A., [5] developed the Salp Swarm Optimization with Deep Belief Network Based Trust Aware Authentication (SSDBN-TAA) technique for optimizing authentication and security in WSN. Initially, the developed approach exploited a weighted clustering technique to categorize the network into a group of clusters. Next, the Salp Swarm Algorithm (SSA) -based hyperparameter tuning process and DBN-based threshold value selection were utilized to enable effective authentication of nodes in WSN. Later, the trust factor was mutually introduced among the nodes present in the network. At last, the SSDBN approach selected the threshold trust value, and the SSA was utilized for optimally adjusting the hyperparameters of DBN. This model ensured enhanced authentication and security in the WSN, exhibited reliable and robust communication, and minimized the vulnerabilities to malicious attacks.

The Elliptic Curve Cryptography (ECC) model with the Optimized Recurrent Neural Network (RNN) model was presented by Pushpa, S.X., and Raja, S.K.S., [16] for ensuring security in WSN. Moreover, the introduced approach was implemented in the attack prediction phase, and the detection of the Denial-of-Service (DoS) attack was performed by the Optimized RNN approach. Then, the Shark Smell Optimization with Opposition Learning and Mutation Process (SSOL-MP) was used for training the RNN. This framework improved the security of the system and reduced the computation cost.

3.2 Cryptography-based models

Cryptography schemes are exploited for authenticating the information in digital environments. This scheme normally depends on protocols and algorithms for protecting sensitive data from tampering, forgery, and unauthorized access. Several methodologies employed for exploring the trust-based authentication schemes in WSN are presented as follows,

Lightweight user authentication and key agreement scheme were presented by Zhao, X. and Li, D., [8] for multi-gateway-based wireless sensor networks using the Rabin cryptosystem. The introduced approach utilized lightweight cryptographic primitives, namely encryption of Rabin, XOR operation, and hash function, for minimizing the overhead. The proposed model had better confidentiality and authentication through provable security, formal analysis, and informal analysis. Moreover, the lightweight user authentication and key agreement framework was optimized for achieving forward secrecy. The proposed scheme achieved higher security with low computational overhead.

Erskine, S.K., [9] derived the Secure Data Aggregation using Authentication and Authorization (SDAAA) protocol for detecting malicious attacks in the WSN. The introduced technique included a node authorization algorithm, which permitted he authorized nodes to interact with the network. Later, a mathematical model was introduced to improve the data freshness, authorization, accuracy, and energy efficiency of the approach. The SDAAA enhanced the QoS parameters and handled the malicious node activities effectively.

Phalaagae, P., et.al.[12] established the Randomized Bi-Phase Authentication Scheme (RBAS) framework for enhancing the security of the data. Further, the RBAS approach was combined with a digital watermarking and advanced cryptography approach to strengthen the internal as well as external security of the network. The RBAS model applied dynamic verification codes, advanced hashing, and cryptography to assure data authenticity and strong error detection, and utilized robust randomization and Cyclic Redundancy Check (CRC) codes to thwart potential attacks. This model achieved a low packet loss rate and optimized energy efficiency.

Sai, K.S., et.al.[15] developed the Elliptic Curve Diffie-Hellman (ECDH) secure communication method for WSN communication using a Message Passing Interface (MPI) parallel program platform. The developed security framework operates in three phases, namely, secure communication, sensor fusion, and sensor data generation. Further, the Linux P thread was employed for the execution of the ECDH approach for all sink nodes and single sink nodes by using a parallel thread to enhance the complete execution time. The utilization of the Linux P threads in the ECC execution maximized the overall execution time. This method enhanced the security and efficiency of the system.

The Attack-Resistant Proxy-Based Path Key Establishment scheme (APPK) and the Attack-Resistant Disjoint-Based Path Key Establishment scheme (ADPK) were proposed by Alimoradi, P., et al. [18] for WSN hierarchical key management and authentication. To find the attack coefficient of the sensor nodes based on their current location in the sensor field, an Attack Matrix (AM) was designed. Due to its highest value of key recovery probability, the APPK was primarily attacked. With reduced path compromise ratio, the ADPK minimized the effect of node capture. The strategy provided improved performance and security.

The Hybrid Key Management Scheme was designed by Sharmila, Kumar, P., [4] to generate key pre-distribution keys in the authentication methods. This scheme exploited the hash function and ECC to produce the pre-distribution keys. Next, the Key establishment was performed by broad casting the identity of the node. In the establishment phase, the amalgamation of hybrid methods in the key pre-distribution approach is exploited for achieving mutual authentication among the sensor nodes. This model minimized the computational complexity with higher security, effectively reduced the latency, and exhibited less energy consumption.

The WSNs-Secure and Lightweight Mutual Authentication Protocol (WSN-SLAP) was derived by Kwon, D.K., et.al. [7] to prevent security vulnerabilities in the WSN. The WSN-SLAP provided mutual authentication and perfect forward secrecy for improving the security of the WSN. Further, the XOR operations and hash function were utilized to extract the efficiency features. The formal security analyses, like Burrows-Abadi-Needham (BAN) logic, Automated Verification of Internet Security Protocols and Applications (AVISPA), and the ROR model, were exploited for determining the security of the WSN-SLAP. This technique provided more efficient and secure communication services.

3.3 Multifactor authentication-based approaches

The Multifactor authentication method is considered a security mechanism that requires users to offer two or more different forms of authentication, previously attaining access to a service or system. Several types of Multifactor authentication-based methods have been used for analyzing trust-based authentication schemes in WSN, as discussed below as,

Renuka, K., et al. [6] designed a three-factor authentication scheme that maintains anonymity for evaluating real-time data directly from the sensor nodes of the WSN. The Das protocol security was enhanced by leveraging the anonymity-preserving three-factor authentication process. The use of the random oracle concept increased the security of the protocols that were developed. Improved performance was provided by the anonymity-preserving three-factor authentication scheme, with the communication and computation costs decreased little. The proposed paradigm optimized performance efficiency and improved protocol security.

Zheng, Y., [10] designed the lightweight secure group key agreement protocol based on a Physical Unclonable Function (PUF) for hierarchical WSNs. The method applies a secure group session key and group authentication for each participating member without using cumbersome public-key algorithms. By hiding the prover's authentication secrets within a secure mask, the verifier did not need to save the secrets but recovered them for authentication by querying its PUF. The proposed model resisted stolen-verifier attacks at the CH and took advantage of lightweight cluster-head authentication at the sensor node. Such a scheme demonstrated outstanding overall computation and communication performance.

The secure two-factor authentication scheme was designed by Mo, J., et.al.[17] to ensure the security of the networks. The Chebyshev chaotic mapping approach was utilized to provide forwarding secrecy and enhance the security and efficiency of session key negotiation. Later, the fuzzy verifier method was used for preventing attackers from offline guessing attacks and resisting smartcard loss attacks. Finally, the heuristic security analysis and BAN logic proof were utilized for preventing the known attacks, accomplishing the key agreement, and mutual authentication. This technique attained the desired security features and maintained better efficiency.

Mo, J., and Hu, Z. [13] introduced the enhanced three-factor user authentication and key agreement protocol based on Chebyshev chaotic mapping for security improvement in WSN. First, the fuzzy verifier technique was utilized to shield the attacker from an offline guessing attack against the user password and identity. Then, the anonymity of the user and sensor was protected by the dynamic identity mechanism to evade the desynchronization attack. Afterwards, the Chebyshev chaotic mapping was utilized to minimize the computation overhead and improve security. This method addressed the security threats but also obtained a more optimal trade off between security and efficiency, hence it was suitable for user authentication in WSNs.

Feng, H. and Cai, B., [20] introduced aprovably secure two-factor authentication protocol for ensuring network security and data integrity in WSN. The two-factor authentication mechanism and Chebyshev chaotic map were utilized in the proposed model to enhance authentication efficiency and optimize security in WSNs. The provably secure two-factor authentication protocol facilitated secure and efficient communication in WSNs across diverse applications.

3.4 Other methods

This section presents a review of works that utilize techniques that exclude the Multifactor authentication-based approaches, DL, and Cryptography-based methods.

Gao, N., et al.'s collaborative neighbor selection method [3] offers defenses against advanced location spoofing attacks. First, the feasibility of the smart attack was investigated and evaluated in the context of the networks' possible threats. Next, to calculate the worst-case scenario for the protectors, the optimal transmit power allocation was constructed. Here the attacker exploits beamforming with optimal power allocation for transmission to learn the intelligent attack action. Eventually, the cooperative PHY-layer authentication method was employed to offer low overhead and high accuracy protection against such an intelligent attack. This model accelerated belief convergence, decreased the overhead, and essentially enhanced the performance of the detection.

The Genetic Algorithm was proposed by Zhang, J., [11] for the secure routing protocol in WSN. Initially, the generation of the biometric key was performed using the genetic algorithm associated with hash function for generating the biometric key. Further, the fuzzy extraction technology was utilized to obtain the user's biometric key. In the base station, the authentication key and encryption key are utilized to improve the network communication security. This approach exhibited a good balance between energy saving and consumption by adding an energy balance module and attained better security and packet delivery rate at low delay.

An effective lattice-based random broadcast authentication system was developed by Yu, W., [19] in order to determine the WSN's mobility. The presented strategy assisted in preventing the quantum assault and was based on the Small Integer Solution (SIS) problems. This approach introduces the two distinct broadcast authentication processes: one-to-many broadcast authentication and one-to-one broadcast authentication. One-to-one and one-to-many broadcast authentication, two distinct types of broadcast authentication, were both taken advantage of in the presented method. The system successfully enhanced communication and authentication while reducing computing overhead.

4 Research gaps and limitations

The challenges and research gaps faced by the methods for evaluating trust-based authentication schemes in WSN are explained as,

The difficulties encountered by the DL models are explained below. The Energy Efficient Routing Protocol algorithm in [1] did not include the application of the fuzzy rules to handle the uncertainty in the WSN. The DL-based PHY layer authentication framework [2] did not address the enhancement of the proposed technique for maintaining low latency and providing high authentication accuracy. The SSDBN-TAA model [5] did not consider lightweight cryptographic solutions to secure the communication.

The SDAAA protocol [9] did not consider the mobility model to explore further state-of-the-art QoS metrics, with different data markings applicable to that situation. The ECDH approach [15] didn't consider the improvement of the WSN system to speed up the independent sequential processes by utilizing parallel computation and failed to explore the trusted third party to handle the key-related problems. TheECC with the optimized RNN model [16] failed to evaluate the processing cost and did not consider the more distributed cloud environment in WSN. The ADPK and APPK approach [18] didn't explore dynamic network environments, such as mobile sensor networks, where nodes frequently change positions. The Hybrid Key Management Scheme [4] failed to explore the implementation of the federated learning algorithm to aggregate the data received from each sensor node and update the global data to the cloud.

The issues encountered by the Multifactor authentication method are outlined below. The anonymity-preserving three-factor authentication protocol [6] failed to explore the security requirements of multi-factor protocols in WSN to enhance the energy efficiency of the approach. The lightweight secure group key agreement protocol using a PUF [10] failed to investigate the dynamic group membership, which enables the new nodes to join the group or existing nodes to exit the group. The secure two-factor authentication scheme [17] failed to utilize advanced public key algorithms to improve the performance of this protocol and reduce the runtime of the public operation. The improved three-factor user authentication and key agreement protocol using Chebyshev chaotic mapping [13] did not explore additional security measures to address emerging threats, such as advanced insider threats or quantum computing attacks. The WSN-SLAP [7] did not consider the whole network and secure protocol to design a new scheme in the WSN. The provably secure two-factor authentication protocol [20] did not consider blockchain technology for enhancing the security of the data.

The challenges faced by the other methods are described below. The cooperative neighbor selection algorithm [3] failed to explore the effect of non-Gaussian noise on measurements in the practical systems and failed to validate the effectiveness of the cooperative PHY-layer authentication scheme in mobile WSNs. The Lightweight user authentication and key agreement scheme [8] approach failed to investigate the advanced cryptographic techniques to strengthen the scheme against emerging threats, such as quantum computing-based attacks. The Genetic Algorithm [11] did not use adaptive algorithms to maintain security even in large-scale deployments. The RBAS [12] failed to consider the improvement of the security mechanisms to address new threats and did not investigate cost-effective deployment strategies crucial for successful real-world deployment. The efficient lattice-based random broadcast authentication protocol [19] failed to support the fully homomorphic encryption and flexible partially hidden predicate encryption policy to improve the efficiency of the developed approach.

5 Results and investigation

This section emphasizes a comprehensive investigation of the numerous techniques oftrust-based authentication schemes in WSN by mainly focusing on the publication data, datasets, metrics, and tools considered in these models.

5.1 Assessment based on methodologies

The techniques utilized for establishing trust-based authentication schemes in WSN include Cryptography-based methods, Multifactor authentication-based approaches, DL-based approaches, and other methods.

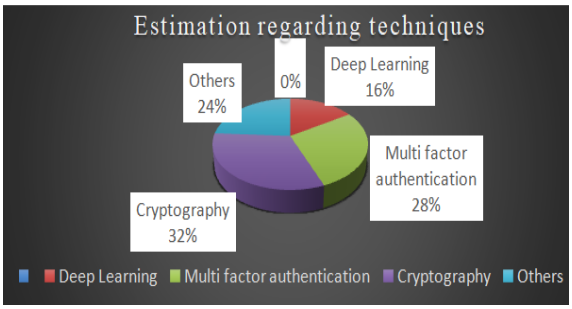

Fig.3. Examinations regarding the techniques.

Figure 3 shows the examination based on the techniques for trust-based authentication schemes in WSN. Among the methods studied, 16% of the papers exploited DL approaches, 28% employed multi-factor authentication models, 24% used other approaches, and 32% utilized cryptography methods. The cryptography approaches were widely exploited for trust-based authentication schemes within WSN.

5.2 Evaluation regarding tools

The valuation of the numerous approaches for trust-based authentication in WSN regarding the tools is illustrated in Figure 4. Tools utilized for executing the trust-based authentication schemes in WSN are MATLAB, NS2 simulator, and OMNET++ simulator. In Figure 4, NS2 simulator is the most frequently utilized tool for establishing trust-based authentication in WSN, while the other tools were used in only one paper each.

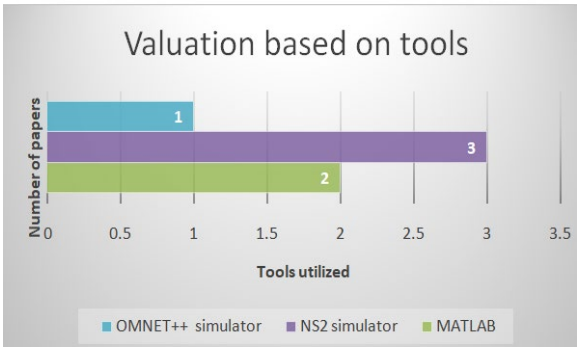

Fig.4. Analysis with respect to tools.

5.3 Valuation in terms of publication year

The investigation of the research papers exploited for trust-based authentication schemes in WSN across distinct years is illustrated in the Figure 5. The analysis shows that1 article was published in 2018, while 2 papers were published in 2019 and 2020. Six papers were taken from the year 2022, and 3 papers were published in the year 2021. Further, seven papers were published in the year 2023, and 4 papers were published in the year 2024.

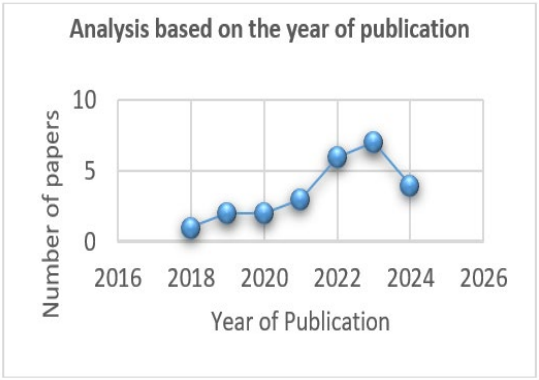

Fig.5. Investigation with respect to the publication.

5.4 Evaluation based on algorithms

Figure 6 investigates performance of machine learning algorithms based on trust authentication. The effectiveness of Tabu Search optimization for RF intrusion detection in WSNs was effectively demonstrated by the authors. They developed an optimized model that greatly enhanced performance on every metric they looked at. A large dataset from WSN-DS, comprising 19 features and 374,661 instances, was used for this. The accuracy improved as a result of these methods [14].

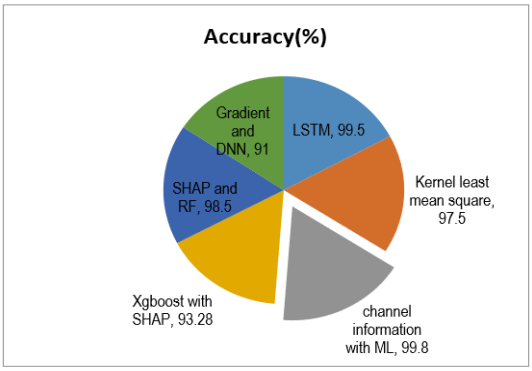

Fig. 6. Summary of machine learning algorithms performance based on trust authentication.

6 Conclusion

This survey provides a detailed overview of numerous techniques utilized for performing trust-based authentication schemes in WSN. Moreover, 25 research articles focusing on trust-based authentication systems in WSN were examined and categorized as Cryptography frameworks, Multifactor authentication

techniques, DL models, and other methods. Moreover, these articles are obtained from academic publishers, namely Springer, MDPI, Elsevier, Hindawi, IEEE, Taylor and Francis, and Wiley. The reviewed articles are investigated based on the publication year, tools, and evaluation metrics applied. Further, most of the research papers are obtained from the year 2023, and MATLABtools are the most commonly exploited tools in this survey. The delay and energy computation metrics are commonly applied in this survey. Furthermore, the NS2 simulator is a frequently utilized tool in the articles. The cryptography techniques play a prominent role in enhancing security and trust in various techniques for authentication in WSN. In addition to these, a detailed explanation of the issues confronted by these techniques is also provided. Future research will focus on dynamically exploring advanced techniques to improve these trust-based authentication systems in WSN.

References

1. T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, A. Kannan, QoS aware trust-based routing algorithm for wireless sensor networks. Wirel. Pers. Commun. **110**, 1637-1658 (2020). https://doi.org/10.1007/s11277-019-06788-y
2. R.F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, M. Cao, Deep-learning-based physical layer authentication for industrial wireless sensor networks. Sens. **19**, 2440 (2019). https://doi.org/10.3390/s19112440
3. N. Gao, Q. Ni, D. Feng, X. Jing, Y. Cao, Physical layer authentication under intelligent spoofing in wireless sensor networks. Signal Process. **166**, 107272 (2020). https://doi.org/10.1016/j.sigpro.2019.107272
4. Sharmila, P. Kumar, S. Bhushan, M. Kumar, M. Alazab, Secure key management and mutual authentication protocol for wireless sensor network by linking edge devices using a hybrid approach. Wirel. Pers. Commun. **130**, 2935-2957 (2023). https://doi.org/10.1007/s11277-023-10410-7
5. S.A. Althubiti, A trust-aware authentication scheme for wireless sensor networks optimized by salp swarm optimization and deep belief networks. Math. Probl. Eng. **2022**, 7842287 (2022). https://doi.org/10.1155/2022/7842287
6. K. Renuka, S. Kumar, S. Kumari, C.M. Chen, Cryptanalysis and improvement of a privacy-preserving three-factor authentication protocol for wireless sensor networks. Sens. **19**, 4625 (2019). https://doi.org/10.3390/s19214625
7. D.K. Kwon, S.J. Yu, J.Y. Lee, S.H. Son, Y.H. Park, WSN-SLAP: Secure and lightweight mutual authentication protocol for wireless sensor networks. Sens. **21**, 936 (2021). https://doi.org/10.3390/s21030936
8. X. Zhao, D. Li, A lightweight user authentication scheme for multi-gateway-based wireless sensor networks using Rabin cryptosystem. IEEE Access **11**, 79874-79889 (2023). https://doi.org/10.1109/ACCESS.2023.3300440
9. S.K. Erskine, Secure data aggregation using authentication and authorization for privacy preservation in wireless sensor networks. Sens. **24**, 2090 (2024). https://doi.org/10.3390/s24072090
10. Y. Zheng, W. Liu, C.H. Chang, A lightweight PUF-based secure group key agreement protocol for wireless sensor networks. In IEEE International Symposium on Circuits and Systems (ISCAS), IEEE, Monterey, CA, USA, July (2023), 1-5
11. J. Zhang, Network security situational awareness based on genetic algorithm in wireless sensor networks. J. Sens. **2022**, 8292920 (2022). https://doi.org/10.1155/2023/8292920
12. P. Phalaagae, A.M. Zungeru, B. Sigweni, S. Rajalakshmi, H. Batte, O.S. Eyobu, An energy-efficient authentication scheme for cluster-based wireless IoT sensor networks. Sci. Afr. **25**, e02287 (2024). https://doi.org/10.1016/j.sciaf.2024.e02287
13. J. Mo, Z. Hu, W. Shen, A provably secure three-factor authentication protocol based on Chebyshev chaotic mapping for wireless sensor networks. IEEE Access **10**, 12137-12152 (2022). https://doi.org/10.1109/ACCESS.2022.3146393
14. R. Ahmad, R. Wazirali, T. Abu-Ain, Machine learning for wireless sensor networks security: An overview of challenges and issues. Sens. **22**, 4730 (2022). https://doi.org/10.3390/s22134730
15. K.S. Sai, R. Bhat, M. Hegde, J. Andrew, A lightweight authentication framework for fault-tolerant distributed WSN. IEEE Access **11**, 83364-83376 (2023). https://doi.org/10.1109/ACCESS.2023.3302251
16. S.X. Pushpa, S.K. Raja, Enhanced ECC-based authentication protocol in a wireless sensor network with DoS mitigation. Cybern. Syst. **53**, 734-755 (2022). https://doi.org/10.1080/01969722.2022.2055403
17. J. Mo, Z. Zhang, Y. Lin, A practically secure two-factor and mutual authentication protocol for distributed wireless sensor networks using PUF. Electron. **14**, 10 (2024). https://doi.org/10.3390/electronics14010010
18. P. Alimoradi, A. Barati, H. Barati, A hierarchical key management and authentication method for wireless sensor networks. Int. J. Commun. Syst. **35**, e5076 (2022). https://doi.org/10.1002/dac.5076
19. W. Yu, L. Yang, S. Wang, New lattice-based broadcast authentication protocol for wireless sensor networks. Secur. Commun. Netw. **2022**, 6809875 (2022). https://doi.org/10.1155/2022/6809875
20. H. Feng, B. Cai, A provably secure and lightweight two-factor authentication protocol for wireless sensor network. Electron. **13**, 4289 (2024). https://doi.org/10.3390/electronics13214289