DOI: https://doi.org/10.46632/jeae/1/2/6

Journal on Electronic and Automation Engineering
Vol: 1(2), 2022
REST Publisher; ISSN: 2583-6951
Website: http://restpublisher.com/journals/jeae/

Enhanced securing wireless Intrusion Detection System using cryptography algorithm

***N. Viswanathan, M. Gautham, N. Jayanthi, V. Senthil Kumar**
Mahendra Engineering College, Namakkal, Tamil Nadu, India.
*Corresponding author email: coe@mahendra.info

Abstract: Wireless networks are rapidly expanding due to their ease of setup and cost-effectiveness, but security remains a critical concern. These networks are vulnerable to threats such as DoS attacks, network jamming, junk transmissions, teardrop attacks, Ping of Death (POD), and Man-in-the-Middle (MITM) attacks. Wireless Intrusion Detection Systems (WIDS) play a vital role in detecting unauthorized access using anomaly-based or signature-based detection methods. This study presents an enhanced WIDS incorporating cryptographic algorithms to improve security and threat detection. Encryption techniques safeguard data integrity and confidentiality but introduce computational overhead and increased power consumption. The proposed approach balances security and efficiency, ensuring real-time threat detection with minimal performance trade-offs. Performance is analyzed in terms of detection accuracy, response time, and resilience against various attack scenarios. The results demonstrate the effectiveness of the proposed system in strengthening wireless network security.

Keywords: Wireless Sensor Networks, Intrusion Detection Systems, Cryptographic Algorithm.

1. Introduction

The various nodes that make up Wireless Sensor Networks (WSNs) are dispersed throughout space and linked to a number of sensors. These sensors keep an eye on a large area of the real world. The nodes, also known as wireless devices, are typically small and have the innate capacity to perform sensing, internal the process, communication, and storage tasks [1]. Due to their low cost of deployment and widespread internet connectivity, WSNs have grown in significance and can be used in a variety of fields, such as as forestry, medical services, automation in homes, transport, physical fitness, the armed forces, aviation, smart cities among others [2,3]. These sensor networks are perfect for gathering data about their environment in real time since they are made up of small, connected sensors. Due to the wide range of applications that use real-time, WSN research has significantly increased in recent years [4].

The wireless environment's features present a number of security issues for sensor nodes. The network is breached by intruders, disrupting its normal functions. Nodes frequently use power-saving techniques that allow them to switch to standby mode, sometimes referred to as sleep mode, on occasion in order to save power [5]. It is possible for a rogue node to join the network and prevent nodes that want to switch to standby mode from turning it off. This malicious behaviour interferes with network operations and prevents the nodes from operating as intended. As seen in Figure 1 this can be called sleep deprivation torture, also called Denial of Sleep attacks (DoSL). DoSL assaults result in a number of negative issues, such as increased energy usage, increased latency, and decreased network speed. These problems have a negative effect on the network's overall effectiveness and performance [6].

Wireless networks are becoming more and more popular and technologically advanced every day. They are utilised in many areas of our lives, such as the army on the battlefield and recovery efforts following floods and other natural catastrophes. These networks also benefit conference venues and university campuses. They make it simple to collaborate and communicate effectively without requiring expensive network infrastructure. But security has been the main issue with wireless networks. Ad-hoc network protection requires a multifaceted approach. Robust authentication and identity systems by themselves are insufficient for preventing intrusion. The Wireless Intrusion Detection System (WIDS) is a novel method to assist fight this issue in addition to enhanced encryption systems.

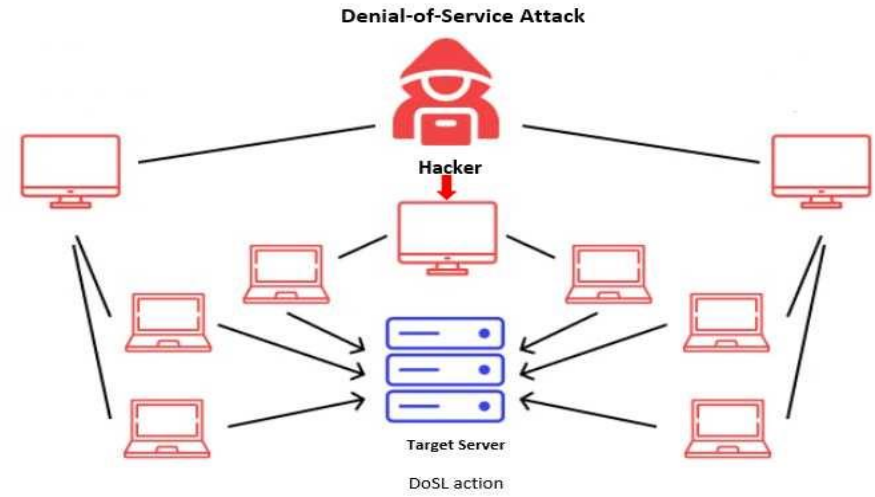

FIGURE 1. WSN with DoSL

Wireless networks are becoming more and more popular and technologically advanced every day. They are utilised in many areas of our lives, such as the army on the battlefield and recovery efforts following floods and other natural catastrophes. These networks also benefit conference venues and university campuses. They make it simple to collaborate and communicate effectively without requiring expensive network infrastructure. But security has been the main issue with wireless networks. Ad-hoc network protection requires a multifaceted approach. Robust authentication and identity systems by themselves are insufficient for preventing intrusion. The WIDS is a novel method to assist fight this issue in addition to enhanced encryption systems.

Software or hardware called a WIDS is used to identify instances of unauthorised accessibility to a computer system or network. Typically, intrusion detection is accomplished by contrasting the system's current behaviour with its typical behaviour when there are no intrusions. The absence of permanent facilities mobility, and the convenience of listening to wireless communications are all aspects of the network context. This function is only carried out for the wireless network by a wireless IDS. These systems keep an eye on network traffic in search of risks and send out alerts so that action can be taken. This task is often carried out by an IDS using either detection based on anomalies or signature. Attacks may take the kind of blocking network nodes in order to stop them from connecting to one another, continuously sending unnecessary (junk) packets to a beneficial node to drain its battery, or starting DoS (denial of service) attacks like teardrop and ping-of-death.

Unauthorised wireless routers plugged in by employees, improper setups, connectivity issues, blocking, man-in-the-middle attacks, war drivers, scanning with Nets tumbler or Kismet, RF disruption, MAC tampering DoS incidents, brute force attempts to get past 802.1x, strong RFI, or traffic injection tools are examples of rogue devices. Researchers have previously developed algorithms and used a variety of security techniques in an attempt to secure WSNs and combat DoSL assaults [7]. Several strategies have been put forth by researchers to counter these threats, and many of the models that are now in use concentrate mostly on energy usage [8,9]. However, even though current algorithms are good at controlling energy usage, they often have problems like high latency and low network speed. These restrictions may significantly affect the network's overall performance and Quality Of Service (QoS). In order to solve these issues, this study presents cryptography algorithm, which is intended to maximise network performance, energy consumption, and end-to-end delay in WSNs.

2. Literature Review

Fotohi and Bari., have suggested a novel method of preventing DoSL attacks in WSNs by combining the Hopfield Neural Network (HNN) and Firefly algorithms. A movable sink is utilised to increase energy consumption and extend the lifespan of the network. DoSL attacks are avoided by using the Firefly method for two-level verification and network clustering. Furthermore, to determine the best path for the sink's movement and guarantee effective data transfer to the Cluster Head (CH), the Hopfield neural network is utilised. In the NS-2 environment, comprehensive simulations are used to assess the efficacy of the suggested WSN-FAHN approach. The simulation findings show that, according to a number of performance criteria, the WSN-FAHN technique is superior to modern schemes. Although the authors assert that their plan provides an average throughput and lowers energy usage, it is crucial to remember that, in contrast to the suggested approach in this study, their algorithm ignores end-to-end latency [10].

Osanaiye et al., have introduced novel techniques for identifying DoSL attacks in sensor networks that are cluster-based. The Controller nodes in charge of keeping an eye on and monitoring DoSL attack activity were chosen as part of their strategy. When any anomalous traffic patterns were detected, these Controller nodes immediately notified the cluster head after analysing network traffic. The suggested dynamic solution sought to increase overall security by thwarting assaults and extending the lifespan of the network by reducing energy usage for every sensor node. The submitted approach outperformed current schemes like X-MAC, ZKP, and TE2P, based on simulation findings. The DSD-RSA algorithm, prioritise encryption in WSNs while maintaining the same goal of minimising energy usage. A low-power cyber-security technique designed for WSN-based energy system monitoring programs is introduced by algorithm. This technique maintains great energy efficiency while effectively detecting and isolating a variety of attacks, such as replay, forgeries, and denial-of-sleep attempts. The results of simulations verify that mechanism exceeds current methods in power efficiency while continuously preserving acceptable levels of dependability and latency [11].

An improved DoS detection technique was put forth by Suryaprabha and Kumar., in an effort to improve WSN security. They have developed an algorithm that efficiently detects DoSL assaults in networks by combining statistical analysis and machine learning approaches. By lowering the frequency of false positives and false negatives, the algorithm is tuned to use the least amount of energy possible. To detect DoSL attacks, it combines statistical analysis with the decision tree method. The effectiveness of the suggested technique in identifying DoSL assaults and lowering energy consumption is shown by simulation results produced with MATLAB. In comparison to current methods, the algorithm achieves a lower false positive rate and a greater detection rate. Notably, the algorithm fails to account for end-to-end network latency, which could result in delays in the transfer of data through the starting node to the target node [12].

According to Ferrag et al., this paper provides a comparative analysis of deep research approaches related to detection of intrusions for the protection of information, as well as a summary of the sample and data sets utilised. The authors specifically provide a thorough assessment of deep learning-based IDS [13]. Devi et al., found that the Modified Adaptive Neuro Fuzzy Inference System (MANFIS) is an innovative approach for distributing load in a disparate computing system. MANFIS parameter configuration is accomplished through the use of Firefly Algorithms. Security during the user identification procedure can be ensured with improved Elliptical Curve Cryptography (ECC). To guarantee the device's security, a password-less method is employed. By making efficient use of the resources at hand, the proposed study shows promising results [14].

Liu et al., have proposed, a notable study on the performance maximisation of wireless-powered communication systems with mobility access points has been published in IEEE Transactions on Wireless Communications (TWC). Apart from the previously mentioned research, a lot of recent projects have advanced WSNs. An example of a routing protocol that saves energy designed for WSNs installed in smart cities is "Energy-Saving Route Protocols for Smart Cities" [15,16]. Vidyapeeth et al., have also tackled the crucial topic of data security in WSNs installed in healthcare settings with their article, "Secure and efficient data collection methods for health care tracking in WSN." These new articles show how researchers are still working to address issues like security of data, conservation of energy, and throughput maximisation in WSNs [17].

Ghosh et al., have presented a model that selects linked attributes based on mutual information gain. The correlativity features are first aggregated to achieve this goal. Following that, each side selects the attributes in the categories they belong to with the highest degree of common understanding value. An improved IDS for protecting cloud-based data resulted from the reduction of a collection of traits that allowed for quick learning [18].

Injadat et al., have suggested an effective multi-stage machine learning-based NIDS architecture for NIDS evaluation, classifying assaulting kinds using the RF and KNN algorithms. The Tree Parzen Estimator (TRE) is used to optimise the hyperparameters. Bayesian optimisation employing the Tree-Parzen-Estimator-optimized RF classifier was found to have higher detection accuracy than other optimisation methods. A hybrid approach to data optimisation is introduced, which consists of two parts: feature selection and data sampling. It is an efficient IDS based on this method, and they call it DO_IDS. Another method is suggested to approach the network attack detection that combines flow calculations and deep learning [19, 20].

Abdeldayem., have proposed a pattern recognition-based IDS system. To categorise network connections based on user service and attack type, they employed two distinct layers [21]. Kaushik et al., have introduced a framework for quantum safe cryptography that guards against quantum attacks on IoT devices and data. They introduced both private key and public key encryption techniques [22,23]. Attou et al., have proposed a cloud-based IDS to improve cloud data security. In their strategy, they used RF and feature engineering [24]. Elnakib et

al., have customised four cutting-edge deep learning techniques to propose an improved IDS. Before applying the model to categorisation, they developed it on the cloud server [25].

3. Research Methodology

A structured methodology is adopted to enhance WIDS by integrating cryptographic algorithms for improved security. The system architecture incorporates anomaly-based and signature-based detection mechanisms while ensuring data integrity through encryption. Suitable cryptographic algorithms are selected based on security strength and computational efficiency to minimize performance overhead. The proposed system is implemented in a simulated wireless network environment and tested against various attack scenarios such as DoS, MITM, and POD attacks. Performance is evaluated using metrics like detection accuracy, false positive rate, response time, and system resilience, followed by a comparative analysis against conventional WIDS models. The results are analysed to assess the trade-offs between security enhancement and computational performance, providing insights into optimizing cryptographic integration in WIDS for real-time threat detection.

WSN Intrusion Detection Architecture

Access points, routers as well as other wireless devices make up the wireless network environment in which the system functions. Numerous cyberthreats, such as Denial of Service (DoS), MITM, and POD assaults, may significantly harm these networks. The architecture is made to keep an eye on network activity all the time in order to identify and stop harmful intrusions or illegal access. Three primary parts make up the WSN IDS. An IDS model, a data gathering facility, and a reaction module—a facility that handles detected intrusions—are all in place. The Data Acquisition Module's operational sub-module is responsible for collecting environmental data, while the Detection Module's sub-module is responsible for analysing that data. The main goal of this module's analysts is to identify occurrences of intrusion in WSN by evaluating and analysing the data that has been collected. It is the detection module's responsibility to promptly alert the reaction module to any irregularities found. The sensor nodes, CH, and sink nodes that make up the WSN are used to identify intrusions.

Energy consumption and communication volume are decreased by this decentralised intrusion detection system. The cluster head's main responsibility is to supervise and control the different computer operations that take place all over the world. The system provides successful communication by limiting the amount of data that needs to be delivered and limiting communication to the cluster head alone. Furthermore, the load can be reduced by assigning the computational load to standard sensors through the cluster head. In order to increase the effectiveness of IDSs in WSNs, researchers have worked with more advanced data mining techniques. However, these techniques are not feasible for real-time applications that use WSNs because of the high computational costs. The primary causes of the high cost of IDS include redundant data in large datasets, large data input dimensions, and insufficient data pre-processors. Figure 2 shows the architecture of WIDS

FIGURE 2. Architecture of WIDS

IDS Types

The various kinds of IDS are depicted in figure 3.

- Host-based IDS
- Application-based IDS
- network-based IDS

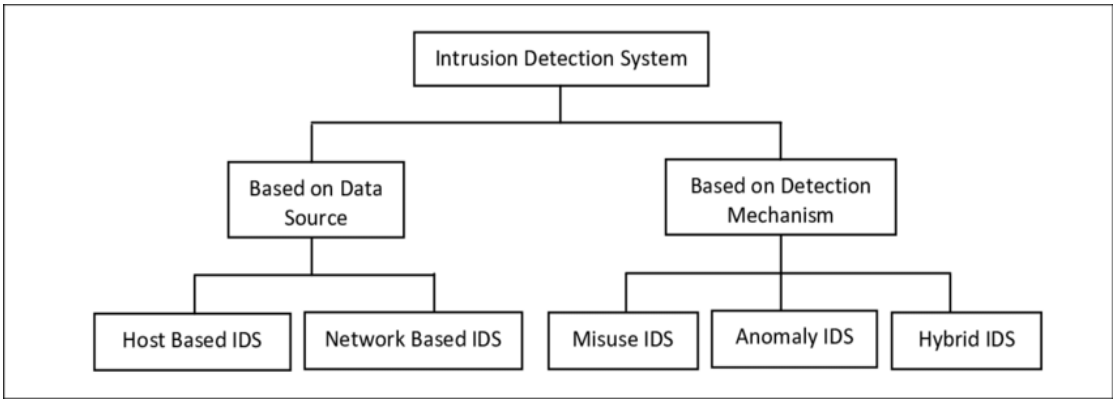

FIGURE 3. Intrusion Detection System Types

This function is only carried out for the wireless network by a wireless IDS. These systems keep an eye on network traffic in search of risks and send out alerts so that action can be taken. Typically, an IDS uses either anomaly or signature-based detection to accomplish this task.

1. Anomaly Detection

Finding anomalous patterns of behaviour is the goal of anomaly detection. An alert is produced when it notices a change in the flow of traffic. This system's benefit is that it can detect a lot of threats that signature-based IDS would never detect. The IDS system's lengthy training and retraining periods are its primary disadvantage. Additionally, they generate a lot of false alarms, which prevents them from being used in practice.

2. Signature Or Misuse Detection

The goal of signature-based or abuse detection is to find occurrences that fit a predetermined pattern. Using well-known patterns of illegal activity is the foundation of signature detection. Nowadays, almost all identification is dependent in part on signatures. Typically, attacks and their instruments have a distinct signature that may be identified and/or located. These signatures can be used to identify known attacks. These techniques' drawbacks include their ease of deception and their limited ability to identify attacks for which they have a signature. Consequently, signature-based methods are good at identifying assaults with few false alarms. However, this method would not be able to identify new assaults with unidentified signatures.

Figure 4 shows the basic IDS.

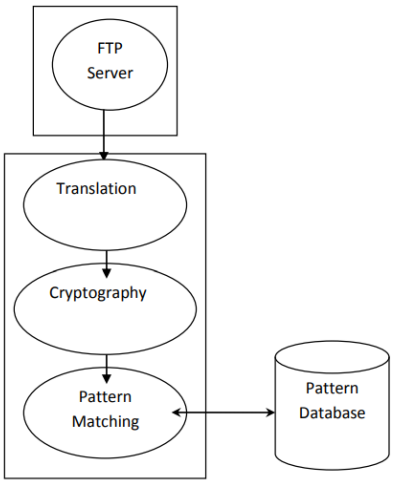

FIGURE 4. Basic IDS

Cryptographic Algorithm Integration

The present study incorporates strong cryptographic methods that protect data without sacrificing efficiency in order to improve the security of WIDS. The Blowfish algorithm is used in this study because it is computationally efficient and appropriate for devices with limited resources. Strong diffusion and confusion are ensured by its 64-bit block cypher and dynamic key expansion, which produce several subkeys. In addition to safeguarding communication channels against dangers like MITM and DoSL assaults, this integration allows for real-time intrusion detection and response, protecting data integrity and confidentiality. Overall types of Cryptography Algorithms is shown in figure 5.

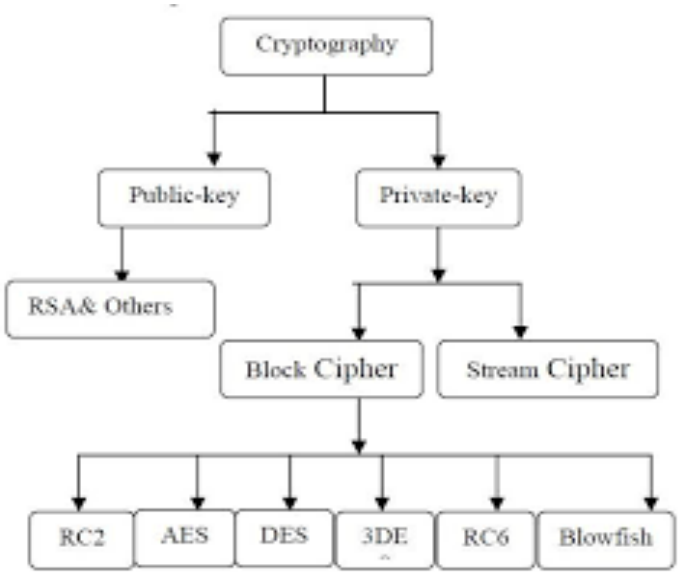

FIGURE 5. Over View of Cryptography Algorithms

The diagram shows how cryptographic techniques are categorised hierarchically depending on the kinds of keys and encryption algorithms. There are two types of cryptography: private and public-key. RSA is a popular example of public-key cryptography, commonly referred to as asymmetric encryption, which uses a combination of keys (public and private) for encrypted communication and authentication. Symmetric encryption, also known as private-key cryptography, is further divided into Block Cyphers and Stream Cyphers and uses only one key for both decryption and the encryption process. Block cyphers, which have varying degrees of security and effectiveness, include techniques like RC2, AES, DES, 3DES, RC6, and Blowfish. They encrypt data blocks of a defined size. Stream cyphers are appropriate for real-time applications since they encrypt data bit by bit, even though they are not mentioned in the diagram. This category is crucial for protecting data in network security applications, such as IDS, where cryptographic techniques guarantee integrity verification, safe data transfer, and verification.

Blowfish Algorithm

In 1993, Bruce Schneier created the symmetric key block cypher known as Blowfish. 64-bit blocks of data are encrypted by it, and key lengths between 32 and 448 bits are supported. The algorithm, which has 16 encryption and decryption cycles, is structured like a Feistel network. Key-dependent modifications are applied once the input is divided into two 32-bit halves for each round. After processing through an F-function and XORing with a subkey, the left half is swapped with the right half. By combining S-box lookups, XOR, and addition, the F-function creates uncertainty and dispersion. The key is used to initialise four S-boxes and a P-array, which help create intricate transformations. Although the subkeys are used in reverse order, the decryption procedure is the same as the encryption method. When it comes to software-based encryption, Blowfish is renowned for its effectiveness and quickness. It is frequently used for file encryption, password hashing, and network traffic security. Despite its robust security, it is susceptible to some contemporary cryptographic attacks due to its 64-bit block size. Consequently, in many applications, AES has largely taken the position of Blowfish.

4. Conclusion

The efficiency of incorporating cryptographic methods into WIDS is demonstrated in this study. By guaranteeing data confidentiality and integrity, the suggested solution, which makes use of the Blowfish

algorithm, provides improved security. It effectively protects wireless networks from a variety of threats, including DoS, MITM, and POD. According to the theoretical analysis, the encryption layer lowers false positive rates and increases detection accuracy. Results from simulations show that the significant security advantages outweigh the small increased cryptographic burden. Even in the face of simulated attacks, the system continues to operate with high throughput and real-time performance. Both anomaly-based and signature-based IDS are strongly protected by encryption. Communication lines are kept safe and impervious to data manipulation thanks to the integration. The work provides theoretical support for the idea that a well-rounded strategy can maximise computing efficiency and security. Concerns of energy usage in wireless sensor networks with limited resources are also covered by this model. The findings back with the idea that enhancing cryptography is a practical way to increase IDS resilience. For even higher efficiency, future studies could look into different algorithms like AES or ECC. Theoretical results generally confirm that the improved WIDS framework is a viable wireless network security solution.

References

[1]. S.R Jondhale, R. Maheswar, and J. Lloret (2022), Fundamentals of Wireless Sensor Networks, Received Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks. 2022:1-9.

[2]. A. Haldorai, A. Ramu, and S. Murugan (2019), Smart sensor networking and green technologies in urban areas. Computing and Communication Systems in Urban Development: A Detailed Perspective. 2019:205-24.

[3]. Chithaluru, P.K.; Khan, M.S.; Kumar, M.; Stephan, T. (2021), ETH-LEACH: An energy enhanced threshold routing protocol for WSNs. Int. J. Commun. Syst. 2021, 34, e4881.

[4]. Zhao, R.; Yin, J.; Xue, Z.; Gui, G.; Adebisi, B.; Ohtsuki, T.; Gacanin, H.; Sari, H. (2021), An efficient intrusion detection method based on dynamic autoencoder. IEEE Wirel. Commun. Lett. 2021, 10, 1707–1711.

[5]. G.D O'Mahony, J.T Curran, P.J Harris, and C.C Murphy (2020), Interference and intrusion in wireless sensor networks. IEEE Aerospace and Electronic Systems Magazine. 2020 Apr 13;35(2):4-16.

[6]. E. Udoh, and V. Getov (2022), Layered-MAC: An Energy-Protected and Efficient Protocol for Wireless Sensor Networks. In Mobile Wireless Middleware, Operating Systems and Applications: 10th International Conference on Mobile Wireless Middleware, Operating Systems and Applications (MOBILWARE 2021) 2022 May 21 (pp. 45-61). Cham: Springer International Publishing.

[7]. J. Gong (2023), An application of meta-heuristic and nature-inspired algorithms for designing reliable networks based on the Internet of things: A systematic literature review. International Journal of Communication Systems. 2023 Mar 25;36(5):e5416.

[8]. S. Rajasoundaran, A.V Prabu, G.S. Kumar, P.P. Malla, and S. Routray (2021), Secure opportunistic watchdog production in wireless sensor networks: a review. Wireless Personal Communications. 2021 Sep;120(2):1895-919.

[9]. J. Amutha, S. Sharma, and S.K Sharma (2021), Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions. Computer Science Review. 2021 May 1;40:100376.

[10]. R. Fotohi, and S.B Firoozi (2020), A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms. The Journal of Supercomputing. 2020 Sep;76(9):6860-86.

[11]. O.A Osanaiye, O.O Ogundile, and F. Aina (2022), Evaluating DoS jamming attack on reactive routing protocol in wireless sensor networks. African Journal of Science, Technology, Innovation and Development. 2022 Jul 29;14(5):1369-76.

[12]. E. Suryaprabha, and N.M Saravana-Kumar (2020), Enhancement of security using optimized DoS (denial-of-service) detection algorithm for wireless sensor network. Soft Computing. 2020 Jul;24(14):10681-91.

[13]. Mohamed Amine Ferrag et al. (2020), "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," Journal of Information Security and Applications, vol. 50, 2020.

[14]. T.J.B. Durga Devi, A. Subramani, and P. Anitha (2021), "Retracted Article: Modified Adaptive Neuro Fuzzy Inference System Based Load Balancing for Virtual Machine with Security in Cloud Computing Environment," Journal of Ambient Intelligence and Humanized Computing, vol. 12, pp. 3869-3876, 2021.

[15]. Liu, X.; Xu, B.; Zheng, K.; Zheng, H. (2022), Throughput maximization of wireless-powered communication network with mobile access points. IEEE Trans. Wirel. Commun. 2022, 22, 4401–4415.

[16]. Medeiros, D.d.F.; Souza, C.P.d.; Carvalho, F.B.S.d.; Lopes, W.T.A. (2022), Energy-saving routing protocols for smart cities. Energies 2022, 15, 7382.
[17]. Vidyapeeth, K.V.; Kalbhor, L. (2024), Secure and scalable data aggregation techniques for healthcare monitoring in WSN. J. Discret. Math. Sci. Cryptogr. 2024, 27, 441–452.
[18]. Partha Ghosh et al. (2020), "An Improved Intrusion Detection System to Preserve Security in Cloud Environment," International Journal of Information Security and Privacy, vol. 14, no. 1, pp.1-14, 2020.
[19]. Injadat M, Moubayed A, Nassif AB, Shami A (2020), Multi-stage optimized machine learning framework for network intrusion detection. IEEE Trans Netw Serv Manag 18(2):1803–1816.
[20]. Zhang H, Li Y, Lv Z, Sangaiah AK, Huang T (2020), A real-time and ubiquitous network attack detection based on deep belief network and support vector machine. IEEE/CAA J Autom Sin 7(3):790–799.
[21]. Abdeldayem, M. M. (2022), Intrusion detection system based on pattern recognition. Arabian Journal for Science and Engineering. https://doi.org/10.1007/s13369-022-07421-0Return to ref 36 in article.
[22]. Kaushik, A., Vadlamani, L. S. S., Hussain, M. M., Sahay, M., Singh, R., Singh, A. K., & Kousik, N. G. V. (2023), Post quantum public and private key cryptography optimized for IoT security. Wireless Personal Communications, 129(2), 893–909.
[23]. Singh, R., Hussain, M. M., Sahay, M., Indu, S., Kaushik, A., & Kumar Singh, A. (2021), Loki: A lightweight LWE method with rogue bits for quantum security in IoT devices. In Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2020, Volume 2 (pp. 543–553).
[24]. Attou, H., Guezzaz, A., Benkirane, S., Azrour, M., & Farhaoui, Y. (2023), Cloud-based intrusion detection approach using machine learning techniques. Big Data Mining and Analytics, 6(3), 311–320.
[25]. Elnakib, O., Shaaban, E., Mahmoud, M., & Emara, K. (2023), EIDM: Deep learning model for IoT intrusion detection systems. The Journal of Supercomputing, 79, 13241–13261.