An Encrypted Rules and Extreme Learning Machine Approach for Enhancement of Data Security

Amit Kumar Chandanan

Department of Computer Science and Information Technology, Guru Ghasidas Vishwavidyalaya, Bilaspur, India

Email: chandanan.amit@ggu.ac.in

Abstract

Among the many uses for WSN, which is an ad hoc wireless system, are conveyance, calamity administration, industrialized observing, health observing, and so on. Intrusion Detection System (IDS) is a top-tier network security measure. In order to prevent cross-layer attacks, IDS detection rates must be high. Using a technique known as the "Rule of Thumb" or ELM (Extreme Learning Machine) algorithm, WSN is able to predict the future with a great grade of accurateness. The projected RELM provides a comprehensive overview of both the attacks and the rules for detecting them. The rules can identify threats at the different layers. If the rule-founded IDS were deployed at the sensor nodes, less data would need to be transmitted over the network, saving power. Relative to the SVM (Support Vector Machine) and BPN (Back Propagation Neural Network) on the NSL-KDD dataset, RELM evaluates ELM's detection rate. Because of its superior detection rate, ELM has been used as the foundation of the IDS deployed at the BS to protect it against intrusion. If the criteria were combined with the ELM algorithm, the resulting system would have a higher detection rate than any currently available alternative.

Keywords: Secure WSN; Extreme Learning Machine; Intrusion Detection System; RELM; Support Vector Machine.

1. Introduction:

The Internet and other networked devices can be accessed through the usage of a WSN, which is a type of wireless local area network (WLAN). It got its moniker from the fact that it was designed with the concept of a WSN, which is an abbreviation for wireless local area network [1]. It is constructed out of sensor nodes that are both affordable and effective. The sensor nodes monitor the situation, communicate with one another to share information, and then send their results to the base station. The sensors send their findings back to the BS on a regular basis, either constantly or on an as-needed basis, or in response to an occurrence. Since the sensors have limited resources, including memory, processing speed, and battery life, they are susceptible to attacks [2]. Data packets may be altered or deleted by attackers, or they may get physical access to sensor nodes and do either of these things. IDS must be incorporated in WSN as a supplementary line of defence to filter out suspect data traffic because intrusion prevention systems (IPS) are not infallible, despite the fact that their primary purpose is to protect data.

Sensor networks are used to keep tabs on the well-being of individuals such as athletes and the elderly, both of whom require continuous monitoring [3]. The utilisation of sensors for the purpose of health monitoring has the potential to reduce the expenses associated with medical care while simultaneously improving patients' quality of life. When it comes to production, the utilisation of a sensor network enables the continuous monitoring of machines, reducing the requirement for human oversight [4]. With the assistance of the sensor network, one is able to monitor a wide variety of factors, including but not limited to temperature, humidity, water content, pollution, fire, smoke, detection of landslides, and so on.

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023

When we talk about keeping sensitive information hidden from prying eyes while it is being transmitted across sensor networks, we are referring to the concept of data confidentiality. This must be assured in both of the following scenarios: (i) The data collected by the sensors are confidential and should not be disclosed to any third parties that are not authorised to receive them. It is vital to encrypt sensitive data such as sensor identification and public keys in order to prevent attacks that involve traffic analysis [5].

The idea of "data integrity" ensures that the information that was received from the sender has not been altered in any manner, shape, or form. There are two different situations that could result in changes to the sensor data. users who are not authorised to do so make changes to the data, or It is likely that the data will be lost as a result of the extremely harsh conditions. Information that is current and is not a rehashed version of a message that was previously transmitted is referred to as having "data freshness" [6]. This may take place whenever shared keys in the sensor network are given a new version. Until the network is caught up to the key exchange, there will be a delay in the process. During this break, the adversary has the opportunity to send another message that is identical to the previous one. When the counter is included in the packets, it provides an additional layer of defence against the replay attack [7].

Having immediate access to the data ensures that the information acquired by the sensors may be accessed at any point in time. The availability of data is put in jeopardy as sensor nodes lose more and more of their energy. In a sensor network, this may take place during the process of sending and receiving massive amounts of data. This should be kept to a minimum [8] so that data accessibility can be ensured.

One example is how modern computer systems are unable to consistently recognise attacks on several tiers when utilising intrusion detection and prevention technologies (also known as IDS). The development of low-overhead strategies for the protection of sensitive health monitoring data is the primary objective of this project. It is recommended that IDS be used as a supplementary line of defence, with implementations at the sensor node and the BS, in order to enhance detection rates and lower power consumption in the face of cross-layer attacks [9].

Due to their dependence on batteries, sensor nodes deployed in outlying regions can quickly run dry and are difficult to repair. More energy is needed to run the sensors, communications, and computation at the sensor node. Sensors' power needs for data transmission outweigh those of the CPUs. One kilobyte of data transmitted 100 metres in a sensor uses as much power as three million instructions executed at one hundred million instructions per second per watt. Power usage would rise if complicated security algorithms were executed. As power usage rises, the useful lifespan of the sensor node declines. Solar-powered sensor nodes are preferred over battery-powered nodes because of their ability to capture energy from the sun, but their performance is optimal only in daylight. The security method therefore needs to be optimised for speed of execution. A longer lifespan for a sensor node would result from a decrease in execution time because it would use less computing power.

2. Related Workd:

Researchers have implemented the cross-layer intrusion detection agent for usage in the physical, MAC, and network layers of their systems. The detection system checks the authenticity of the Request to Send frame by comparing it with two different parameters: i) the node that is currently available in the routing table, which indicates whether or not the Request to Send frame was received from a legitimate neighbour; and ii) the received signal strength indicator value [10]. The IDS provides a novel way for detecting a variety of cross-layer attacks, including flood assaults, cloning assaults, and sink hole assaults, to name just a few of the possibilities. In spite of what you may believe, there is some kind of logic behind all of this chaos, and it is referred to as a single detection system.

According to the authors, the Hybrid IDS can be broken down into three distinct phases. First and foremost, material that does not conform to the standard is discarded via a rule-based anomaly detection mechanism [11]. In the second stage, the filtered and anomalous data are sent to a misuse detection model. Within this model, a back propagation neural network (BPN) classification method is employed to eliminate the known forms of assault. The rule-based decision making model may be able to identify the attacks and the exact sort of attack after the anomaly detection model and the misuse detection model have merged their findings. It will then inform the administrator. The abuse detection model receives only filtered input, and the criteria in the decision making model allow for the option to be made more quickly, which both contribute to the system's ability to save energy [12-13].

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023

Every node in the network, including the sink, the cluster head, and the sensor node, has its own proposed IDS. At the sensor node, the rule-based approach of detecting inappropriate use of the system is put into operation. A hybrid intrusion detection system is utilised at the cluster's hub in order to detect both anomalous behaviour and hostile activity. Following this, the findings are entered into a decision-making model, which subsequently generates a plan for the attack as well as a method for the attack [14-16]. At the sink node, an Intelligent Hybrid Intrusion Detection System (IDS) has been installed in order to detect attacks that have not yet been discovered. This intrusion detection system is equipped with a decision making model, a learning mechanism, an anomaly detection mechanism, and an abuse detection mechanism. The intelligent hybrid intrusion detection system uses a type of learning that boosts performance and increases the rate at which potential dangers are identified [17].

It has been seen in the research that a central agent will use decision tree techniques at the BS, whereas a local agent will use threshold-based metrics at the mote. This is something that has been documented in the academic research. If the local agent observes something out of the ordinary, it will communicate this information to the main agent [18]. The local agent's alarm is examined by the central agent, and if the alert is confirmed, the central agent will transmit its decision to all of the local agents. If the alert is not confirmed, the central agent will not broadcast its conclusion. In the event that a sinkhole or sleep deprivation attack takes place, the central agent is utilised to determine the nature of the issue [19].

Researchers have employed a similar two-pronged strategy to detecting assaults that involve the discarding of packets or the insertion of fraudulent packets into a network. This approach has been successful in detecting these types of attacks. To begin, measures that are based on thresholds are used to identify behaviour that is not typical. The threshold technique can be applied to aspects of traffic such the packet reception rate and the packet inter arrival time [20-23]. In the second stage, a fuzzy inference system is utilised for the purpose of determining whether or not an assault is currently taking place. The strategy is implemented on the network's neighbours that are accessible through a single hop. If an attack is identified, the node will notify the responsible node to the BS and remove it from the list of nodes that are close [24-25].

An intrusion detection and prevention system that is appropriate for use in manufacturing is suggested by the authors. The protection that an IPS offers against eavesdropping, as well as protection for data and node authentication [26-27], is invaluable. The intrusion detection system (IDS) is a secondary line of defence that is designed to stop any attacks on the network that were overlooked by the intrusion prevention system (IPS). Additionally, a hierarchical architecture is proposed for the purpose of detecting the other attacks, and the significance of the one-hop clustering is proved with real motes [28].

Keeping data safe while collection in a WSN is no easy task. Misleading summation could cause severe disruption in the sensor system. Attacks against sensor nodes can have serious consequences, including human life in the case of health-related applications and national security in the case of military ones. Attacks against data aggregation, selective message forwarding, black hole attacks, sinkhole attacks, and sybil attacks are only a few examples. Therefore, data privacy, data integrity, data authenticity, and data timeliness are all necessary for secure data aggregation.

The aggregators in a cipher text-based approach compile the cipher text sent to them by their lower-level nodes and send it on to the BSs at the next level. When gathering information, the aggregator node does not decrypt the cipher text it receives. This method is referred to as robust estimation or end-to-end encryption. There is less data being sent than necessary, and privacy is protected from beginning to end with this strategy.

3. Objective of the research work:

The focus of the current investigation is on developing methods that reduce overall energy use while simultaneously enhancing overall levels of safety. IDS, which is used at both sensor nodes and BS to identify cross layer assaults and to enhance detection rate while simultaneously reducing energy consumption, is advised to be used as a second line of defence to be given by the network. This recommendation comes from the fact that IDS is utilised at both sensor nodes and BS. IDS is also utilised by BS.

4. The Proposed Work:

Most intrusion detection systems (IDS) have a tendency to disregard the physical layer, the MAC layer, and the application layer when looking for threats to the network layer. It is conceivable for an assault on one layer to expand to the other layers if it is successful. If an attack on the physical layer is successful, the node that was compromised could decide to either throw away or modify the packet before it reaches the network layer. The identification of cross-layer attacks, which is the name that has been given to these specific forms of assaults, is the focus of this particular study.

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023

In order to zero in on cross-layer attacks, the suggested RELM makes use of previously established principles that were developed by security professionals. The hybrid model that was presented by RELM for the purpose of detecting attacks include, as one of its components, rule-based intrusion detection at the sensor nodes. After then, the BS intrusion detection makes use of the ELM in order to perform additional filtering on any suspect packets before passing them on. In the event that an attack is identified, an alert will be transmitted to the administrator of the system.

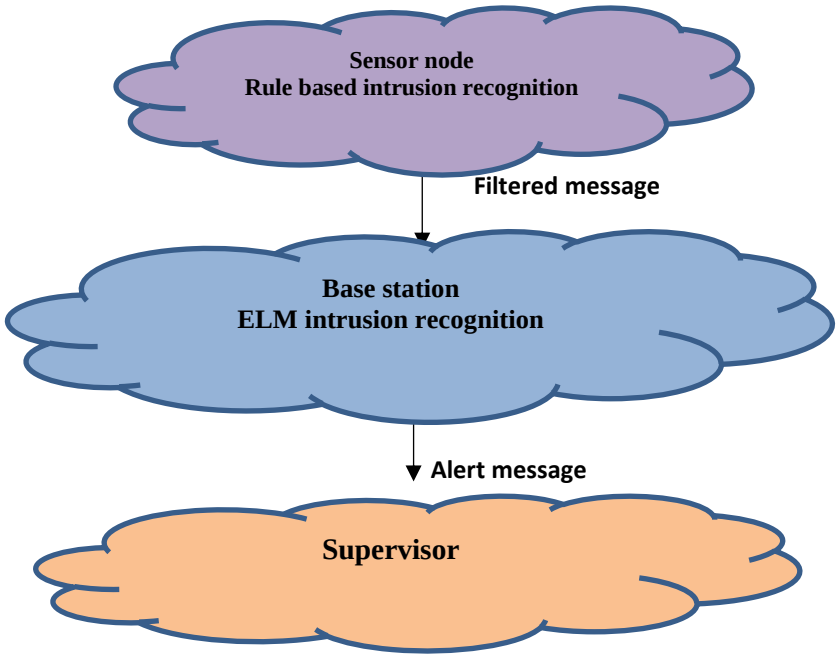

Figure 1: The Fusion based System Prototype

The model of the hybrid system that was proposed can be seen in Figure 1. Nearly every type of monitoring system makes use of the sensor nodes in some capacity. In today's modern industrial monitoring, a wide variety of sensors are utilised in order to keep an eye on both the equipment and the surrounding environment. A significant challenge posed by these configurations is the transmission of inaccurate data to the administrator. The proposed RELM technique includes the utilisation of intrusion detection in both of its phases. In phase I, rule-based intrusion detection is utilised by each sensor node in order to identify potentially malicious packets. In particular, cross-layer rule-based intrusion detection can be used to filter out threats at the physical, media access control (MAC), network, and application layers. Because of this first filtering mechanism, the sensor network is able to reduce the number of packets it sends to the BS, which allows it to consume less power.

In the second phase of the process, the filtered packets are sent to the BS intrusion detection system, which then puts into motion an ELM-based classification mechanism. The IDS that is located at the BS makes use of machine learning since it is more powerful than the IDS that is located at the sensor nodes, which can stick to technique that is based on rules. The BS examines each of the packets and notifies the administrator of the network if it identifies any that appear to be malicious.

Unsupervised learning algorithms do not have access to training data; instead, they rely on the algorithm's own predictions to classify the data into meaningful categories. This is in contrast to supervised learning algorithms, which do have access to training data. Clustering is another name for the processes of unsupervised learning. The supervised learning method known as ELM is used by the suggested RELM since it is necessary for it to differentiate between typical and unexpected packets.

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023

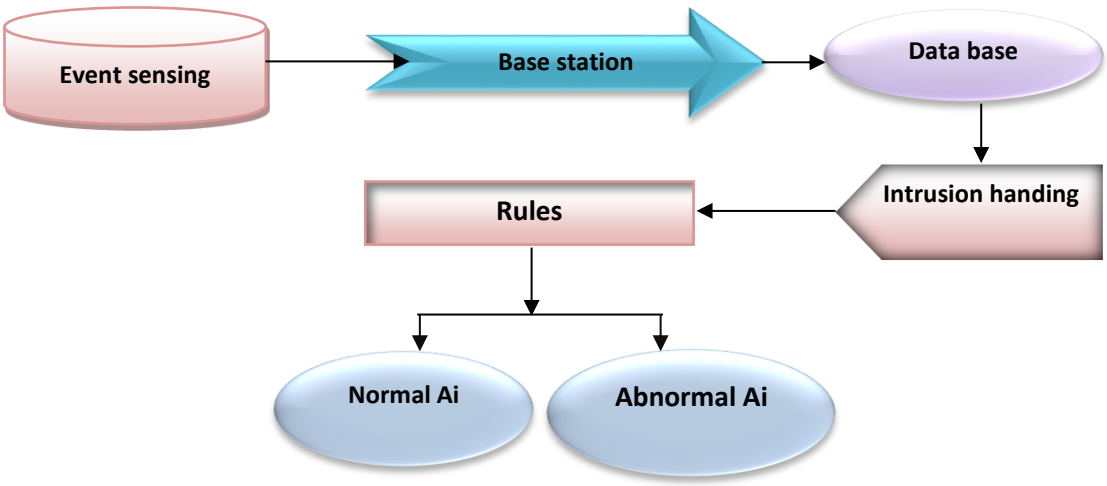

Figure 2: The Projected System prototype.

Any information that doesn't conform to the predetermined standards is discarded, and the BS is alerted to the nature of the attack if the threshold value is exceeded.

The ELM network can include one or more layers of hidden nodes and is a feedforward neural network. Weights between the yield level and the secreted level can be computed systematically, whereas the input bulks and prejudices of concealed nodes can be allocated at random. When compared to the BPN, the ELM algorithm has a significantly shorter learning time. Below is an example of a single hidden layer ELM algorithm, where the hidden nodes' output weights are learned all at once.

4.1. Support Vector Machine: The collaborative system trained three binary support vector machine classifiers, with each individual's classifier learning to search for orthogonal set homology (OSH) between the feature trajectories of one class ('N') and those of the other two classes ('H' and 'A').
Response data with topographies 1 to m:

$$X = x_1, x_2, \dots\dots\dots x_m \quad (1)$$

$$W^1 = w^1, w^1, \dots\dots\dots .. w^1 \quad (2)$$

W^h : signifies weightiness set at level h,

W^1: signifies weightiness set at primary secreted level.

$f(\,)$ is a step utility

$f(Z)$ is stimulation utility

$$h_i^i = f(Z) \quad (3)$$

n: whole numeral of topographies

m: no. of topographies mined.

μ: Despicable of preparation tasters

σ: Standard deviation of preparation tasters

h_i^i : signifies i[th] neuron in i[th] secreted level.

The superscript i signifies level though subscript signifies neuron numeral.

k: numeral of modules

$$\hat{y} = \{y_1, y_2, y_3, y_4\} \quad (4)$$

$\hat{\mathbf{y}}$ is set of $\{y_1, y_2, y_3, y_4\}$ are modules markers for Regular, Cautioning, Attentive, Disaster

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023

$softmax\ (z)$ Squashes the trajectory [z] of real standards into real tenets in the collection [0, 1] that add up to 1.

4.2. Algorithm for ELM

The formula for the input is @ = f(xi; ti) j xi 2 Rd; ti 2 Rm; I = 1;::: ; Data set: Ng

L = total number of neurons (L< d).

g(x): the role of activation

1 Set the parameters of the secreted layer to their default values (wi, bi), I = 1;::: ;L in Eq.

$+1/\sqrt{\text{reduced dimension}}$ for Probability-based dimensional reduction: 0.5

$-1/\sqrt{\text{reduced dimension}}$ for decreased dimensionality with a 0.5 probability

Step 2: Regulate the matrix H that represents the output of the secreted layer;

Step 3: Estimate the mass of the final production;

5. Result and Discussion:

In RELM, the efficiency of the ELM method is compared to that of the widely used BPN and SVM classifiers. Because experts are the ones who establish the rules, it is the experts themselves who decide whether or not the rules are accurate. On the NSL-KDD dataset, an independent comparison between the ELM and the BPN and SVM is performed as a result. Because the sizes of both the training and testing datasets are sufficient, there is no need to take a sample from the dataset in order to carry out the experiments. On several different datasets, the classification algorithms are evaluated to see how well they perform. The effectiveness of BPN, SVM, and ELM can be evaluated based on the True Positive Rate (TPR), the False Positive Rate (FPR), and the accuracy of the tests.

5.1. **Accuracy:**

It is a typical metric for classifying test results numerically. Increased precision indicates a more efficient system.

$$\text{Accuracy} = \frac{TN+TP}{Total\ data\ Sample}\ X100 \tag{5}$$

5.2. Specificity:

Specificity was defined as the absence of incorrect data classification. True Negative Rate is another name for it (TNR). Figure IV displays the recall of the current method in comparison to commonly utilized methods.

$$\text{Specificity} = \frac{TN}{TN+FP}\ X100 \tag{6}$$

5.3. Precision:

The present work is believed to have the precision to provide useful outcomes. The value of precision indicates what fraction of valid affirmative identifications were made. Figure III displays the results of a comparison between the current model and the commonly used techniques in terms of accuracy. The present system's accuracy was determined by

$$Precision = \frac{TP}{TP+FP} \tag{7}$$

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023

5.4. Sensitivity:

The accuracy with which the model places the test data into one of its classes constitutes the present method's sensitivity. How many true positives were successfully detected was the question it addressed. True Positive Rate is another name for it.

$$Senstivity = \frac{TP}{TP+FN} X100 \quad (8)$$

Table 1: Performance of classification techniques on first test record.

S. No.	Parameters/ Method	BPN	SVM	ELM
1	Sensitivity	95.34	98.58	99.25
2	Specificity	91.27	93.48	95.63
3	Precision (%)	88.27	91.47	93.18
4	Accuracy (%)	92.75	95.38	97.57

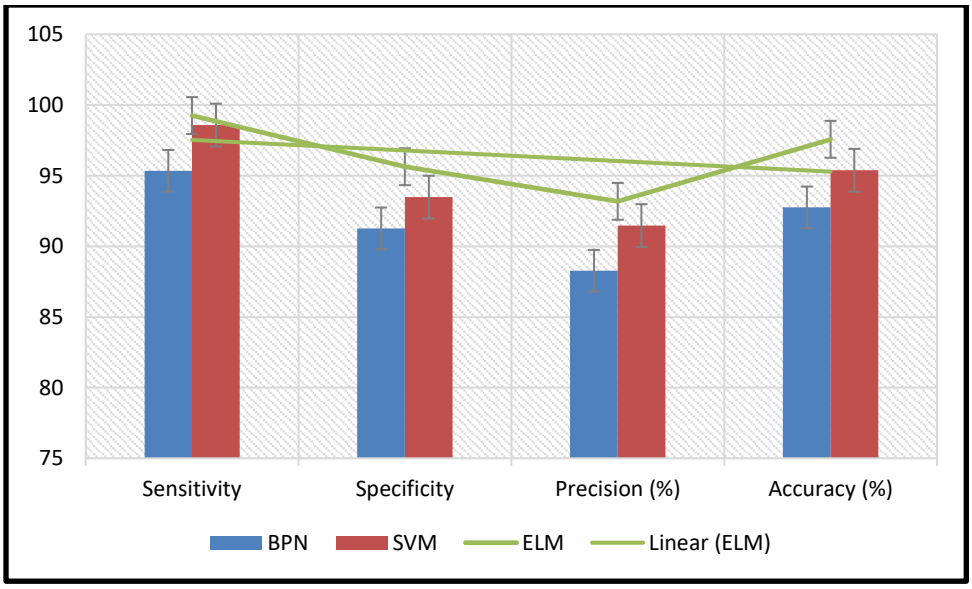

Figure 3: Performance of classification techniques on test record.

The test record is used to evaluate BPN, SVM, and ELM. In all three examples, ELM outperforms BPN and SVM in terms of detection rate. In ELM, the hidden nodes' output weights are learned in a single step, and only their input weights need to be updated until a target value is reached at an acceptable pace. Without using cross-layer rules, ELM is able to obtain a 97.57 percent average detection rate across all test scenarios. Combining ELM with the cross-layer rules undoubtedly improves accuracy to levels above 97.57%.

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023

Table 2: Performance of classification techniques on second test record.

S. No.	Parameters/ Method	BPN	SVM	ELM
1	Sensitivity	93.47	98.38	99.12
2	Specificity	94.36	98.27	98.89
3	Precision (%)	92.58	98.67	98.52
4	Accuracy (%)	94.37	97.68	99.24

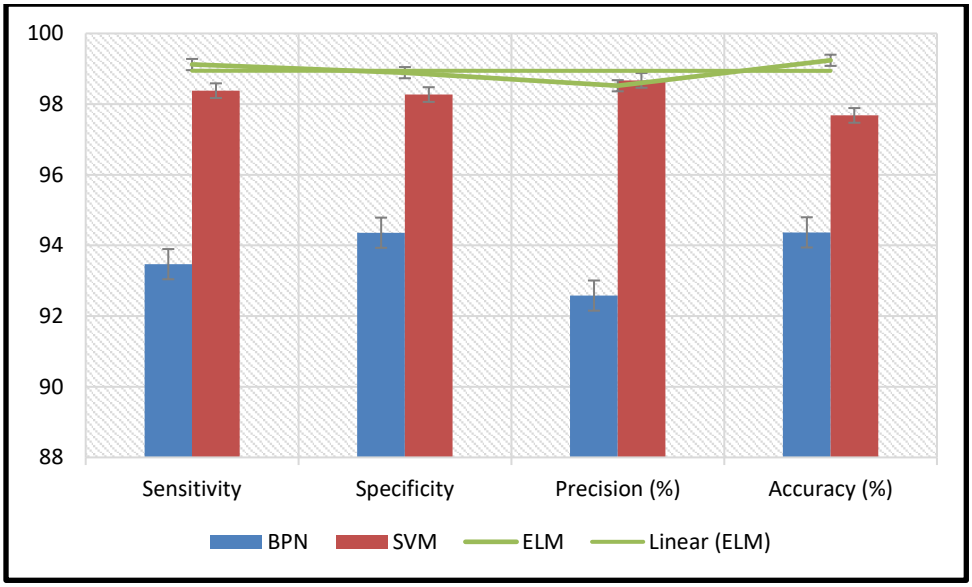

Figure 4: Performance of classification techniques on second test record.

When comparing BPN, SVM, and ELM, the test record is what's used. ELM has a higher detection rate than BPN and SVM in all three situations. With ELM, the output weights of the hidden nodes are learned in a single pass, while the nodes' input weights require only incremental updates until the desired value is achieved at an acceptable rate. The average detection rate for all test situations using ELM is 99.24 percent, and this is without the use of cross-layer rules. Integrating ELM with the cross-layer rules unquestionably raises precision to above 99.24%.

When the data fails to conform to the predetermined standards, the information is destroyed and BS is alerted to the nature of the assault. Device is used to store the data, design the user interface, and analyse the data for anomalies.

6. Conclusion

Protecting this information is a pressing area of research that needs to be done as soon as possible because of how easily adversaries can get sensor data. Even though there have been significant advancements made to existing security approaches, the majority of the currently available intrusion detection systems (IDS) can only identify attacks on the network layer. Next, research has been done with the intention of developing IDS for cross-layer attacks. In order to successfully carry out this task, research on the attack layer, the attack impact, and the detection rules is carried out. The NSL-KDD dataset is utilised to examine a variety of classification strategies, such as SVM, BPN, and ELM, among others. According to the findings, ELM demonstrates greater accuracy than both SVM and BPN.

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023

According to the findings of the research, a RELM strategy is the most effective way to efficiently identify cross-layer threats. At sensor nodes, filtering attacks by employing a rule-based intrusion detection system (IDS). Through the delivery of filtered packets to the BS, the sensor network is able to achieve reduced levels of energy consumption. The BS makes use of an ELM-based intrusion detection system in order to avoid unwanted intrusions. The detection rate that would be supplied by the combination of rules and ELM would be much greater than that provided by the systems that are now in place. In future work, before communicating health status to medical professionals, data classification methods based on fuzzy logic might be used. Also, the security of medical picture data can be engineered. It is possible to provide a safe method of tracking people's health.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1]. Xu, S & Wang, J 2016, „A fast incremental extreme learning machine algorithm for data streams classification", Expert Systems with Applications, vol. 65, pp. 332- 344.

[2]. C. Lin, D. He, X. Huang, and K.-K. R. Choo, "Secure and Privacy-Preserving Smart Contract-Based Solution for Access Control in IoT," IEEE Blockchain Technical Briefs, July 2018.

[3]. Yi, X, Bouguettaya, A, Georgakopoulos, D, Song, A & Willemson, J 2015, „Privacy Protection for Medical Sensor Data", IEEE Transaction on Dependable and Secure Computing, vol. 13, no. 3, pp. 369–380.

[4]. Wang, SS, Yan, KQ, Wang, SC & Liu, CW 2011, „An Integrated Intrusion Detection System for Cluster-based Wireless Sensor Networks", Expert Systems with Applications, vol. 38, no. 12, pp. 15234-15243.

[5]. Wang, C, Feng, T, Kim, J, Guiling, W & Wensheng, Z 2012, „Catching Packet Droppers and Modifiers in Wireless Sensor Networks", IEEE Transaction on Parallel and Distributed Systems, vol. 23, no. 5, pp. 835-843.

[6]. Roshan, S, Miche, Y, Akusok, A & Lendasse, A 2018, „Adaptive and online network intrusion detection system using clustering and Extreme Learning Machines", Journal of the Franklin Institute, vol. 355, no. 4, pp. 1752-1779.

[7]. Roy, S, Conti, M, Setia, S & Jajodia, S 2014, „Secure Data Aggregation in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 681- 694.

[8]. Khalid A. Darabkh, Mohammad Z. El-Yabroudi, and Ali H. El-Mousa, "BPA-CRP: A Balanced Power-Aware Clustering and Routing Protocol for Wireless Sensor Networks," Ad Hoc Networks, vol. 82, pp. 155-171, 2019.

[9]. Taochun Wang, Xiaolin Qin, Youwei Ding, Liang Liu, and Yonglong Luo, "Privacy-Preserving and Energy-Efficient Continuous Data Aggregation Algorithm in Wireless Sensor Networks," Wireless Personal Communications, vol. 98, no. 1 pp. 665-684, 2018.

[10] B. Murugeshwari, K. Sarukesi and C. Jayakumar, "An Efficient Method for Knowledge Hiding Through Database Extension," Test Conference International, pp. 342-344, 2010. Crossref, https://doi.org/10.1109/ITC.2010.93.

[11] A, Jenice and D, Hevin, "An Energy Efficient Secure Data Aggregation in Wireless Sensor Networks," Research Square, 2021. Crossref, https://doi.org/10.21203/rs.3.rs-364741/v1.

[12] Shraddha Deshmukh, A. R. Bhagat Patil and Harshad Nakade, "Implementation of Effective Key Management Strategy with Secure Data Aggregation in Dynamic Wireless Sensor Network," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 4, no. 2, pp. 358-364, 2018.

[13] Dou H, Chen Y and Yang Y, "A Secure and Efficient Privacy-Preserving Data Aggregation Algorithm," Journal of Ambient Intelligence and Humanized Computing, vol. 13, pp. 1495–1503, 2022. Crossref, https://doi.org/10.1007/s12652-020-02801-6.

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023

[14] Xiaohan Qi, Xiaowu Liu, Jiguo Yu and Qiang Zhang, "A Privacy Data Aggregation Scheme for Wireless Sensor Networks," Procedia Computer Science, vol. 174, pp. 578-583, 2020. Crossref, https://doi.org/10.1016/j.procs.2020.06.127.

[15]. Jeyalakshmi. C, Balasubramaniam, Murugeshwari and Karthick, M, "HMM and K-NN based Automatic Musical Instrument Recognition," IEEE, pp. 350-355, 2018. Crossref, https://doi.org/10.1109/I-SMAC.2018.8653725.

[16] Khalid A. Darabkh, Saja M. Odetallah, Zouhair Al-qudah, Khalifeh Ala'F, and Mohammad M. Shurman, "Energy-Aware and Density Based Clustering and Relaying Protocol (EA-DB-CRP) for Gathering Data in Wireless Sensor Networks," Applied Soft Computing, vol. 80, pp. 154-166, 2019. Crossref, https://doi.org/10.1016/j.asoc.2019.03.025.

[17] Mohamed Elshrkawey, Samiha M. Elsherif, and M. Elsayed Wahed, "An Enhancement Approach for Reducing The Energy Consumption In Wireless Sensor Networks," Journal of King Saud University-Computer and Information Sciences, vol. 30, no. 2, pp. 259-267, 2018. Crossref, https://doi.org/10.1016/j.jksuci.2017.04.002.

[18] Bala subramaniam Murugeshwari, Daniel Raphael and Raghavan Singaravelu, "Metamaterial Inspired Structure with Offset-Fed Microstrip Line for Multi-Band Operations," Progress in Electromagnetics Research, vol. 82, pp. 95-105, 2019.

[19] Vinod Kumar and Om Prakash Roy, "A Reliable and Secure Inter-and Intra-State Routing Protocol for VoIP communication," International Journal of Engineering Trends and Technology, vol. 70, no. 7, pp. 479-490, 2022. Crossref, https://doi.org/10.14445/22315381/IJETT-V70I7P250.

[20] Tianshu Wang, Gongxuan Zhang, Xichen Yang, and Ahmadreza Vajdi, "Genetic Algorithm for Energy-Efficient Clustering and Routing in Wireless Sensor Networks," Journal of Systems and Software, vol. 146, pp. 196-214, 2018. Crossref, https://doi.org/10.1016/j.jss.2018.09.067.

[21]. Piyush Kumar Shukla, Vandana Roy, Prashant Kumar Shukla, Anoop Kumar Chaturvedi, Aumreesh Kumar Saxena, Manish Maheshwari, Parashu Ram Pal, An Advanced EEG Motion Artifacts Eradication Algorithm, *The Computer Journal*, 2021;, bxab170, https://doi.org/10.1093/comjnl/bxab170.

[22] D. Dhinakaran, D. A. Kumar, S. Dinesh, D. Selvaraj and K. Srikanth, "Recommendation System for Research Studies Based on GCR," 2022 International Mobile and Embedded Technology Conference (MECON), Noida, India, pp. 61-65, 2022. Crossref, https://doi.org/10.1109/MECON53876.2022.9751920.

[23]. K.Sudharson, Ahmed Mudassar Ali and N.Partheeban, "NUITECH – Natural user Interface Technique Foremulating Computer Hardware," International Journal of Pharmacy & Technology, vol. 8, no. 4, pp. 23598-23606, 2016.

[24] S. Arun and K. Sudharson. "DEFECT: discover and eradicate fool around node in Emergency Network using Combinatorial Techniques," Journal of Ambient Intelligence and Humanized Computing, pp. 1-12, 2020. Crossref, https://doi.org/10.1007/s12652- 020-02606-7.

[25] J. A. Shanny and K. Sudharson, "User Preferred Data Enquiry System using Mobile Communications," International Conference on Information Communication and Embedded Systems (ICICES2014), pp. 1-5, 2014. Crossref, https://doi.org/10.1109/ICICES.2014.7033943.

[26]. K.Priyadharshini, "A Review on Wireless Sensor Networks-Security Issues and Disputes," International Journal of P2P Network Trends and Technology, vol. 9, no. 2, pp. 6-9, 2019.

[27] Korada Kishore Kumar and Konni Srinivasa Rao, "An Efficient users Authentication and Secure Data Transmission of Cluster-based Wireless Sensor Network," SSRG International Journal of Computer Science and Engineering, vol. 5, no. 1, pp. 1-5, 2018. Crossref, https://doi.org/10.14445/23488387/IJCSE-V5I1P101.

[28] Khalid A. Darabkh, Noor J. Al-Maaitah, Iyad F. Jafar and Ala'F Khalifeh, "EA-CRP: A Novel Energy-Aware Clustering and Routing Protocol in Wireless Sensor Networks," Computers & Electrical Engineering, vol. 72, pp. 702-718, 2018. Crossref, https://doi.org/Crossref, https://doi.org/10.1016/j.compeleceng.2017.11.017.

Doi : https://doi.org/10.54216/JCIM.110205
Received: November 20, 2022 Revised: January 25, 2023 Accepted: March 21, 2023