International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1409-1417
Journal homepage: http://iieta.org/journals/ijsse

Enhanced SVM and RNN Classifier for Cyberattacks Detection in Underwater Wireless Sensor Networks

Atyaf Ismaeel Altameemi, Sahar Jasim Mohammed, Zainab Qahtan Mohammed, Qusay Kanaan Kadhim*, Shaymaa Taha Ahmed

Department of Computer Science, University of Diyala, Baqubah 32001, Iraq

Corresponding Author Email: dr.qusay.kanaan@uodiyala.edu.iq

https://doi.org/10.18280/ijsse.140508

Received: 6 January 2024
Revised: 9 July 2024
Accepted: 24 July 2024
Available online: 31 October 2024

Keywords:
Underwater Wireless Sensor Networks (UWSN), cyberattacks, support vector machine (SVM), deep learning, machine learning, recurrent neural network (RNN), cyberattacks

ABSTRACT

Researchers have been paying greater attention to Underwater Wireless Sensor Networks (UWSN) lately because of their advancements in ocean surveillance, application deployment, and marine monitoring. However, because of its intrinsic qualities, this sensor network is susceptible to several kinds of cyberattacks, including Active Attacks, Sybil Attack, Denial-of-Service (DoS), Passive Attacks and Traffic Analysis. The Sybil assault is one of the deadliest cyberattacks and causes significant network damage among other attacks. This research proposes an intelligent techniques model-based cyber-attack detection system that combines deep learning and machine learning technologies for identifying cyber-attacks. Additionally, a feature reduction approach using machine learning methods Support Vector Machine (SVM) and Principal Component Analysis (PCA) is used to identify the attributes that are most strongly linked to the chosen attack categories. The study assesses the accuracy of a suggested Recurrent Neural Network (RNN) an algorithm for classifying and detecting intrusions that are based on deep learning. The proposed system achieves (97%) accuracy after dimensional reduction and optimization. This study will help the researchers design the routing protocols to cover the known cyber-attacks and help industries manufacture the devices to observe these cyber-attacks, which could reduce the possible attack chances in UWSN communication.

1. INTRODUCTION

One common application for Underwater Wireless Sensor Networks, or UWSNs, is the detection and monitoring of the underwater environment. It is equipped with multiple sensors and cars positioned to carry out particular functions in a predetermined region [1]. To process the observed data further, these networks are further connected to satellites and base stations. The first numerous applications, including resource exploitation, disaster avoidance, monitoring, maritime surveillance, river and sea pollution detection, and oceanographic data compilation, are supported by UWSNs. Using a hybrid feature reduction technique, intelligence techniques is used to detect cyber-attacks in UWSNs by building a system that can efficiently identify and categorize cyber-attacks [2]. Researchers and industry alike find the UWSN to be a fascinating field. The hostile underwater environment, the open audio channel, and its inherent capabilities make it vulnerable to dangers and malicious cyber-attacks. The basic characteristics of this sensor network, however, make it vulnerable to a variety of assaults, including as traffic analysis, denial-of-service (DoS), sybil attacks, active attacks, and passive attacks. Among other attacks, the Sybil assault is one of the deadliest cyberattacks and seriously damages networks. These features make it simple for cybercriminals to steal data between the source and the destination.

The attenuation of radio signals in an underwater environment makes it impossible to find sensor nodes using the Global Positioning System (GPS) [3]. Because of this, UWSNs use auditory communication to send and receive data between the source and the destination. Terrestrial Wireless Sensor Networks (TWSNs) and UWSNs have various features and purposes. These differences can be observed in a variety of ways. To begin with, UWSNs use acoustic signals rather than radio waves for communication, in contrast to TWSNs. TWSNs have more static networks compared to UWSNs' more dynamic networks [4].

Thirdly, in contrast to TWSNs, the underwater site is confined and uncontrolled. It is more difficult to locate nodes in UWSNs than in TWSNs. Moreover, underwater sensor devices have more expensive hardware and are constrained by memory and energy [5].

These factors cause changes in the sound speed in underwater environments. There are several uses for wireless sensor networks (WSNs), which provide an essential link between the physical world and the Internet of Things.

The underwater wireless sensor network environment is shown in Figure 1.

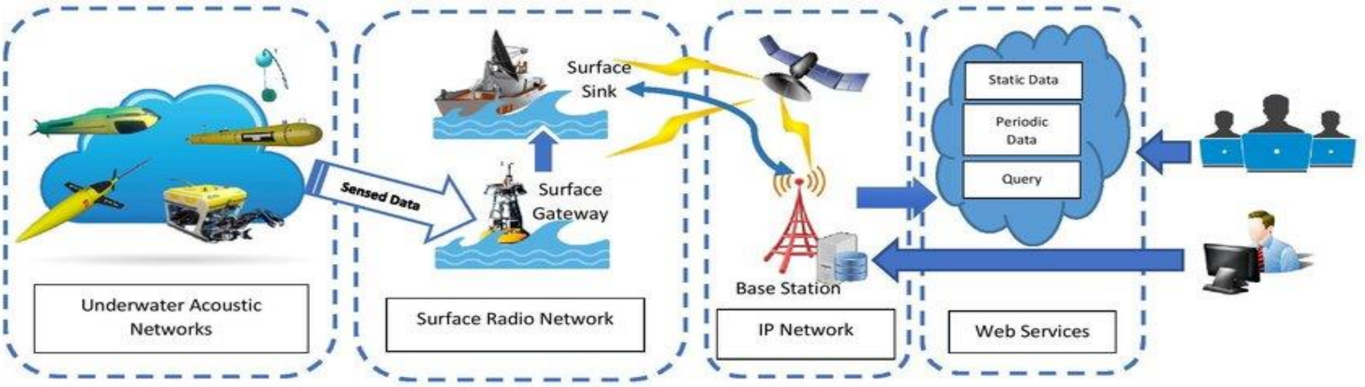

Figure 1. Overview of Underwater Wireless Sensor Networks [6]

Underwater Wireless Sensor Networks (UWSN) have recently emerged as a powerful method for aquatic applications and their importance in the present time [7]. These applications are becoming increasingly important in many fields, including: environmental and pollution monitoring, environmental and oceanic data collection, early warning systems, disaster prevention, distributed tactical surveillance, water navigation, and resource discovery [8]. This is because water covers approximately two-thirds of the Earth's surface (70%), so most of the resources under the surface of the water have only been discovered, a small part of which [9].

The industry uses WSNs extensively for continuous object boundary detection, which is crucial to WSNs [10]. In multichip underwater networks, incorrect packet size determination reduces network performance in terms of latency, resource usage, throughput efficiency, and energy consumption [11].

Using a hybrid feature reduction technique, intelligence techniques is used to detect cyber-attacks in UWSNs by building a system that can efficiently identify and categorize cyber-attacks [12]. The method improves intrusion detection performance by reducing the high-dimensional feature space by combining machine learning and deep learning approaches. To do this, the most pertinent features are extracted using a hybrid feature reduction technique. Next, to precisely classify network traffic, the system is trained using RNN algorithm. The main objective is to provide high-performance learning and early detection systems for efficient cyber-attack detection and prevention in UWSNs environments. Cyber-attacks are destroying the Wireless Sensor Network (WSN).

The cyber-security applications employ Machine Learning (ML), a subset of artificial intelligence, for prediction systems and zero-day attack detection [13]. The four categories of machine learning approaches are unsupervised, supervised, semi-supervised, and reinforcement learning [14]. ML is intended to be supplied in regular conditions. Therefore, a situation could become unstable due to cyber-attacks. The Machine learning enables real-time threat detection by being exceptionally good at spotting anomalies in network behavior. It is capable of analyzing enormous volumes of data to find unknown viruses, insider threats, and policy infractions. The Deep learning can be defined as a collection of machine learning algorithms that go through multiple stages and are taught on different datasets. Cyber-security is identifying threats in UWSNs to protect shared and stored information and data in light of the rise in cybercrime. Simulated attackers for SCADA and VANET intrusion detection systems may become ineffective due to a variety of machine learning techniques [15]. The Deep learning is an effective method that has multiple applications in enhancing cybersecurity. It can be used to recognize and thwart phishing attempts, find and halt malware, and even forecast potential threats in the future.

We used the SVM and PCA because can withstand outliers and noisy data, which are frequent in actual cyberattack scenarios. This guarantees dependable performance even while working with erroneous or incomplete data.

We choose the RNN because RNNs are so good at finding patterns in sequential data; they are perfect for spotting anomalies in network traffic that could point to a cyberattack. By analyzing a vast amount of security data, the suggested model can identify cyberattacks by deciphering their intricate underlying structure, hidden sequential links, and hierarchical feature representations. The effectiveness of SVM and RNN machine learning algorithms for cyber security issues is assessed in this research.

The proposed work is evaluated by taking into account the employed dataset, NSL-KDD. The accuracy, precision, and F-measure of the suggested method are assessed for each dataset in both the full features and reduced features scenarios [16]. Additionally, a comparison is made between the results of benchmark machine learning approaches and the suggested (SVM-PCA-RNN). Three stages of this approach-feature reduction, feature extraction, and categorization-combine deep learning with machine learning. These steps are necessary to stop the early attack detection-related decrease in resource availability.

2. RELATED WORKS

Due to the increasing reliance of Underwater Wireless Sensor Networks (UWSNs) on networked devices, robust cyber-security measures are necessary. Among other threats, these networks are vulnerable to eavesdropping, denial-of-service attacks, and data breaches. Effective cyber-security is essential for protecting sensitive data, ensuring dependable communication, and protecting critical infrastructure. Because of their limited communication capabilities and dangerous underwater environment, UWSNs provide unique cyber-security challenges. Underwater channels are dynamic, which could make implementing security much more challenging. Additionally, typical security protocols might not be suitable for these networks [17]. Machine learning and deep learning techniques are crucial for enhancing cyber-security protocols and protecting computer systems against various cyber-attacks, hacking incidents, and data thefts. Table 1 shows the four methods for the NSL-KDD combination.

Table 1. Summary of work results related to the four methods for the NSL-KDD dataset

Methods	Accuracy	Precision	F1-Measure
ML	83.9%	82.9%	83.01%
DL	85.19%	83.66%	84%
Hyper PCA & RNN	88.06%	87.49%	89.01%
Hyper SVM & RNN	90.4%	91.18%	91.06%

A lot of research has been done on cyber-security, a critical topic in computing systems, to develop secure systems that can recognize and isolate cyber-attacks, particularly in UWSNs. The primary and secondary categories of machine learning that were employed in malware detection in cyber-security, DOS assaults, phishing websites, spam, and biometric identification were provided by researchers [18]. In the study of Berman et al. [19], numerous machine learning approaches were employed in Vehicular Ado Network (VANET) cyber-security applications. Using the recommended techniques, this was done to identify the different sorts of attacks. These methods, which mimic attackers utilizing Supervisory Control and Data Acquisition (SCADA) systems and spying determine, could render attackers ineffectual. While the six machine learning techniques the authors of the paper introduced Nave Bayes, Decision Trees, Random Forests, Neural Networks, Gradient Boost, and Multilayer Perception [20]. However, a team of scientists suggested by Apruzzese et al. [21] models for predicting correlation based on deep learning that made use of the Mixed Convolutional Neural Network (WL-DCNN) and the Wifelier-Lehman kernel for quick sub-graph tagging and extraction [22]. This was done to improve the topological mining features' remarkable performance and great degree of generality through self-learning. On the CICIDS2017 datasets, Hussein et al. [23] proposed a DL model that could detect Distributed Denial-of-Service (DDoS) cyber-security assaults with an accuracy of up to 97.16%. Reliable and current deep learning research has already applied massive convolutional neural networks with data sets [24]. This indicates that deep learning intelligence algorithms are now popular. In the study of Dixit and Silakari [25], a comparison research and offering evaluation of different using deep learning and machine learning techniques, the WSN-DS dataset may be saved and intruders may be recognized. It was demonstrated that ML techniques were inferior to deep learning classifiers in terms of intrusion detection results.

3. ISSUES AND ATTACKS IN UWSNS

The UWSN is a network designed to monitor activities across a certain area. It consists of intelligent sensors and vehicles that have been modified to cooperate in wireless communication. The data is retrieved from sensor nodes via the surface sink. A transceiver on the sink node is capable of controlling acoustic signals that are received from nodes underwater. Long-range radio frequency signals can be sent and received by the transceiver in order to communicate with the onshore station. For a specific use, the gathered data are either locally utilized or connected to another network [22].

Deployable nodes on the surface and below the water make up Underwater Wireless Sensor Networks. With other nodes in the same network as well as with the base station, all nodes must be able to communicate and exchange data. Data transmission using optical, electromagnetic, or acoustic wave media is a function of sensor network communication systems. Because of its attenuation qualities in water, audio communication is the most utilized and well-liked of these medium kinds. When energy is absorbed and transformed into heat in water, a factor of low transmission is produced. Long-distance transmission and reception of acoustic signals is made possible by their low frequency operation. Marine surveillance, sea monitoring, deep sea archaeology, oil monitoring, etc. are some of the main uses of UWSN. This work's primary objective is to present a thorough analysis of underwater sensor networks, including their applications, deployment strategies, and routing algorithms.

The UWSNs are more vulnerable to cybersecurity threats than terrestrial networks because of the hostile underwater conditions and limited use of acoustic communication. Among these difficulties are restricted bandwidth and significant latency are compared to radio transmission in the air, acoustic communication underwater is substantially slower and has a smaller bandwidth. Large-scale data transmission and real-time communication are hampered by this. High energy consumption is sensor nodes' battery life may be shortened by acoustic communication, which uses more energy than radio transmission. Physical security is sensor nodes are susceptible to theft or other physical threats.

Limited computing resources is complex security methods may be challenging to implement on sensor nodes because to their limited memory and processing capability.

The UWSNs and underwater acoustic channels suffer from several limitations that create potential safety risks. As a result, UWSNs become vulnerable to many malicious threats and attacks [26]. Depending on the actions taken by the malicious attacker, these attacks can be passive or active.

Figure 2 illustrates the Issues and attacks in to Underwater Wireless Sensor Networks (UWSN).

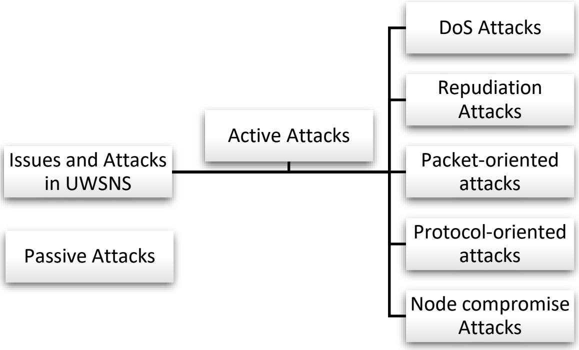

Figure 2. Issues and attacks in UWSNS

3.1 Cyberattacks

Cyber-attacks are ruthless and illegal attempts to steal sensitive data and information from a particular person without that person's knowledge [27]. As cyber-attacks increase yearly, hackers are making money off sensitive data belonging to valuable organizations. More than $500k has been lost to cybercrime in recent years [28]. The most widespread types of cyber-attacks a malware the term "malware" describes unauthorized software, apps, worms, and viruses. Malware software is installed when a customer clicks on email and message links and downloads unauthorized software. Phishing the fraudulent practice of sending emails containing personal information from the same source repeatedly is known as phishing. Credit card details and other financial data are commonly obtained using this type. Through the email link, the hacker installs malware on computers and mobile devices with the intention of stealing important data [28]. Man in the middle of the attack hackers who produce network traffic are usually involved in man-in-the-middle attacks, also known as bug attacks. Once into the network, the hacker will introduce vulnerability into the system that will allow them to access data on any machine owned by the victim. When a user logs in to public WiFi, the hacker takes advantage of network flaws to create traffic. SQL injection Structured query language (SQL) injection assaults occur when hackers inject code into the server that is infected with malware or contains access control code. When a victim executes the malicious malware on their computer, the hacker obtains access through this gateway, enabling them to steal personal data. DNS tunneling: This method allows network-connected devices that are not connected to the DNS server protocol on a specific port number to communicate with each other by sending HTTP or another protocol via DNS. Once linked, the hacker can steal data online by utilizing the DNS protocol [29].

3.2 Cyber security

There are many different types of cyber-security, such as end-point security, network security, application security, cloud security, mobile security, zero trust, and IOT security [30]. Cloud security cloud security is also known as cloud computing. Cloud computing is being used by a lot of enterprises these days. Making sure the cloud is secure is a top priority [31]. Cloud safety encompasses services, rules, and solutions that protect the cloud communications and architecture of the entire enterprise [32]. To protect an organization's cloud data, cloud security businesses typically offer a third-party solution [33]. Mobile security It's important to guard against malicious software, phishing scams, and instant messaging attacks even on laptops, locked smartphones, and other small electronic devices [34]. Mobile security measures guard user data while thwarting these intrusions. Mobile device management (MDM) solutions ensure or supply access to the designated application when they are linked to the company's resources. Security with zero trust a different term for zero-trust security is Zero-Trust Architecture (ZTA). Building walls with fortifications around the organization's most valuable assets is recommended by the traditional security concept, which emphasizes the perimeter. Nevertheless, this approach has a number of serious issues, including potential dangers. Maintaining the legitimacy of digital contact is the goal of zero-trust security, a strategic approach to cyber security. The network security attacks happen frequently only in this area. Network security software and programmers exist to prevent hackers from breaching networks. Data usability and integrity on computer networks and personal computers will be protected. Next-generation firewall limits, Network Access Control (NAC), Identity Access Management (IAM), and Information Loss Prevention (DLP) are some of the tactics used to prevent data theft.

Application security Operating system security is referred to as application security. Because web apps link directly to the internet, they are susceptible to data theft. Online applications are vulnerable to issues including injection, failed authentication, and cross-site scripting. Applications and APIs are protected from unauthorized access by application security [35]. IoT security One method for shielding IoT systems from threats is IoT security. Nowadays, with the Internet of Things permeating every aspect of the business, the efficiency of IoT devices increases productivity. Protection against threats and breaches is aided by Internet of Things (IOT) security tools. The IoT system security can be enhanced via data encryption, device authentication, and device identification. End-point security Every organization has remote computer access [36]. End-point security is the management of an organization's exit or end points, such as computers, laptops, and electrical controllers.

4. METHODOLOGY

This section explains the method for detecting intelligent techniques for cyber-attacks Detection in Underwater Wireless Sensor Networks (UWSN). The suggested cyber-security solution is made using clever methods that incorporate machine learning and deep learning. Most UWSN security research is still in its early stage. Network security is a complex issue, and the use of artificial intelligence is optimal in detecting cyber-attacks in Underwater Wireless Sensor Networks (UWSN). If a node in UWSN is attacked and rejected, it will cause serious damage. In this case, it is necessary to configure security systems periodically, in order to detect and classify cyber-attacks. The suggested system's structure is depicted in Figure 3, which also features a multi-stage workflow that begins with feature reduction and continues through feature extraction and classification.

These days, it's common to detect aberrant data using machine learning algorithms. The majority of machine anomaly detection techniques in use today require the node to store the complete training set and operate in a stationary context. The SVM was employed in this paper to detect anomalies in UWSNs. Local functions that only employ the subset of data are used to carry out the present forecasts. Thus, a low computation complexity is one of the UWSN requirements. Principal Component Analysis (PCA) is used online to reduce the dimensionality of the input data by handling duplicated and unnecessary data. Following the prediction procedure, an RNN algorithm is used to calculate the value in order to identify any differences between the expected value and the actual detected value. The 97 percent identification rate and extremely low error rate.

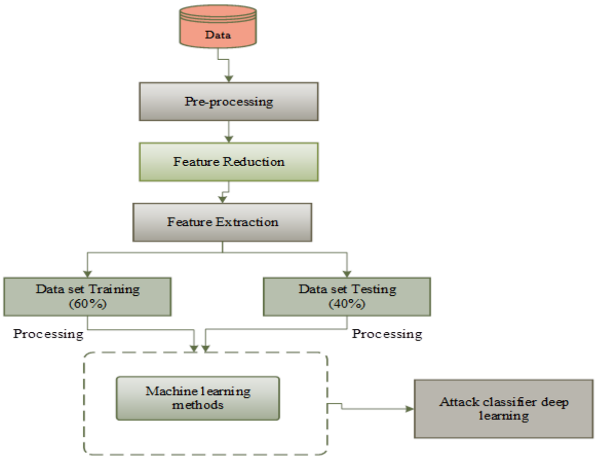

Figure 3. Proposed methodology for detecting attacks in UWSN

This picture illustrates that the adopted datasets of the NSL-KDD dataset (55 features) are the input of the proposed system. To prepare the dataset parameters for entry into the feature reduction stage, the preprocessing step involves normalizing and reformatting the dataset parameters.

In the NSL-KDD dataset, feature reduction is achieved by reducing them from (55 to 20) using machine learning algorithms. Utilizing the combined capabilities of DL and ML, the attributes of the reduced features are altered by inserting them into the proposed hybrid model. To run the feature extraction model, they are split for 60% training data and 40% test data. In the final step, the cyber-attack classifications are applied using deep learning technique (RNN).

The suggested hybrid model enhances the quality of the reduced attributes by fusing the advantages of DL and ML.

4.1 The stage of preprocessing

The unprocessed data gathered from a model environment makes up the adopted datasets. To guarantee that the suggested system performs on a high precision scale, these datasets must be handled. The databases contain a variety of information kinds that can be manipulated and analyzed to provide false results. In this work, a dataset is transferred using a variety of approaches, including the Min-Max method. The Min-Max normalization uses a linear adjustment of the raw data [33].

4.2 Feature reduction stage

Feature reduction, also known as dimension reduction, refers to the sensing-based feature count reduction that keeps the data in the legitimate formulation. As more qualities are eliminated, the number of variables is decreased. This is done to speed up and simplify the computer's tasks [37]. The adopted feature reduction process's block diagram is displayed in Figure 2. It is evident that the two machine learning techniques used in this stage-SVM and PCA-are intended to reduce the number of characteristics.

The generated feature reduction models utilizing PCA and SVM are briefly demonstrated for further clarification. PCA searches for k-dimensional orthogonal vectors that can be applied to the data formulation process [38]. In order to minimize the dimensions, the original data was directed towards a smaller region. A little size alternate set of variables is created by PCA in order to merge the attributes from the NSL-KDD data set. This smaller group can then see the raw data. It takes into account the connections between characteristics it would not frequently occur, enabling interpretations that were not suspected in previous stages [39]. Data processing is finished before this stage because PCA works with digital data, as shown in Figure 3.

A popular supervised machine learning method for pattern identification and classification issues is called Support Vector Machine (SVM). By building a multidimensional hyperplane that maximizes the margin between two data clusters, the SVM algorithm effectively discriminates between two classes. This technique provides strong discriminative strength by applying unique nonlinear functions called kernels to turn the input space into a multidimensional space [40].

To distinguish between two classes in an n-dimensional space, the SVM technique's fundamental principle is to build an n-1 dimensional separating hyperplane. One thinks of a data point as an n-dimensional vector. A straight line (one-dimensional) dividing the space in half would be the separating hyperplane, for instance, if two variables in a dataset created a two-dimensional space. The maximum-margin separating hyperplane is the ideal separating hyperplane that SVM looks for when more dimensions are involved. The goal is to maximize the distance (referred to as support vectors) between the hyperplane and the closest data point on each side [41]. A linear hyperplane separating two classes is the ideal situation. Real-world circumstances are not often that straightforward, though. It's possible that some data points from the two classes fall into a "grey" area where it's difficult to distinguish them. In order to solve this problem, SVM uses: 1) a user-specified parameter C that specifies the trade-off between the minimization of misclassifications and the maximization of margin; 2) the addition of more dimensions to the low-dimensional space using kernel functions, which typically include linear, polynomial, sigmoid, and radial basis functions (RBF), because of this, two classes might be able to be distinguished in the high-dimensional space. An example of an inseparable two-dimensional space that becomes separable following the low-dimensional input space's transformation into a multidimensional one is depicted in Figure 4. Essentially different from multiple logistic regressions, the SVM technique tends to classify things without offering estimates of the probability of class membership in the dataset [42].

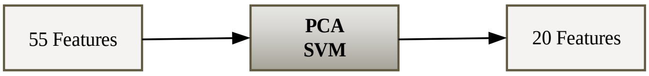

Figure 4. Stage of feature reduction

4.3 Feature extraction stage using RNN

It is important to emphasize that this work's greatest contribution is the hybrid model it proposes, which incorporates the deep learning structure [43]. The capabilities of a classic neural network, which can only handle inputs with fixed length, are expanded to take variable-length input sequences by a recurrent neural network (RNN), as illustrated in Figure 5. Using the yield of the shrouded units as an extra contribution for the subsequent component, the RNN forms inputs for each component individually. RNNs may thereby handle issues related to temporal sequence, discourse, and language. A "state vector" that retains a memory of prior occurrences in the grouping can be maintained by an RNN's hidden units. The duration of this "memory" can be changed based on the kind of RNN hub that is being used. The more long-term scenarios an RNN can learn, the longer its memory [44].

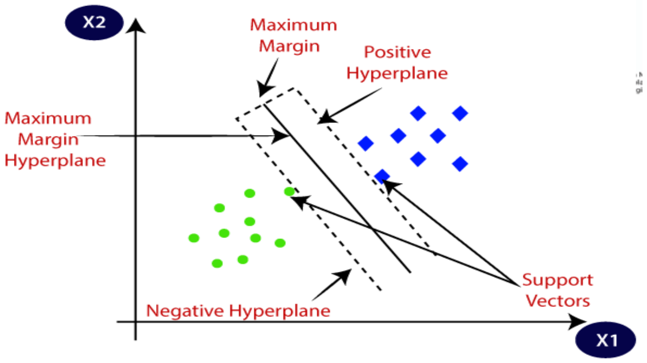

Figure 5. SVM classification [39]

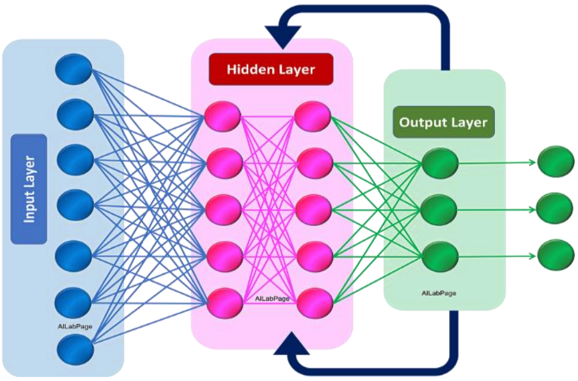

Figure 6. A Recurrent Neural Network (RNN) [45]

As seen in Figure 6, a recurrent neural network (RNN) can accommodate variable-length input sequences, extending the capabilities of a typical neural network, which can only accept fixed-length information inputs. The yield of the shrouded units is used by the RNN as an extra contribution for the subsequent component, forming inputs for each component one at a time. Consequently, RNNs are capable of handling issues related to temporal sequence, discourse, and language. The hidden units of an RNN are appropriate for preserving a "state vector" that contains a memory of prior occurrences in the cluster. The duration of this "memory" can be changed based on the kind of RNN hub that is being used. The more long-term scenarios an RNN can learn, the longer its memory.

5. EVALUATION OF EFFICIENCY

There are two types of cyberattack classifications found in the literature, based on the number of classes (i.e., attacks): multi-class classification, where the number of considered classes is greater than two if more than one attack has been detected and sampled in the dataset, and binary classification, where there are only two classes, attack or normal. Different assessment criteria are used in both situations throughout the testing stage of the creation of an ML model. The performance of the suggested hybrid model is evaluated using a variety of metrics, including F1-measure, accuracy, and precision. The accuracy (Acc) that corresponds to the classification efficiency can be calculated as [46]:

$$\mathrm{Acc} = \mathrm{T}N + \mathrm{T}P / \mathrm{T}N + \mathrm{F}P + \mathrm{F}N + \mathrm{T}P \tag{1}$$

When, TP: The methods label it as positive even though the actual class is positive. FN: The methods label it as negative even though the actual class is positive. FP: The methods identify it as positive even though the actual class is negative. TN: The methods identify it as negative even though the actual class is negative [47].

Additionally, the accuracy, which is the correction ratio for correctly anticipating the positive outcomes, is assessed as follows:

$$Precision = \mathrm{TP} / \mathrm{F}P + \mathrm{TP} \tag{2}$$

While recall and precision's harmonic mean, or the F1-measure is determined as follows:

$$F1measure = 2\mathrm{xPrecision} \times Recall \,/\, Precision + Recall \tag{3}$$

6. RESULTS AND DISCUSSION

The author has covered cyber security based on SVM-PCA and RNN. Sensitive data-like academic, financial, or personal information-may make up a sizable amount of the data, along with other kinds of information for which improper access or introduction could have dire repercussions. Using the previously mentioned NSL-KDD dataset, the suggested cyber-security solution is evaluated. This approach allows the author to identify different kinds of attacks through the use of machine learning and deep learning techniques. Work area application that alerts the webserver system when it detects a UWSN attack. Compared to typical systems, Gated Recurrent Units can produce many comparable outputs with less preparation time. RNN's layers are able to get successive associations from these higher level highlights, as demonstrated above. Models are developed to assess the probability of succeeding whole number dispersion into the termed sequences on typical named successions.

The likelihood of a complete sequence is then predicted by browsing the limit of characterizations as a scope for harmful logarithm probability esteems. The sequences of full number calls make up the system call that follows. The varied and dynamic environment of system call structures makes it challenging to discern between normal and abnormal activity in Underwater Wireless Sensor Network. An assault is defined as any attempt to find, modify, change, weaken, empower, destroy, take, or add illegal access to or usage of information in PCs and PC systems.

A cyber-attack is a type of cyber-attack that goes after computer networks, devices, systems, or data bases. The people or processes known as attackers try to gain unauthorized access to data, capacity, or other restricted portions of the system, possibly with malicious intent.

Figure 7 shows the results of the proposed SVM-PCA-CNN method with the highest degree of accuracy among other methods, reaching 97% to detect anomalies in network traffic that indicate a cyberattack detection in UWSN that contributes to reducing the chances of attack.

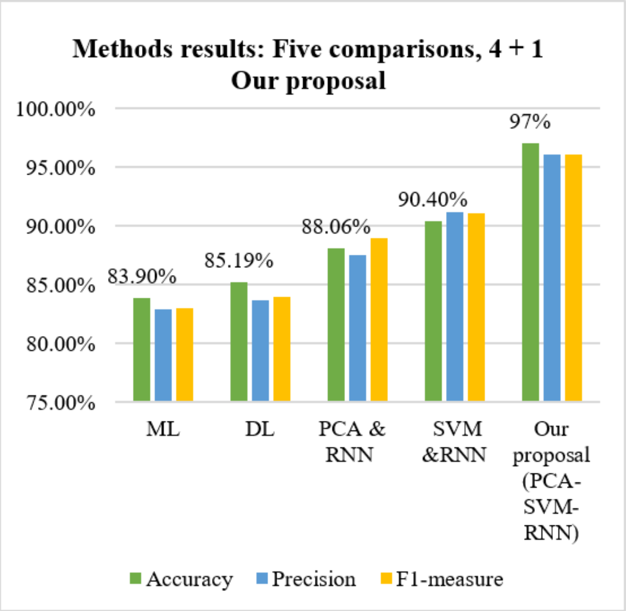

Figure 7. The results

Figure 8 shows the training accuracy on the trained data set in cyberattack classifications. By training us to classify cyberattacks with the highest possible accuracy, the proposed hybrid approach enhances the quality of contribution by integrating the advantages of deep learning and machine learning by measuring accuracy and effectiveness using the proposed method detects UWSN attack.

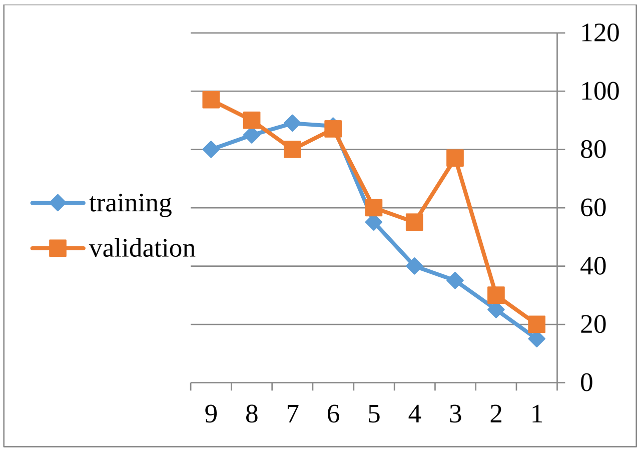

Figure 8. The accuracy for proposed method

7. CONCLUSIONS

These days, wireless sensor networks are a fascinating field for academics. This field is expanding more quickly than other fields as a result of technological improvements. Due to the network's design, transmissions are disseminated in an open space. The Underwater Wireless Sensor Network taxonomy was examined in this study using up-to-date research articles and reputable databases. Additionally, this study lists and evaluates the existing layer-by-layer security risks for Underwater Wireless Sensor Networks. Although UWSNs have advanced significantly in recent years, more work needs to be done, particularly in the area of large-scale system construction. This investigation evaluated the F-measure, accuracy, and precision of the suggested technique using the NSL-KDD dataset as its main focus. In addition, the suggested SVM-PCA for machine learning techniques. Additionally, the DL model was used for additional feature extraction and RNN attack categorization.

The SVM and PCA were employed because they can tolerate noisy data and outliers, both of which are common in real-world cyberattack scenarios. This ensures dependable performance even when dealing with partial or inaccurate data. This paper evaluates the accuracy of a proposed deep learning-based intrusion detection and classification technique called Recurrent Neural Networks (RNNs). We selected the RNN because, due to its exceptional ability to identify patterns in sequential data, it is ideally suited to identify anomalies in network traffic that may indicate a cyberattack.Our goal in this research is to examine how these two technologies might be combined to create a lightweight security framework for UWSNs. In order to improve UWSN security, we will take into account putting the suggested framework into practice and assess the integrated system's performance in subsequent work.

REFERENCES

[1] Naser, S.M., Ali, Y.H., OBE, D.A.J. (2022). Deep learning model for cyber-attacks detection method in wireless sensor networks. Periodicals of Engineering and Natural Sciences, 10(2): 251-259. https://doi.org/10.21533/pen.v10i2.2838

[2] Behiry, M.H., Aly, M. (2024). Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. Journal of Big Data, 11(1): 16. https://doi.org/10.1186/s40537-023-00870-w

[3] Saeed, K., Khalil, W., Al-Shamayleh, A.S., Ahmad, I., Akhunzada, A., ALharethi, S.Z., Gani, A. (2023). Analyzing the impact of active attack on the performance of the AMCTD protocol in Underwater Wireless Sensor Networks. Sensors, 23(6): 3044. https://doi.org/10.3390/s23063044

[4] Majid, M., Habib, S., Javed, A.R., Rizwan, M., Srivastava, G., Gadekallu, T.R., Lin, J.C.W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6): 2087. https://doi.org/10.3390/s22062087

[5] Duo, W., Zhou, M., Abusorrah, A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges. EEE/CAA Journal of Automatica Sinica, 9(5): 784-800. https://doi.org/10.1109/JAS.2022.105548

[6] Fattah, S., Gani, A., Ahmedy, I., Idris, M.Y.I., Targio Hashem, I.A. (2020). A survey on Underwater Wireless Sensor Networks: Requirements, taxonomy, recent advances, and open research challenges. Sensors, 20(18): 5393. https://doi.org/10.3390/s20185393

[7] Maseer, Z.K., Kadhim, Q.K., Al-Bander, B., Yusof, R., Saif, A. (2024). Meta-analysis and systematic review for anomaly network intrusion detection systems: Detection methods, dataset, validation methodology, and challenges. IET Networks, 1-38. https://doi.org/10.1049/ntw2.12128

[8] Mohsan, S.A.H., Mazinani, A., Othman, N.Q.H., Amjad, H. (2022). Towards the internet of underwater things: A comprehensive survey. Earth Science Informatics, 15(2): 735-764. https://doi.org/10.1007/s12145-021-00762-8

[9] Hussain, A., Hussain, T., Ullah, I., Muminov, B., Khan, M.Z., Alfarraj, O., Gafar, A. (2023). CR-NBEER: Cooperative-relay neighboring-based energy efficient routing protocol for marine underwater sensor networks. Journal of Marine Science and Engineering, 11(7): 1474. https://doi.org/10.3390/jmse11071474

[10] Kumar, D.P., Amgoth, T., Annavarapu, C.S.R. (2019). Machine learning algorithms for wireless sensor networks: A survey. Information Fusion, 49: 1-25. https://doi.org/10.1016/j.inffus.2018.09.013

[11] Yazdinejad, A., Kazemi, M., Parizi, R.M., Dehghantanha, A., Karimipour, H. (2023). An ensemble deep learning model for cyber threat hunting in industrial internet of things. Digital Communications and Networks, 9(1): 101-110. https://doi.org/10.1016/j.dcan.2022.09.008

[12] Ahmed, S.T., Kadhem, S.M. (2023). Optimizing Alzheimer 's disease prediction using the nomadic people algorithm. International Journal of Electrical and Computer Engineering (IJECE), 13(2): 2052-2067. https://doi.org/10.11591/ijece.v13i2.pp2052-2067

[13] Kadhim, Q.K., ismaeel Altameemi, A., Mohammed, S.J., Alsiadi, W.A.W. (2023). Artificial intelligence techniques for colon cancer detection: A review. AL-

Yarmouk Journal, 21(2): 11-18. https://www.iasj.net/iasj/article/289579

[14] Handa, A., Sharma, A., Shukla, S.K. (2019). Machine learning in cybersecurity: A review. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 9(4): e1306. https://doi.org/10.1002/widm.1306

[15] Kadhim, Q.K., Alwan, O.F., Khudhair, I.Y. (2024). Deep learning methods to prevent various cyberattacks in cloud environment. Revue d'Intelligence Artificielle, 38(3): 893-900. https://doi.org/10.18280/ria.380316

[16] Dhahi, S.H., Dhahi, E.H., Ahmed, S.T., Kadhim, Q.K. (2024). Predicting Parkinson's disease using filter feature selection method. AIP Conference Proceedings, 3051(1): 030002. https://doi.org/10.1063/5.0191620

[17] Kadhim, Q.K., Yusof, R., Mahdi, H.S., Selamat, S.R. (2017). The effectiveness of random early detection in data center transmission control protocol-based cloud computing networks. International Journal on Communications Antenna and Propagation (IRECAP), 7: 1-7. https://doi.org/10.15866/irecap.v7i5.10104

[18] Sudhakar, M., Kaliyamurthie, K.P. (2022). Machine learning algorithms and approaches used in cybersecurity. In 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), Bangalore, India, pp. 1-5. https://doi.org/10.1109/GCAT55367.2022.9971847

[19] Berman, D.S., Buczak, A.L., Chavis, J.S., Corbett, C.L. (2019). A survey of deep learning methods for cyber security. Information, 10(4): 122. https://doi.org/10.3390/info10040122

[20] Reddy, G.N., Reddy, G.J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. IOP Conf. Series: Materials Science and Engineering, September. arXiv Preprint arXiv:1402.1842. https://doi.org/10.48550/arXiv.1402.1842

[21] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, pp. 371-390. https://doi.org/10.23919/CYCON.2018.8405026

[22] Alwan, O.F., Kadhim, Q.K., Issa, R.B., Ahmed, S.T. (2023). Early detection and segmentation of ovarian tumor using convolutional neural network with ultrasound imaging. Revue d'Intelligence Artificielle, 37(6): 1503-1509. https://doi.org/10.18280/ria.370614

[23] Hussein, A.A., Ramadhan, A.J., TaeiZadeh, A., Issa, M.H. (2024). A Salp Swarm Algorithm for interpreting model predictions. BIO Web of Conferences. EDP Sciences, 97: 00162. https://doi.org/10.1051/bioconf/20249700162

[24] Ferrag, M.A., Maglaras, L., Moschoyiannis, S., Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50: 102419. https://doi.org/10.1016/j.jisa.2019.102419

[25] Dixit, P., Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. Computer Science Review, 39: 100317. https://doi.org/10.1016/j.cosrev.2020.100317

[26] Zhou, B., Li, S., Wang, J., Cheng, Y., Wu, J. (2023). A secure model against mobile sink replication attacks in unattended sensor networks. Computer Networks, 221: 109529. https://doi.org/10.1016/j.comnet.2022.109529

[27] Ahmed, S.T., Kadhem, S.M. (2021). Applying the MCMSI for online educational systems using the two-factor authentication. International Journal of Interactive Mobile Technologies, 15(13): 162-171. https://doi.org/10.3991/ijim.v15i13.23227

[28] Thamilarasu, G., Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the internet of things. Sensors (Switzerland), 19(9): 1977. https://doi.org/10.3390/s19091977

[29] Sajmath, P.K., Ravi, R.V., Majeed, K.K.A. (2020). Underwater wireless optical communication systems: A survey. In 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, pp. 1-7. https://doi.org/10.1109/ICSSS49621.2020.9202150

[30] Hadi, T.H., Kadum, J., Kadhim, Q.K., Ahmed, S.T. (2024). An enhanced cloud storage auditing approach using boneh-lynn-shacham's signature and automatic blocker protocol. Ingénierie Des Systèmes d'Information, 29(1): 261-268. https://doi.org/https://doi.org/10.18280/isi.290126

[31] Kadhim, Q.K., Yusof, R., Mahdi, H.S., Ali Al-shami, S.S., Selamat, S.R. (2018). A review study on cloud computing issues. Journal of Physics: Conference Series, 1018: 012006. https://doi.org/10.1088/1742-6596/1018/1/012006

[32] Ahmed, S.T., Khadhim, B.J., Kadhim, Q.K. (2021). Cloud services and cloud perspectives: A review. IOP Conference Series: Materials Science and Engineering, 1090(1): 012078. https://doi.org/10.1088/1757-899X/1090/1/012078

[33] Jin, X., Liang, J., Tong, W., Lu, L., Li, Z. (2017). Multi-agent trust-based intrusion detection scheme for wireless sensor networks. Computers & Electrical Engineering, 59: 262-273. https://doi.org/10.1016/j.compeleceng.2017.04.013

[34] Khadhim, B.J., Kadhim, Q.K., Khudhair, W.M., Ghaidan, M.H. (2021). Virtualization in mobile cloud computing for augmented reality challenges. In 2021 2nd Information Technology to Enhance E-Learning and Other Application (IT-ELA), Baghdad, Iraq, pp. 113-118. https://doi.org/10.1109/IT-ELA52201.2021.9773680

[35] Kadhim, Q.K., Altameemi, A.I., Abdulkader, R.M., Ahmed, S.T. (2024). Enhancement of data center Transmission Control Protocol performance in network cloud environments. Ingénierie des Systèmes d'Information, 29(3): 1115-1123. https://doi.org/10.18280/isi.290329

[36] Kadhim, Q.K., Al-Nedawe, B.M., Hameed, E.M. (2021). Encryption and decryption of images using GGH algorithm: Proposed. IOP Conference Series: Materials Science and Engineering, 1090(1): 012063. https://doi.org/10.1088/1757-899X/1090/1/012063

[37] Mohammed, H.A.A., Ahmed, S.T., Zaki, R.M.H., Kadhim, Q.K. (2024). Detection and localization of wrist fractures in x-ray imagery using deep learning teaching. Review of Computer Engineering Research, 11(3): 85-98. https://doi.org/10.18488/76.v11i3.3850

[38] Hameed, E.M., Hussein, I.S., Altameemi, H.G., Kadhim, Q.K. (2022). Liver disease detection and prediction using SVM techniques. In 2022 3rd Information Technology to Enhance e-Learning and Other Application (IT-ELA), Baghdad, Iraq, pp. 61-66. https://doi.org/10.1109/IT-ELA57378.2022.10107961

[39] Mohammed, H.A., Nazeeh, I., Alisawi, W.C., Kadhim, Q.K., Ahmed, S.T. (2023). Anomaly detection in human disease: A hybrid approach using GWO-SVM for gene selection. Revue d'Intelligence Artificielle, 37(4): 913-919. https://doi.org/10.18280/ria.370411

[40] Singh, S., Agrawal, S., Rizvi, M.A., Thakur, R.S. (2011). Improved support vector machine for cyber attack detection. In Proceedings of the World Congress on Engineering and Computer Science, San Francisco, USA.

[41] Veena, K., Meena, K., Teekaraman, Y., Kuppusamy, R., Radhakrishnan, A. (2022). C SVM classification and KNN techniques for cyber crime detection. Wireless Communications and Mobile Computing, 2022(1): 3640017. https://doi.org/10.1155/2022/3640017

[42] Ghanem, K., Aparicio-Navarro, F.J., Kyriakopoulos, K.G., Lambotharan, S., Chambers, J.A. (2017). Support vector machine for network intrusion and cyber-attack detection. In 2017 Sensor Signal Processing for Defence Conference (SSPD), London, UK, pp. 1-5. https://doi.org/10.1109/SSPD.2017.8233268

[43] Jha, S., Prashar, D., Long, H.V., Taniar, D. (2020). Recurrent neural network for detecting malware. Computers & Security, 99: 102037. https://doi.org/10.1016/j.cose.2020.102037

[44] Becerra-Suarez, F.L., Tuesta-Monteza, V.A., Mejia-Cabrera, H.I., Arcila-Diaz, J. (2024). Performance evaluation of deep learning models for classifying cybersecurity attacks in IoT networks. Informatics, 11(2): 32. https://doi.org/10.3390/informatics11020032

[45] Khadhim, B.J., Kadhim, Q.K., Shams, W.K., Ahmed, S.T., Wahab Alsiadi, W.A. (2023). Diagnose COVID-19 by using hybrid CNN-RNN for chest X-ray. Indonesian Journal of Electrical Engineering and Computer Science, 29(2): 852-860. https://doi.org/10.11591/ijeecs.v29.i2.pp852-860

[46] Urmi, W.F., Uddin, M.N., Uddin, M.A., Talukder, M.A., Md. Hasan, R., Paul, S., Chanda, M., Ayoade, J., Khraisat, A., Hossen, R., Imran, F. (2024). A stacked ensemble approach to detect cyber attacks based on feature selection techniques. International Journal of Cognitive Computing in Engineering, 5: 316-331. https://doi.org/10.1016/j.ijcce.2024.07.005

[47] Gopalakrishnan, T., Ruby, D., Al-Turjman, F., Gupta, D., Pustokhina, I.V., Pustokhin, D.A., Shankar, K. (2020). Deep learning enabled data offloading with cyber attack detection model in mobile edge computing systems. IEEE Access, 8: 185938-185949. https://doi.org/10.1109/ACCESS.2020.3030726