ELIMINATION OF DATA MODIFICATION IN SENSOR NODES OF WSN USING DEEP LEARNING MODEL

B. Chellapraba[1], M.S. Kavitha[2], K. Periyakaruppan[3] and D. Manohari[4]
[1]*Department of Information Technology, Karpagam Institute of Technology, India*
[2,3]*Department of Computer Science & Engineering, SNS College of Technology, India*
[4]*Department of Computer Science and Engineering, St. Joseph's Institute of Technology, India*

Abstract

This study focuses on removing the possibility of malicious data manipulation in wireless sensor networks (WSN) by utilising a deep learning method. When training deep neural networks, datasets that have been the subject of an attack that alters the data are used as the building blocks. This is done in preparation for putting the networks to the test in the real world. We find out through simulation with a 70:30 cross-validation across a 10-fold sample size that the proposed technique is superior to the current state of the art in terms of the packet delivery rate, latency and throughput.

Keywords:

Deep Learning Model, Data Modification, WSN, Throughput

1. INTRODUCTION

In recent years, there has been a surge in the amount of data that has been captured and transferred in the form of streams across the network. As a result, there has been a significant increase in the amount of interest from academics in this topic. A breach in the security of a computer network could result in the revelation or destruction of sensitive data, in addition to a loss of productivity and the financial advantage that would have accrued from their use [1]. Anomaly-based detection and misuse-based detection, both of which are types of signature-based detection, are two important kinds of ways to identify abnormalities that may indicate the manifestations of intrusions and are used to protect network security. Both of these types of signature-based detection are important ways to identify abnormalities that can be used to protect network security. Signature-based detection is another name for detection that is based on past misuse [2].

The methodologies for detecting misuse based on audit streams begin by extracting the properties of the audit streams themselves, which are then compared to signatures developed by specialists in the relevant fields. Patterns or rules could represent these signatures depending on the context. When certain aspects match up to one or more specified signatures but not all of them, this is known as the discovery of an incursion. When applied to the process of identifying typical types of infiltration, the misuse-based detection techniques give solid results and are not difficult to put into practise [3]. Misuse-based detection systems are ineffective due to the fact that professionals in the relevant domains do not have knowledge about incursions that have not been found before. As a result of this lack of awareness, it is difficult to identify potential dangers. Detection methods that are based on anomalies, on the other hand, develop models or profiles of normal data and then interpret any data that deviates from the norm as possibly posing a threat [4].

Using these strategies, it is feasible to recognise newly started invasions. On the other hand, they usually have a high false positive rate (FPR), and the vast majority of them do not have sufficient processes to deal with false positives. Nevertheless, they are able to detect a higher proportion of true positives. They rely exclusively on automated technologies to carry out extra screening of the identified irregularities, as opposed to putting all of their faith in human persons (such as security agents), who could potentially make mistakes [5]. Procedures that are similar to these take a considerable amount of time and have a high risk of creating errors. As a result of the growing importance placed on the detection of new attacks as a priority above maintaining a low rate of false positives, anomaly-based detection strategies are becoming an increasingly common method of choice (FPR). The difficulty of outlier detection is substantially comparable to that of the concept of detection based on anomalies, which is essentially the same thing. Utilizing the outlier identification methodologies that have been developed over the course of the past several years is therefore a solution that can be put into practise as a remedy to the problem of anomaly detection [6].

Data streams that originate from wireless networks are typically characterised as arriving in the form of a stream of high-dimensional connection-oriented records. This is because wireless networks enable connections to be made between devices in the network. These records each contain a range of characteristics that can be applied to the process of quantifying the quantity of network traffic that is currently taking place. It is a feature of high-dimensional data to have practically all anomalies confined within particular lower-dimensional subspaces. One characteristic that differentiates high-dimensional data from other types of data is this one [7]. When talking about high-dimensional space, these kinds of irrationalities are referred to as projected anomalies, which is a word coined by the authors of the paper. You can thank the Dimensional Tragedy for getting you out of this problem because it was caused by it. When there are a greater number of dimensions, the values are dispersed across the space in a manner that is more uniform. Because of this, distinguishing between various data points will get progressively more difficult as time goes on [8].

The only data subspaces that enable the detection of substantial outliers in the data are those with a dimensionality that is either moderate or low. The challenge of identifying anomalies that have been projected in high-dimensional data streams might be stated as follows:

Given a data stream D with a theoretically limitless number of dimensional data points, each data point $p_i = p_{i1}, p_{i2},..., p_i$ in D will be labelled as either a projected anomaly or an ordinary data point if it is discovered to be abnormal in one or more subspaces. In other words, the issue can be described in the following manner: In the event that this step is skipped, the data will be processed as though it were a typical piece of data, despite the fact that its size could be unconstrained at any point. The boundary subspace that corresponds to an anomaly that has been projected, denoted by p_i, will be included in the output [9].

The vast majority of traditional outlier and anomaly detection algorithms can only be utilised on data sets that have a low dimensionality and are static, which severely restricts their applicability. This is because these two types of algorithms require a relatively uniform distribution of data points. Finding and analysing anomalies in high-dimensional data as well as data streams that are being collected in real time is a field of study that is attracting an increasing lot of attention.

On the other hand, at this point in time, there has not been a whole lot of serious research done on the prospect of combining these two strong academic fields. Because so many of the techniques for detecting projected outliers in high-dimensional spaces involve doing many scans of the data, these techniques are unable to deal with data streams that are always in motion. In addition, the measurements that are utilised in the process of determining whether or not points constitute an outlier are unable to undergo incremental updates. It is not possible to locate the projected outliers using these approaches since the conclusions that may be drawn from the methods for identifying data stream outliers depend on having access to the entire dataset [10].

We have developed a novel strategy that makes use of a deep learning model for the aim of spotting anomalies in high-dimensional data streams. This approach that we have created was developed by us. WSN has begun the process of implementing a deep learning model in order to protect itself from attacks that include the manipulation of data. When training deep neural networks, datasets that have been the subject of an attack that alters the data are used as the building blocks. This is done in preparation for putting the networks to the test in the real world.

2. RELATED WORKS

On the topic of denial-of-service attacks and security for wireless sensor networks, there has only been a small amount of research that has been published. Research has been done on the topic of denial-of-service (DoS) attacks on WSN and the countermeasures that have been taken to prevent these attacks.

The authors of [8] did study in 2002 on the topic of denial-of-service (DoS) attacks and the mechanisms that are used to protect against them. In this research, two effective methodologies for sensor networks were studied to detect probable entry sites for a denial-of-service attack. In addition to providing the most recent statistics on DoS attacks and strategies to protect against them in WSN, the authors of [9] also provide a poll for readers to participate in. They analysed the denial-of-sleep attack, which is meant to disrupt sensor networks by disrupting their energy-saving systems. They conducted an investigation into this attack. In addition to analysing the features of these networks, the researchers looked into a wide range of security approaches that may be implemented to address the problems that were found. On the other hand, the findings of our survey offer up-to-date information regarding the aforementioned risks and the preventative measures that can be taken. In addition, we compared and contrasted these safeguards, as well as evaluated them, providing constructive criticism as well as recommendations regarding how they could be enhanced.

There has not been a lot of research carried out on the subject of WSN security up until this point. The authors of [10] carried out a comprehensive investigation into the problems and threats that are connected to WSN security. Their findings are presented in this article. They started their research of the problems with the security of WSNs from the highest level of the network and worked their way down, looking at the attacks and defences at each successive tier of the network. A significant amount of back-and-forth conversation took place about cryptography, key management, secure routing, safe data aggregation, and intrusion detection, as well as the challenges and potential solutions that are related with each of these issues on their own. The findings of yet another in-depth investigation on the subject of defending wireless sensor networks were published in [11], which was done by the same team of researchers. We took a look at some of the most widespread concerns regarding the security of WSNs, as well as some potential ways to address those concerns. The authors provided a detailed investigation of the perils, preventative safety measures, and difficulties posed by wireless sensor networks at [12]. The study may find the poll that compares the security of WSNs with that of wired and other wireless networks (and more) at [13]. This survey was made accessible by the authors and can be found at that location.

After offering a quick assessment of the state that WSN security is in at the moment, the authors of [14] present an explanation of the challenges that are now being encountered by this field. They explored a variety of frequent forms of attacks and arranged them into categories in accordance with the OSI stack model. These attacks are focused on one or more layers in particular. In addition to this, we presented a list of potential countermeasures and reactions to these attacks, as well as research gaps and difficulties that require more exploration. Both the limits that are imposed by a WSN and the safeguards that are put in place to protect them from potential vulnerabilities were meticulously documented by the authors of [15], who carried out a comprehensive examination into the safety of WSNs. Another problem that was brought up was how difficult it might be to design and implement reliable security mechanisms.

Several surveys about WSNs have been carried out on various fields of application, including but not limited to healthcare, the military, artificial intelligence, automation in industry, and other similar topics. The overwhelming majority of this research concentrated on general, overarching concerns about WSN security as well as ways to manage or minimise the dangers associated with such concerns. Even though research has been done on DoS attacks on WSN, none of the earlier studies have focused on attacks that can bring the whole WSN to a standstill.

The primary focus of our research is on malicious activities directed toward wireless sensor networks, one of which is the manipulation of data. Because attacks that change data are so common in wireless networks, and because they create a large demand on the resources that are available on wireless nodes, these attacks are able to effectively negate the purpose that was intended for the deployment of the system. As a consequence of this, we make current information regarding data modification attacks on WSN available to our customers. Within the framework of the hybrid layering concept, we classify these attacks and the tactics used to defend against them as belonging to a variety of different layers. In addition, in order to address the concerns and difficulties that have surfaced, we have proposed a number of improvements that might be made to the current state of the art in defensive strategies. These suggestions have been made in order to address the concerns that have been raised and the difficulties that have been encountered.

3. PROPOSED METHOD

This study focuses on removing the possibility of malicious data manipulation in wireless sensor networks by utilising a deep learning method (WSN). When training deep neural networks, datasets that have been the subject of an attack that alters the data are used as the building blocks. This is done in preparation for putting the networks to the test in the real world. The Fig.1 is one illustration that demonstrates this point. The necessity for data manipulation is shown to be eliminated in Fig.1, which explains how deep learning (DL).

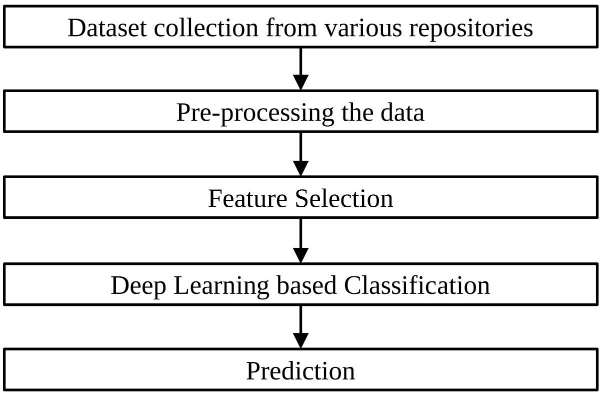
Dataset collection from various repositories
Pre-processing the data
Feature Selection
Deep Learning based Classification
Prediction

Fig.1. Data Modification Elimination

The learning phase and the detection phase are the two key stages that are involved in our DL-DME approach to the detection of anomalies in data streams. We may think of these stages as having a two-phase structure. Because of this simplification, we will have an easier time comprehending the procedure. In addition to this, DL-DME may also make it possible for learning to take place offline in addition to online. During the offline learning phase of the procedure, the SST is formed utilising both labelled anomalous examples as well as unlabeled training data. These labelled cases are contributed by domain experts. The data sparsity and outliers that are displayed in the SST subspaces are much more prominent when compared to those that are displayed in the other subspaces.

However, adding unsupervised and supervised subspaces is totally voluntary in DL-DME, despite the fact that fixed subspaces are required for the algorithm. The DL-DME is useful for gaining an understanding of the potential locations in high-dimensional space where expected anomalies may be found. The bulk of the time, DL-DME is manufactured without the use of marked samples being applied. Even though DL-DME has made substantial headway, it is still possible to improve it even more by utilising the indicated anomalous exemplars. This is the case despite the fact that DL-DME has achieved significant success. Because of its adaptability, DL-DME can be utilised in a wide variety of real-world applications, some of which may or may not have access to labelled examples. This flexibility makes it possible for DL-DME to be deployed. This capacity is what gives DL-DME its adaptability, therefore it important to remember that.

During the phase of detection, DL-DME has the capability to begin the screening for expected anomalies using the data that is continuously being input. This screening uses the data that is being continuously input. The process of amending the data summary for each region will include the incorporation of any new information that becomes available as part of the revision process. The data will be tagged as abnormal, and the flagging process will begin, if the summary value drops below certain constraints; this will cause the procedure to begin. The Outlier Repository is a database where all of the abnormalities that have been found are compiled and kept a record of for future reference. After the detection phase is complete, customers will either receive a subset of the top anomalies from the Outlier Repository or all of the top anomalies from the Outlier Repository, depending on which option they choose.

During the phase of detection, DL-DME may opt to take part in periodic online training sessions if they so wish. One component of online training is called retraining, and it involves making use of DL-recently DME found sparse subspaces. This part of the procedure takes place in accordance with the data attributes that are now available as well as any anomalies that have been spotted. The ability of DL-adaptability DMEs to accommodate shifting data streams can be strengthened through participation in online training.

3.1 DEEP LEARNING MODEL

It is possible to learn an efficient encoding or representation of the original data by utilising a deep autoencoder, which is a specific type of DNN whose output has the same dimension as its input. In other words, its output has the same number of dimensions as its input. This is something that can be attained through the process of learning. The autoencoder is a nonlinear feature extraction method that does not require the use of class labels as a prerequisite for its application. Despite the fact that the two goals are occasionally intertwined, the extracted feature gives information preservation a greater priority than classification tasks. This is due to the fact that information preservation is more important.

The input layer, which shows the original data or feature, is positioned below the one or more hidden layers, which represent the modified feature. This is because the input layer is located below the one or more hidden layers that represent the modified feature. Above the input layer is where you'll find the output layer, which displays the original data or feature and corresponds to the input layer for the purpose of reconstruction. Finding out whether or not an autoencoder has more than one buried layer enables one to evaluate whether or not the autoencoder is considered deep. It is entirely conceivable for the dimension of the hidden layers to be smaller or larger than the dimension of the data that was first supplied. One or the other is a distinct possibility.

Backpropagation can be executed in a great number of distinct ways, and auto-encoders are often educated utilising one of these versions. Despite the fact that it has certain fundamental flaws, back-propagation is often a pretty effective method for training networks that have a large number of hidden layers. However, it does have its own set of constraints. Errors are brought down to such a low level when back-propagated to the initial few layers of the network. As a result, additional training is virtually futile. Despite the fact that more recent approaches to backpropagation constitute an improvement, this method still produces extremely poor learning and worse solutions all around. As was discussed in earlier chapters, having your parameters originally established using an unsupervised pretraining approach, like as the DBN pretraining algorithm, could help alleviate some of the stress produced by this issue. This is because these methods are used to train models without human supervision.

The Fig.2 illustrates a deep generative model of spectrogram patches, which may be observed in the figure. This model has the capability of having 1, 3, 9, or 13 frames, and it has 256 frequency bins. One layer of linear variables with Gaussian noise and one layer of between 500 and 3000 binary latent variables are found in undirected graphical models that are known as Gaussian-Bernoulli RBMs. Both levels are contained within a single layer that sits between them. When training a second Bernays-Bernoulli RBM, the activation probabilities of the previously learned Gaussian-Bernoulli RBM hidden units are then used as input. This is done so that the new Bernoulli-Bernoulli RBM can learn from the previous model. When two RBMs are combined to form a deep belief net, it is not difficult to deduce the states of the second layer of binary hidden units based on the input in a single forward pass. This can be done after the RBMs have been merged. This can be accomplished with just one pass in the forward direction (DBN). The Fig.2 depicts the DBN that was utilised in this inquiry, are two RBMs, each of which is depicted in the relevant box that it occupies.

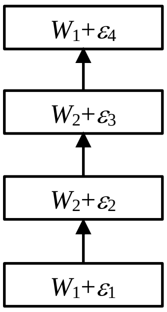

Fig.2. DBN model

We make use of the weight matrices that are generated by the DBN in order to unroll it and produce the deep autoencoder that has three hidden layers. This allows us to produce the deep autoencoder. In this particular instance of a deep autoencoder, the process of matrix encoding happens in the lower levels, while the process of matrix decoding happens in the upper layers, albeit in the reverse order. The Fig.2 depicts an illustration of how the deep autoencoder is fine-tuned by employing error back-propagation in order to reduce the overall amount of reconstruction error.

Following completion of the training, the procedure that will be outlined in the following paragraphs can be utilised to encode and reconstruct any spectrogram that possesses a length that is susceptible to modification. In order to supply a deep autoencoder with input data, we must first zero-mean and unit-variance normalise N consecutive overlapping frames of 256-point log power spectra. This step is necessary because we need to provide the autoencoder with data to work with. This step is carried out prior to the data being input into the autoencoder. After this step, the first hidden layer applies the logistic function to the activations that have real-valued inputs. These actual values are passed on to the subsequent coding layer in order to enable codes to be derived from the information that is provided. When the quantization threshold is set to 0.5, the activations of hidden units in the coding layer undergo a transformation that causes their underlying real values to be converted into integer values.

One of the most significant benefits is that the deep autoencoder many stages of nonlinear processing make it feasible to obtain accurate code from feature vectors. This is an advantage that cannot be overstated. On the other side, the outcome of implementing this method is to produce code that is resistant to being altered in any way. To put it another way, if the input feature vector is altered in any way, the code that is extracted will also shift in an unexpectedly different manner. This can be illustrated by the following example. This can be advantageous if the code evolves in such a way that it can be predicted to represent some underlying transformation-invariant property of the material as it is observed.

Capsules are small, self-contained sub-networks that each extract a single, specified feature representing a single visual or audio item. These sub-networks are referred to as capsules. Capsules are self-contained, miniature sub-networks that are the building blocks from which transforming auto-encoders are constructed. A changing auto-encoder receives a vector of input data as well as an output vector of interest; both of these vectors are then altered by a straightforward global transformation mechanism after being processed by the auto-encoder. The vector of interest that is produced as an output can then be used. The presumption here is that openness is being shown in relation to global change. The capsule outputs are used to generate the coding layer whenever a transforming autoencoder is being utilised as the method of data compression. In the course of the training phase, the various capsules learn to extract a range of entities in order to close the gap that currently separates the output they produce from the target they are aiming for.

4. RESULTS AND DISCUSSIONS

This simulation is used to evaluate the proposed routing algorithm by comparing its performance to that of the GA, which is the industry standard algorithm for usage in WSN routing. The evaluation is carried out with the assistance of this simulation. It has been shown that the proposed technique performs better than the baseline GA in each of the simulated benchmarks, and this fact has been demonstrated.

The results of the proposed deep learning model are depicted in Fig.2 in terms of the numerous sensor nodes where the attacks are prevented. The findings of the simulation indicate that the number of attempts to breach the network security increases in direct correlation with the size of the network node population. On the other hand, the simulation illustrates that the process of removing attacks can be sped up by defending against modification attacks. This is one of the key takeaways from the simulation. According to the findings, the proposed method may give an improvement over the existing state of the art in terms of the packet delivery rate.

The Fig.3 illustrates that the proposed method expedites the flow of data packets from the source nodes to the destination nodes while simultaneously and expeditiously removing any potential threats.

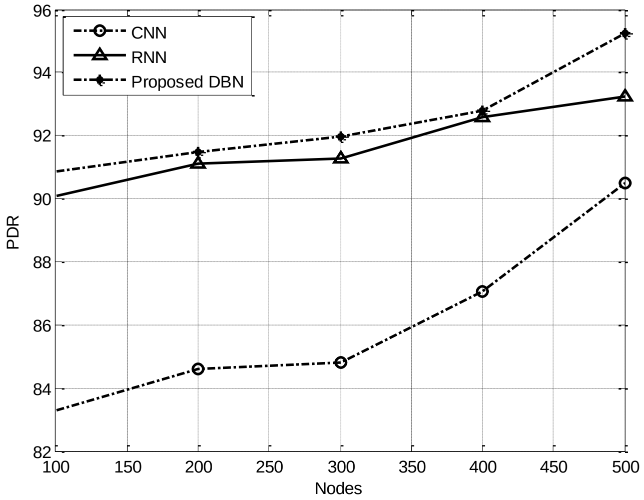

Fig.2. Packet Delivery Rate

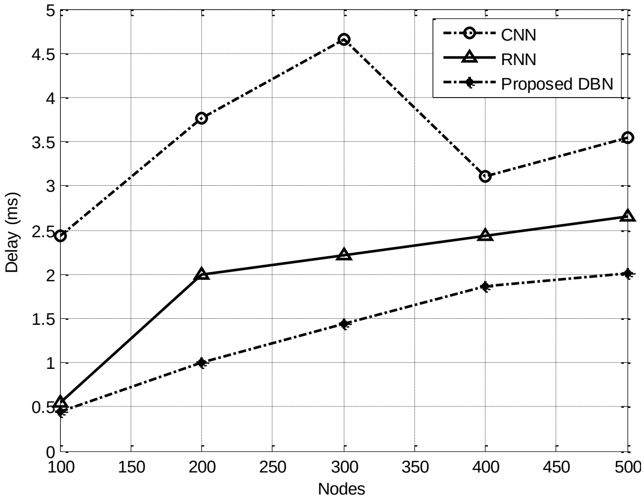

Fig.3. Delay

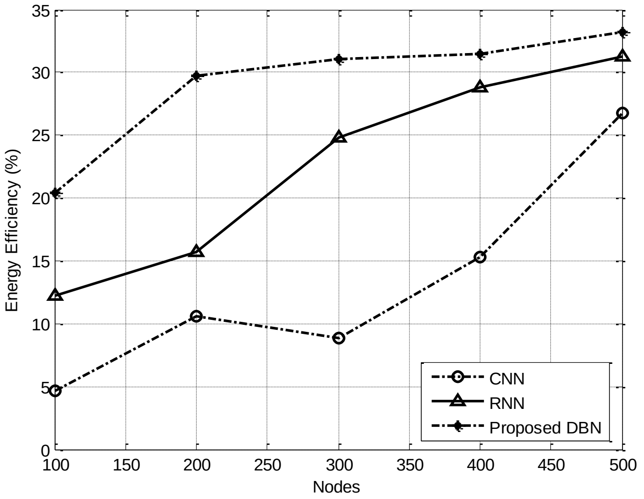

Fig.4. Throughput

Even while this leads to an overall improvement in the performance of the network (as can be seen in Fig.4), the attacks themselves are problematic for the system. This is the case despite the fact that the performance of the network improves. However, the solution that has been proposed eliminates the need to defend against attacks while simultaneously improving the capacity of the network.

The majority of the protective measures taken against modification attacks are based on methods such as acknowledgments, encryption, authentication, and others. These methods are at the core of the majority of these protective measures. These solutions are effective methods for addressing the problem of WSN updates being made to different networks. On the other hand, these nodes in the WSN are typically quite basic, have a restricted supply of power, and use a considerable number of resources.

5. CONCLUSIONS

This study focuses on removing the possibility of malicious data manipulation in WSN by utilising a DL method. When training deep neural networks, datasets that have been the subject of an attack that alters the data are used as the building blocks. This is done in preparation for putting the networks to the test in the real world. The results of a simulation that was run using 70:30 cross-validation across a 10-fold dataset show that the recommended method outperforms the current state of the art in terms of the packet delivery rate, latency, throughput, and energy efficiency. This was determined by comparing the results to the current state of the art. In addition, the results of the simulation show that the method that was offered is an efficient way to combat the network hazards, which enables the WSN to function normally. This was revealed by the findings of the simulation. In the future, it will be possible to thwart a bigger number of network attacks if the research is carried out using an unsupervised deep learning model.

REFERENCES

[1] S. Sundaram, M. Pajic and G.J. Pappas, “The Wireless Control Network: Monitoring for Malicious Behavior”, *Proceedings of IEEE Conference on Decision and Control*, pp. 5979-5984, 2010.

[2] L.M. Abdulrahman and K.H. Sharif, “A State of Art for Smart Gateways Issues and Modification”, *Asian Journal of Research in Computer Science*, Vol. 63, pp. 1-13, 2021.

[3] Z.H. Pang and G.P. Liu, “Detection of Stealthy False Data Injection Attacks against Networked Control Systems via Active Data modification”, *Information Sciences*, Vol. 546, pp. 192-205, 2021.

[4] M. Soni and D.K. Singh, “LAKA: Lightweight Authentication and Key Agreement Protocol for Internet of Things based Wireless Body Area Network”, *Wireless Personal Communications*, Vol. 122, 1-18, 2021.

[5] T. Karthikeyan and K. Praghash, “Improved Authentication in Secured Multicast Wireless Sensor Network (MWSN) using Opposition Frog Leaping Algorithm to Resist Man-in-Middle Attack”, *Wireless Personal Communications*, Vol. 123, No. 2, pp. 1715-1731, 2022.

[6] T.H. Hadi, "Types of Attacks in Wireless Communication Networks", *Webology*, Vol. 19, No. 1, pp. 1-13, 2022.

[7] R. Rajendran, "An Optimal Strategy to Countermeasure the Impersonation Attack in Wireless Mesh Network", *International Journal of Information Technology*, Vol. 13, No. 3, pp. 1033-1038, 2021.

[8] X.S. Shen and B. Ying, "Data Management for Future Wireless Networks: Architecture, Privacy Preservation, and Regulation", *IEEE Network*, Vol. 35, No. 1, pp. 8-15, 2021.

[9] M. Ponnusamy, P. Bedi and T. Suresh, "Design and Analysis of Text Document Clustering using Salp Swarm Algorithm", *The Journal of Supercomputing*, Vol. 87, pp. 1-17, 2022.

[10] Z. Bin and H. Jian Feng, "Design and Implementation of Incremental Data Capturing in Wireless Network Planning based on Log Mining", *Proceedings of International Conference on Advanced Information Technology, Electronic and Automation Control*, pp. 2757-2761, 2021.

[11] D. Dilmurod, S. Norkobilov and I. Jamshid, "Features of Using the Energy-Saving LEACH Protocol to Control the Temperature of Stored Cotton Piles via a Wireless Network of Sensors", *International Journal of Discoveries and Innovations in Applied Sciences*, Vol. 1, No. 5, pp. 278-283, 2021.

[12] W. Sun and Y. Gao, "The Design of University Physical Education Management Framework based on Edge Computing and Data Analysis", *Wireless Communications and Mobile Computing*, Vol. 122, pp. 1-16, 2021.

[13] H. Khalid, S.J. Hashim and M.A. Chaudhary, "Cross-SN: A Lightweight Authentication Scheme for a Multi-Server Platform using IoT-Based Wireless Medical Sensor Network", *Electronics*, Vol. 10, No. 7, pp. 790-810, 2021.

[14] A.N. Kadhim and S.B. Sadkhan, "Security Threats in Wireless Network Communication-Status, Challenges, and Future Trends", *Proceedings of International Conference on Advanced Computer Applications*, pp. 176-181, 2021.

[15] S. Jain, S. Pruthi and K. Sharma, "Penetration Testing of Wireless Encryption Protocols", *Proceedings of International Conference on Computing Methodologies and Communication*, pp. 258-266, 2022.