ISSN: 0067-2904

Proposed Security Models for Node-level and Network-level Aspects of Wireless Sensor Networks Using Machine Learning Techniques

A. Abirami , S. Palanikumar

Information Technology Department, Noorul Islam Centre for Higher Education, Tamilnadu, India

Received: 23/2/2022 Accepted: 22/11/2023 Published: 30/12/2023

Abstract

As a result of the pandemic crisis and the shift to digitization, cyber-attacks are at an all-time high in the modern day despite good technological advancement. The use of wireless sensor networks (WSNs) is an indicator of technical advancement in most industries. For the safe transfer of data, security objectives such as confidentiality, integrity, and availability must be maintained. The security features of WSN are split into node level and network level. For the node level, a proactive strategy using deep learning /machine learning techniques is suggested. The primary benefit of this proactive approach is that it foresees the cyber-attack before it is launched, allowing for damage mitigation. A cryptography algorithm is put forth and contrasted with the current algorithms at the network level. Elliptic Curve Cryptography combined with the Koblitz encoding technique produced superior results. By implementing machine learning and deep learning techniques, wireless sensor networks are protected against cyber-attacks, and the suggested encryption approach ensures the confidentiality of data transfer. The estimated encryption and decryption times were evaluated with various file sizes and contrasted with the current systems. The suggested solutions were successful in achieving security at both the node level and network level.

Keywords: Wireless Sensor Network, Cyber Security, Data Science, Machine Learning, Artificial Intelligence.

1. Introduction

Cyber security is a booming industry as per the need of the current situation. Hackers are quite clever when it comes to identifying system flaws and launching attacks. Sensitive information is the major target of attackers nowadays. This sensitive data includes personal information, bank details, patient data, etc. Active and passive attacks are two types of cyber-attacks. Active attacks are direct assaults on the system designed to destroy it. Because of an active attack, the data and the available resources are modified, which affects the normal functioning of the system. On the other hand, a passive attack silently exploits vulnerability in the system to enter the network using malware to collect sensitive data and use it without the knowledge of the owner. Hackers had more advantage, especially during the pandemic situation. Attacks, such as phishing attacks, credit card fraud, launching various malware through messages/ emails, etc., are more expected during such situations.

The traditional intrusion detection system is vulnerable to the new attacks launched by hackers. By using machine learning or deep learning methods to train the system, it is possible to identify both active and passive threats more effectively. The various stages of a machine learning-based study model for cyber security are explained in detail in this paper. The system

[*]Email: abi.lecturer@gmail.com

is trained effectively with the help of a dataset. The most popular dataset used in the field of cyber security is KDD Cup 1999, and UMASS dataset, etc. According to the survey, deep learning algorithms are more accurate than typical machine learning algorithms in terms of detecting assaults.

A cyber security assault consists of a series of one or more exploits that are used in succession or in parallel against a target system or a group of systems to reveal vulnerabilities and change the status of the targeted systems [1]. Hackers normally target computer systems, sensors, network communication mediums, websites, and sensitive information [2]. The victims' machines are targeted to hold control over the network by using botnets and other malware. There are so many challenges related to cyber security that every organization must have an analyst who makes sure that their system is secured. The main challenge related to cyber security is securing confidential data and servers of the organizations. An example of the most common cyber security attacks are Dark Hotel, Mirai, Stuxnet, WannaCry,and so on.

Vulnerability is a flaw in a system's design, execution, or maintenance that can be exploited. Vulnerability is a combination of one or more preconditions [1]. A system becomes vulnerable when it provides the opportunity for a threat to gain access to the system. Vulnerabilities [3] are majorly caused by the not updating the systems on a timely basis. Humans, data artifacts, and policies can all have weaknesses that adversaries can take advantage of, and exploits do not rely on just the network, software, or hardware vulnerabilities.

According to the 2016 Cisco Midyear Cyber Security Report, the average of the industry for detecting threats is 100-200 days and this rate is not fast enough. It is important to have a cyber security plan ready to face the ever-evolving security threats. Detection of Cyber Security Attacks is the scenario when one finds out that they or their organization have become the victim of a cyber-attack. However, many times the victims are completely unaware, and the attackers keep taking advantage of this situation and exploit it to satisfy their greed. As a result, cyber-attacks can be divided into two categories: passive and active.

A passive attack compromises the network's secrecy and privacy by listening in on data transmission between different entities [4]. In other words, using these types of attacks the attackers can sniff the messages between the nodes and analyze them to obtain sensitive information about the network of communication [5]. These types of attacks are hard to detect but easy to stop. An active attack sends data to all parties, functioning as a liaison and allowing server compromises. These types of attacks are easy to detect but difficult to stop.
Cyber Security's main purpose is to safely transport data, which emphasizes the creation of secure network architecture. These security services are necessary to safeguard data from many types of threats. Confidentiality, Integrity, Availability, and Non-repudiation [6] are the essential objectives.

In the subject of machine learning, learning algorithms can be represented as a hierarchical tree structure. The tree structure gives a simplified schema representation to rationalize the various types of learning algorithms in machine learning. Broadly, the algorithms of Traditional Machine Learning are divided into two types- Supervised and Unsupervised Learning. Models are trained using labeled data in supervised learning. Classification models, such as decision trees, Hidden Markov models, Random Forest, K-Nearest Neighbor(KNN), Naive Bayes, Support Vector Machine, and Regression models such as Linear regression and Logistic regression use supervised learning techniques. Models in Unsupervised Learning attempt to discover structure and patterns from incoming data. Clustering techniques like K-Means,

Singular Value Decomposition, DBSCAN, and Dimensionality are prominent unsupervised learning methods. Principal Component Analysis, Linear Discriminant Analysis, Gaussian Discriminant Analysis, and Association Mining algorithms like FP-Growth and Apriori are examples of reduction methods.
Modern Machine Learning algorithms are classified as Supervised and Unsupervised Learning, similar to Traditional Machine Learning algorithms. In most cases, supervised learning takes place in the context of classification or regression. It can be further classified as Feed Forward Deep Neural Network, Convolutional Neural Network, and Recurrent Neural Network. A Sine Cosine Optimization based RNN, which is a special type of Recurrent Neural Network popularly known as SCO-RNN [7,8]. Unsupervised learning models are implemented using algorithms such as Deep Belief Network, Restricted Boltzmann Machine, Deep Boltzmann Machine [9], and Auto Encoders.

The remaining paper is structured as follows. Section 2 discusses the various Machine learning algorithm related to cyber-security. Section 3 highlights the deep learning techniques that support the security aspects in the digital world. Section 4 outlines the proposed method concerning the security aspects of the Wireless sensor network. Section 5 discusses the implementation details and the comparative analysis of the existing system. Finally, we conclude the paper by providing suggestions for future research.

2. Machine learning for cyber security

In recent years, the domain of cyber security played the most important role in many fields. Due to its diversity and application areas, a huge data amount is generated from many heterogeneous sources. Such voluminous data provides greater scope and opportunities to cyber security experts and data scientists. Cyber security is one of the fields that are rapidly growing nowadays, especially in a pandemic situation, becoming an essential part to evolve an unknown pattern. Hence, we explore the variety of cyber-attack models for securing the network and applications.

Machine learning models have a greater potential for the adaptation of any new pattern. These technologies help to provide valuable contributions for protecting any IT infrastructure against cyber-attacks. This section discusses a few cyber-attack categories and their analysis using various machine learning techniques. Such adaptive techniques will help researchers to develop better methods and tools to detect and defend against attacks autonomously.

In general, for most cyber security applications, machine learning models follow the workflow depicted in Figure 1.

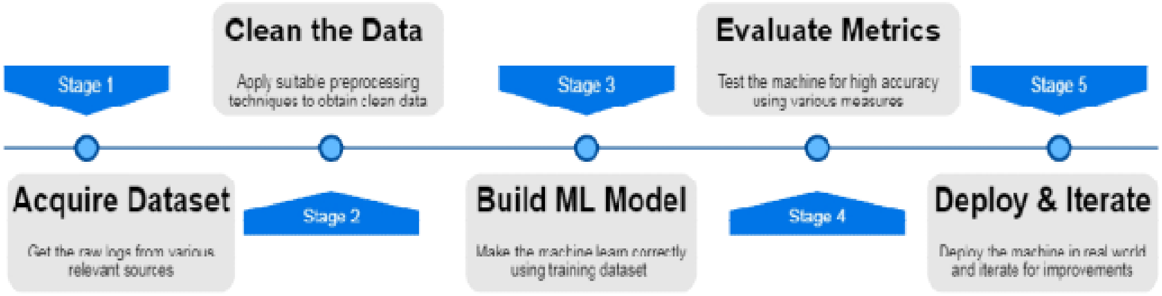
Stage 1
Acquire Dataset
Get the raw logs from various relevant sources
Stage 2
Clean the Data
Apply suitable preprocessing techniques to obtain clean data
Stage 3
Build ML Model
Make the machine learn correctly using training dataset
Stage 4
Evaluate Metrics
Test the machine for high accuracy using various measures
Stage 5
Deploy & Iterate
Deploy the machine in real world and iterate for improvements

Figure 1: Workflow of Machine Learning Model

2.1. Acquire Dataset :

As defined in **Figure 1**, stage 1 indicates the data collection from single or various sources available in different forms. The most challenging factor is the collection of real, labeled, and new datasets with sufficient size along with a proper description of each parameter. It is a known fact that a good dataset and the use of better methodology help in the analysis of data to make decisions and take proper actions appropriately. The various forms of the dataset used in cyber-attack detection are shown in **Figure 2**.

In the cyber security domain, the most frequently available datasets sources are KDD Cup 1999 datasets [10], NSL-KDD datasets, UMASS datasets, UNSW-NB15 datasets, DARPA datasets, etc. M.A. Ferrag, L. Maglaras, and S. Moschoyiannis et al.[9] classified publicly available datasets into seven types of datasets based on network traffic, Electrical network, Internet traffic, Virtual private network, Android applications, IoT traffic, and Internet-connected devices. R. Coulter [10] analyzed popular datasets, such as MODBUS SCADA datasets, used in detection models of cyber-attacks like android malware and software vulnerability.

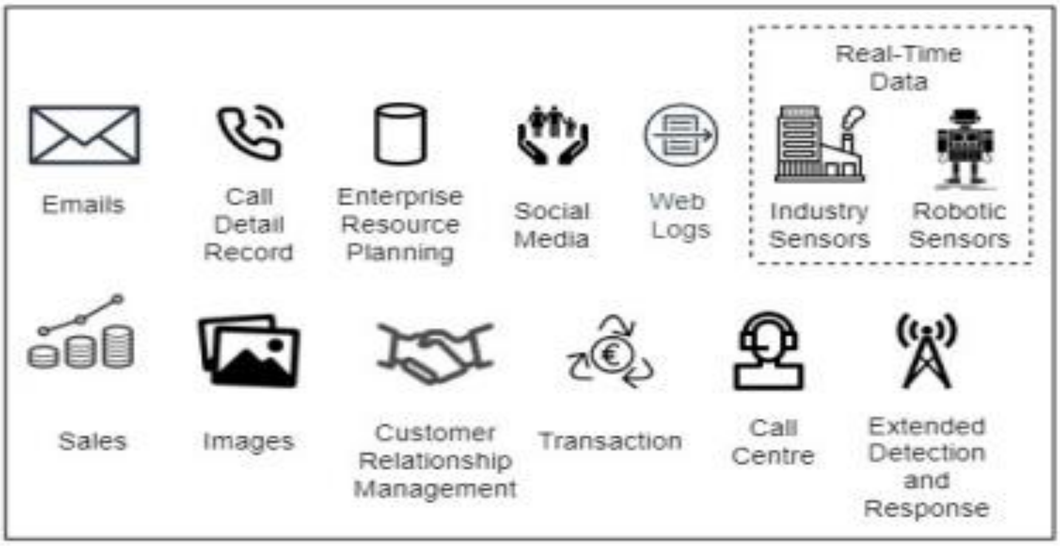

Figure 2: Various forms of cyber-attack dataset

Recently, cyber security has become an essential requirement in robotic and the Internet of Things (IoT) based systems. Many automated industrial systems use mobile robots for managing operational-level activities. There are more chances of cyber-attacks on these real-time systems. An example is examined in [13] to detect the power grid disturbances in the energy system, used real-time logs generated by phasor measurement units. Á.M. Guerrero-Higueras [12] discussed DoS and spoofing attack detection using a real-time recorded dataset collected from the wheeled robot and real-time location systems. M. Shafiq, Z. Tian, Y. Sun[13] used a Bot-IoT dataset for the identification of anomaly detection in an IoT environment. Such real-world datasets are mostly imbalanced and hence proper methodology is yet to be used to build prediction ML models.

2.2. Data Preprocessing

Data preprocessing is a key element in any machine learning model. It is used to simplify the raw data or real-time data to remove inconsistencies. There are various preprocessing techniques applied to the obtained data, such as managing missing values, imbalanced data, normalization, etc. These techniques are tailored with the aim of improving the performance of the machine learning-based model.

S. Agarwal [14] used the KDD99 dataset for intrusion detection systems and performed data conversion to meet the standards required to train the model. N. Neha [11]used the Secure Water Treatment testbed (SWaT) dataset in the proposed methodology. The SWaT dataset was preprocessed using a normalization technique to assign parameter values to a specific range instead of the existing range. In addition to replacing infinity and Not a Number (NaN) values, normalization techniques, such as Min-max and Z-score were also applied to the multi-classification dataset to improve the speed and accuracy of the trained model.
[17] discusses few studies that developed a cyber-attack detection model by applying feature selection as one of the techniques before the model was trained. Feature selection scheme helps in reducing the number of features and improving prediction accuracy for anomaly detection.

2.3. Build ML Model

Traditional Machine learning models, also known as shallow models, include supervised and unsupervised models. The detailed description of these models and their various algorithms is included in the later part of this paper. After data preprocessing, the cleaned dataset is divided into a training set and a testing set. Once the training dataset is prepared well with instances of events, detection or prediction models are developed. R. Coulter [10] demonstrated the detection of cyber-attacks in smart grids by using a feature extraction mechanism. Here, the training model used deep feature extraction with the aim of reducing the dimensionality of feature space, which also improves the efficiency and accuracy of the system.

Á.M. Guerrero-Higuer as used various ensembles and predictor algorithms to train the model to detect Denial of Service attacks and Spoofing attacks. Among these ML algorithms, the MLP classifier provided the best results for both Denial of Service and Spoofing attacks. In power grid systems to identify the faults and cyber-attacks, [12] proposed a detection model using a few classifier ML algorithms in the training phase. Adaboost being a powerful classifier performs better based on the combined features.

M. Shafiq [13], Z. Tian, and Y. Sun proposed a new framework for Bot-IoT attack identification using five different shallow machine learning algorithms for choosing the best classifier. Certain studies to detect cyber-attacks on certain infrastructure systems like [18] used Hidden Markov Model and Artificial Neural Network during the training phase. M. Swarnkarand N. Hubballi [17] detected an application-specific attack in the network traffic using one class Multinomial Naive Bayes classifier for training the model. H. Malhotra [15] used three ML algorithms, such as SVM, Naive Bayes, and Neural Network in their proposed study for anomaly detection and found that the neural network is one of the best classifiers depending on their comparative study.

3. Deep learning for cyber security

Deep neural networks or current machine learning models are the next sophisticated machine learning model to manage the complicated and massive datasets of any real-world situation. For the past several years, the number of researchers working in the cyber security space who use deep learning models has exploded. The main advantage of deep learning models is automatic feature engineering from the original data and working in an end-to-end way [19]. According to the studies, Deep learning models are majorly classified into the Deep Discriminative model and the Generative Neural Network model.

3.1. Deep Discriminative / Supervised Neural Network Models

A deep discriminative model is defined as a layered hierarchical architecture, which directly estimates and optimizes conditional probability distribution, p (y|x). Deep learning models have been found to attract more attention in a variety of sectors, according to researchers. It is mostly owing to its excellent capacity to extract features and achieve high accuracy using feature extraction methods [20]. Especially for large datasets, deep learning models have a greater advantage than traditional neural network models.

3.1.1. Feed Forward Deep Neural Network

The continual increase in cyber-attacks makes it more challenging to defend against such attacks using shallow machine learning. Hence Deep learning algorithms had a greater opportunity to build more discriminative and generalized models, helping in the detection of various attacks in the cyber security domain.

A feed-forward neural network is a complex neural network architecture, which requires large numbers of iterations to achieve the best accuracy. Dahl uses DNN for malware classification by combining feature selection techniques in dimensionality reduction. Deep neural network is used in the identification of Android malware classification, Incidents, and fraud detection [21]. Among all use cases using shallow and deep learning to classify malware and fraud detection, DNNs achieve better accuracy.

3.1.2. Recurrent Neural Network

A recurrent neural network overcomes the constraints of a standard neural network by being able to accommodate input sequences of varying durations. It works with one element at a time, using the concealed units' output as additional input for the following element [21]. RNNs are widely employed in the field of cyber security since the auto-encoder approach is one of the most popular among researchers for detecting malware, and RNNs are good at detecting information security concerns.

3.1.3. Convolution neural network

It is, as previously mentioned, a neural network designed to process information stored in arrays. A two-dimensional array of pixels, for example, is a color or grayscale image. These are frequently used to process 2D and 3D picture arrays, as well as audio spectrograms. Their use of 1D arrays is less prevalent but expanding. The operation of the convolutional and pooling layers allows the DNN network to gain additional spatial information. As a result, it achieves remarkable results in picture applications and has wide-ranging applications in this arena. [21].

3.2. Generative / Unsupervised NN Models:

A Generative Model learns the models by the actual distribution of data using joint probability distribution p(x, y). The model describes the distribution of data and predicts the conditional probability with the help of the Bayes Theorem.

3.2.1. Deep belief network

In the proposed model, researchers used DBN to improve the accuracy of the classifier. Here the dataset is preprocessed using a normal distribution technique. DBN is designed as a stochastic neural network to extract data that is linearly separable. It is observed that in DBN with traditional machine learning, One class Support Vector Machine (OCSVM) has achieved higher accuracy compared to standalone shallow machine learning.

Restricted Boltzmann Machine

RBMs are used to detect security threats and are one of the most common methods in deep learning algorithms due to their simplicity and ease of implementation [23]. It is an unsupervised algorithm that helps to train one layer at a time. RBMs are stacked to form multiple layers, known as stacked RBMs to improve the accuracy of the system. Generally, DBN based on several stacked RBMs [22] are used in attack detection mechanisms. H. Wang proposed a deep belief network framework to detect the injection of false data into the network. It was found to be an effective detection mechanism irrespective of grid topology, environmental, and other operational conditions.

3.2.2. Deep Auto-Encoders

Deep Auto-encoders are used as a feature selection technique for network anomaly intrusion detection and malware classification [25]. M.A. Ferrag, L. Maglaras and S. Moschoyiannis[9] presented the comparative study of various unsupervised algorithms of deep learning in detecting various attack types. Among these generative models, the performance of auto encoders shows the highest detection rate for attacks such as Brute Force, DoS attacks, and infiltration. Deep auto encoders have achieved high accuracy of 97% with different hidden nodes and learning rates.

4. The proposed approach for wireless sensor network security

The wireless sensor network is an extended version of the wireless network. This network is a peer-to-peer ad hoc network. The major components of the Wireless sensor network are the Sensing Unit, Processing Unit, Communication Unit, and Power Unit [24,26]. The various techniques used to overcome the attacks are presented in this section. Previous research has categorized the security aspect into two levels: Node Level aspects and Network Level aspects [27, 28].

4.1. Node level Aspects

How can a node be secured? The previous research only talked about cryptography to provide node security. The cryptography can be either done by hardware filter or kernel-based cryptography can be implemented. But it is applied to maintain data confidentiality transmitted between the nodes. The main question here is how to predict the attack and how to be safe from attackers. The approach discussed here is entirely from a different angle. The node-level security can be classified into two type's reactive and proactive security models as shown in **Figure 3**.

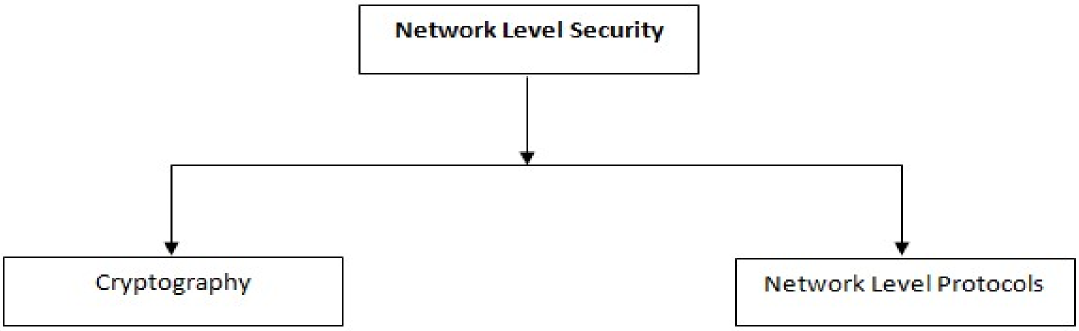

Figure 3: Node Level Security

4.1.1. Reactive Security Models

This approach will allow the attack to happen, and then find a solution to recover. By the time the attack may have fully destroyed the node and could start affecting the other nodes too. For example, in network spoofing, once the spoofing is done, the spoofed data has been accepted by the receiver. So, this reactive approach will not help to face the current situation.

4.1.2. Proactive Security models

The currently available reactive security models are used once the attack was detected in the system. The reactive system only works when the attack is done in the node. For the current scenario, we expect a system that will prevent the attack before it occurs. The proactive system will be feasible for the current scenario. The proactive system will scan all the packets and find whether the packet is malicious or no malicious before it enters the system [8]. One proposed model for the proactive intrusion detection system is introduced in **Figure 4**.

In the proposed proactive intrusion detection system, a data set is used for the classification of malicious and nonmalicious packets. A classifier is constructed based on the features of the packets. Once the packet enters the sensor node, the packet features are extracted and given as input to the classifier. The classifier will analyze the packet and identify whether the packet is malicious or not. Once the packet is finalized as a nonmalicious packet, it is accepted, else the packet is destroyed and creates an alert and intimate to the neighboring nodes. Machine learning concepts [10] are introduced to make the system even more efficient.

4.2. Network level Aspects

Wide scope of the attack is possible at the network level; the network is responsible to provide secured data transmission. Confidentiality, integrity, availability, and robustness are the major concerns at this level. The typical ways to provide the security goals are shown below in **Figure 5**.

4.2.1. Cryptography

Cryptography is used to achieve confidentiality security goals. Because the sensor nodes have limited computational capacity and memory, standard encryption algorithms are ineffective. In the sensor nodes, a modified version of the cryptographic algorithms is used. Symmetric and asymmetric cryptography are the two primary forms of encryption.

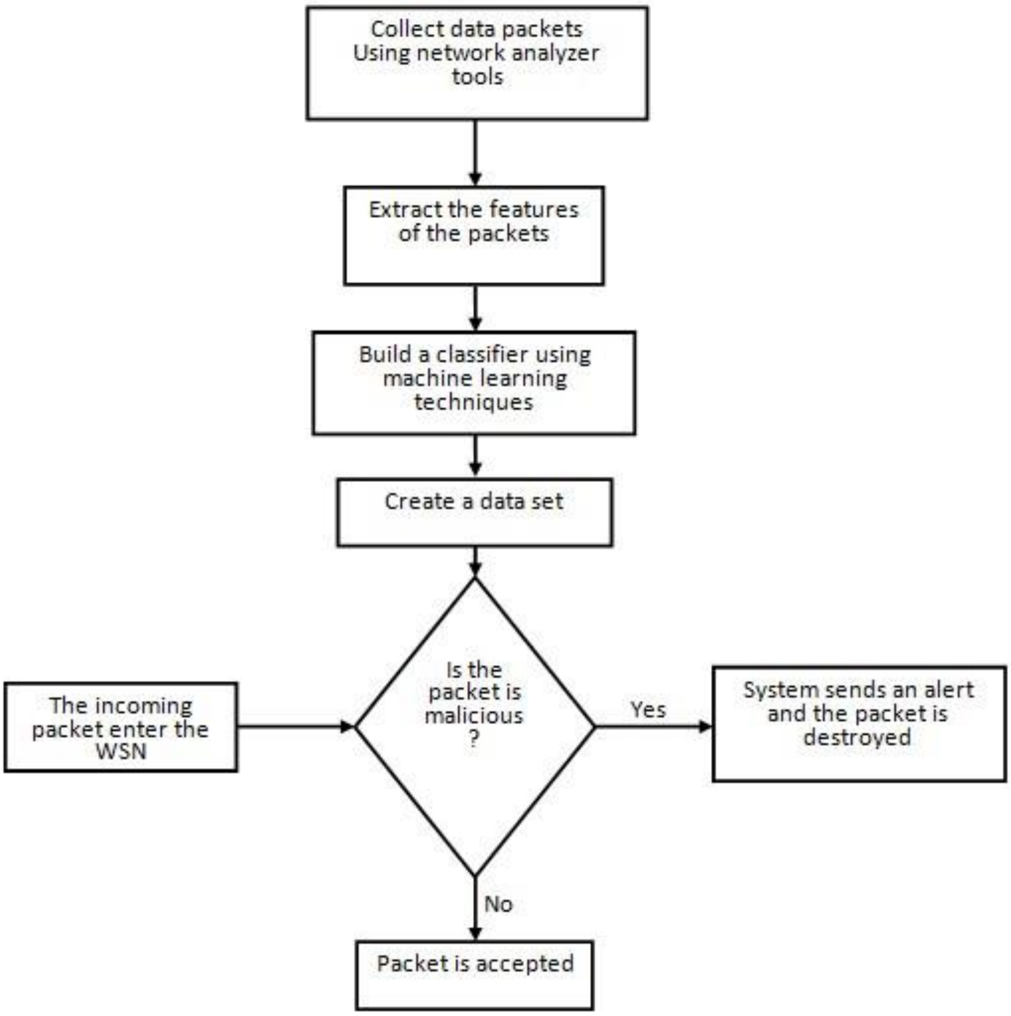
Collect data packets Using network analyzer tools
Extract the features of the packets
Build a classifier using machine learning techniques
Create a data set
The incoming packet enter the WSN
Is the packet is malicious ?
Yes
System sends an alert and the packet is destroyed
No
Packet is accepted

Figure 4: Proactive Security Model

The same key is used for encryption and decryption in symmetric key cryptography. Symmetric encryption is ineffective in the case of the WSN because the key can be easily stolen by a man-in-the-middle attack. Examples of the secured and efficient symmetric key encryption algorithms are AES, DES etc., The symmetric algorithms are more efficient in computation and in energy as compared to the asymmetric key algorithms.

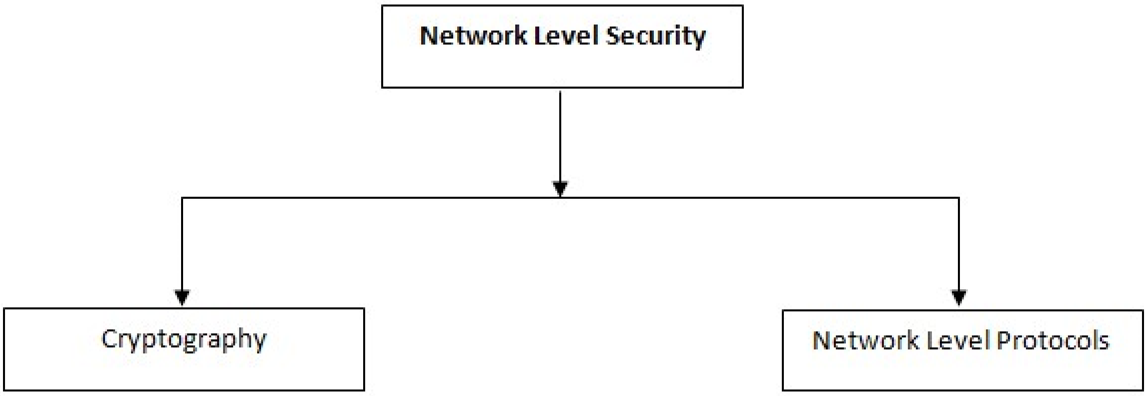

Figure 5: Network Level Securities

Two distinct keys are used in asymmetric key cryptography. Encryption is done with the public key, while decryption is done with the private key. This method consumes more energy and is so costly because of the generation of two different keys. It utilizes the bandwidth to share the public key between the nodes [29]. A popular public-key cryptosystem for safe data transmission is RSA. Which is also among the oldest? The surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly published the algorithm in 1977, are the origin of the abbreviation "RSA". A method of public-key encryption known as elliptic-curve cryptography (ECC) was built on the algebraic structure of elliptic curves with finite fields. Compared to non-EC cryptography, ECC enables fewer keys to give equal security. The comparison between RSA and ECC [29] is provided below in **Table 1**

Table 1: The comparison between RSA and ECC

Algorithm	Key Size	Specifications
RSA-1024	1024 bit keys	Offer equal security for smaller key size
ECC-160	160 bit keys	
RSA-2048	2048 bit keys	New minimum key size, both are equivalent
ECC-224	224 bit keys	

The basic advantages of ECC are smaller key size, low power consumption, low memory usage, and benefits over its competitors.

4.2.1.1. Proposed Algorithm

The primary aim of the proposed algorithm is to provide high security of data transmission in WSN. The proposed algorithm provides confidentiality and integrity. The confidentiality is provided by ECC, and the integrity is provided by the hashing methods and the digital signature. As a part of confidentiality, it has been proved in [29] that ECC with Koblitz encoding enhances security.

ECC with Koblitz's encoding

Encoding an Elliptical Curve (EC), described by a, b and p, is chosen. The (ASCII) values of all the messages need to be mapped with EC. The ASCII value is considered as the x coordinate for the point, (x, y) on the EC. The corresponding y coordinate is obtained by substituting the value of x in the given equation

$$(y^2)\ \mathrm{mod}\ p=(x^3+ax+b)\ \mathrm{mod}\ p \text{ ------------------------------ } (1)$$

For every x, xÎ {0, 1, (p-1}, there need not necessarily exist a corresponding y value, which is the major problem of ECC. Koblitz's encoding method brings the solution forthe problem by extending the range of x values, which enables the encryption of the entire message set in EC. In Koblitz's method, for a message character, m, its x value is computed by,

$$x = (m*k) + 1 \text{ --- } (2)$$

Where, k is an auxiliary base parameter.

This computed x value is substituted in **(1).** For this x, if the corresponding y point exists, then the (x, y) is the encoding point of the message on the EC. Else, iteratively identify the value y by varying x from

$$X= [(m*k) + 2] \text{ to } [(m*k) + (k-1)] \text{ ---------------------------------- } (3)$$

Even after substituting x = **(3),** if there does not exist a y value, then the value of **k** is incremented by 1. The highest value of **k** is concluded as the auxiliary parameter for the entire message set. At the receiver side, the decryption of the received cipher point results in a message point on the EC. By taking the x- coordinate of this message point, (x-1)/k is calculated. The quotient of this divisionoperation corresponds to the ASCII value of the message, m. Decoding takes a smaller number of computations than encoding. In[32], the researcher specified that the number of modulo operations required for the Koblitz's encoding is about 35 percent less than that of the ECC encryption.

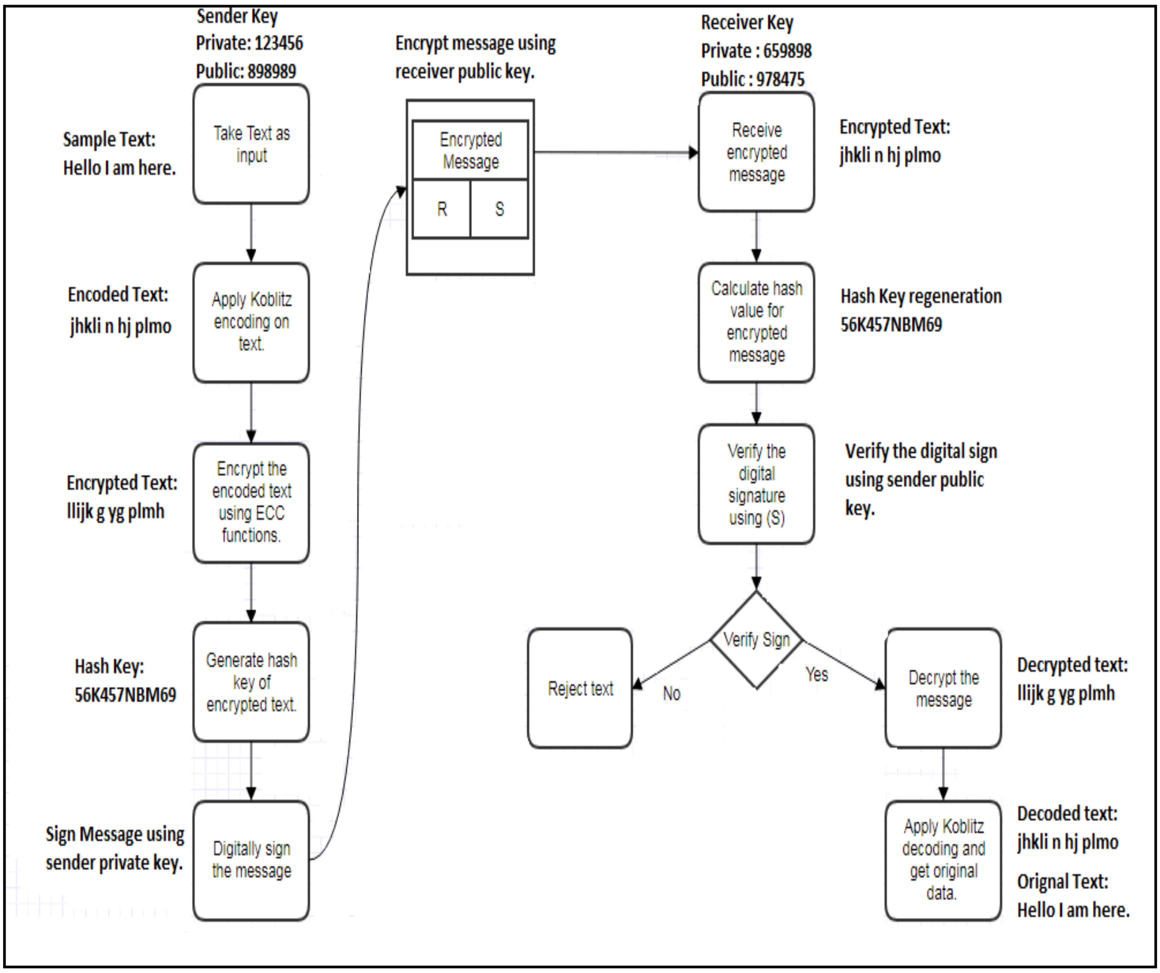

Figure 6: Proposed Cryptographic Method

MD 5 hashing function can be used in the proposed algorithm, which is depicted in **Figure 6.** Since it is one of the fastest hashing methods, the security gap in this MD5 will be covered by the other modules of the proposed algorithm. The encoded message from the Koblitz's encoder module is encrypted using the ECC algorithm, then a hash is generated using MD5 and is digitally signed to make the message more secure. The reverse operation is done in the receiver side.

4.2.1.2. Network Level Protocols

Network level protocols play a key role in the security aspect of the WSN. The protocols are subdivided into two categories such as security in stationery and in mobile node as depicted in **Figure 7.** The various protocols [30-35] are explained in detail.

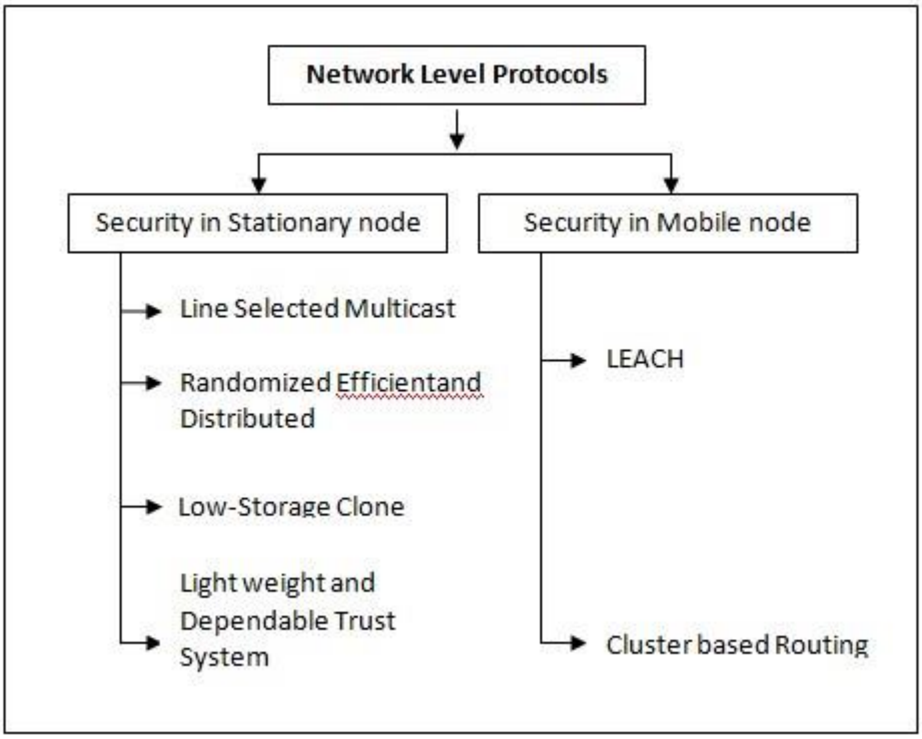

Figure 7 : Classifications of Network Level Protocols

5. Implementations and result discussion

The proposed Elliptic Curve Cryptography with Koblitz encoding method was implemented on the Ubuntu Linux operating system (64-bit) with an Intel Core i5-6200U CPU @ 2.40 GHz and 8.00 GB RAM. A Java Pairing-Based Cryptography library (JPBC) v.2.0.0 was used in this system to execute ECC algorithm and Koblitz encoding. Also, it helps the entities to communicate with each other.

Using Java libraries (java.security and java.security.spec), communication among the entities was measured. Furthermore, the communication was secured via Secure Socket Layer Framework. The parameters, such as Koblitz encoding time, ECC key generation time, encryption time, Koblitz decoding time, file decryption time, and security overhead were measured to evaluate the performance of the proposed scheme in a proactive network forensic environment.

5.1. Computation time of Koblitz encoding and decoding

The time taken to perform Koblitz encoding on the input data blocks of various size was measured and is shown in Table 2. The size of the data blocks were, 1024KB, 2048KB, 3072KB and 4096KB.

Table 2: Computation time of Koblitz encoding and decoding

S. No	Size of the data block	Computation time to perform Koblitz encoding (Seconds)	Computation time to perform Koblitz decoding (Seconds)
1	1024	0.056	0.001
2	2048	0.089	0.002
3	3072	0.132	0.003
4	4096	0.156	0.004

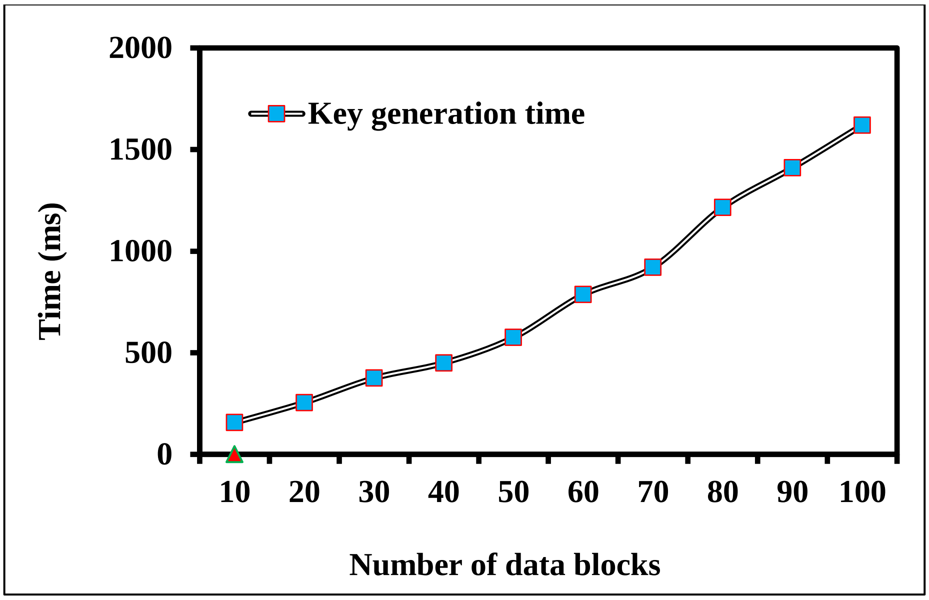

Figure 8: Time taken to generate keys of proposed ECC method

5.2. Timetaken to generate keys of the proposed ECC method

The time taken to generate the keys of the ECC algorithm was measured. The key generation time in this system was calculated for the set of 10 data blocks to 100 data blocks at the time interval of 10 units. Figure 8 shows that the key generation time rises with the rise of the number data blocks as expected. The analysis of the time consumption on key generation reveals that the rise in time consumption is not equivalently proportional to the growth of data blocks. The time taken to generate keys for the ECC algorithm is compared with the existing scheme in Table 3.

5.3. Time taken to encrypt and decrypt the data block using the ECC algorithm

Figure 9 shows the time taken to encrypt and decrypt the data block using ECC. The time taken to encrypt the data block by the user was measured. The file encryption time, the file decryption time, and the key computation time were considered to estimate the computational overhead in the file upload and download process. Both encryption and decryption times were estimated with different file sizes from 0.1 MB to 500 MB.

Table 3: Comparison of proposed model with the existing models

Number of Users	Methodologies (Time in Seconds)				
	CL-PRE (Xu et al. 2012)	Certificateless encryption (Seo et al. 2014)	PRE (Khan et al. 2014)	AES (Ali et al. 2017)	Proposed ECC
10	1.494	1.594	1.534	0.004	0.00212
20	1.598	1.741	1.606	0.00425	0.00235
30	1.673	2.321	1.684	0.00476	0.00286
40	1.791	1.888	1.799	0.005	0.00302
50	1.907	1.952	1.866	0.00512	0.00328
60	1.954	2.193	1.923	0.0055	0.0035
70	1.994	2.286	2.034	0.00598	0.00398
80	2.092	2.694	2.129	0.00632	0.00427
90	2.401	2.827	2.388	0.00664	0.00463
100	2.495	2.887	2.545	0.00697	0.00499

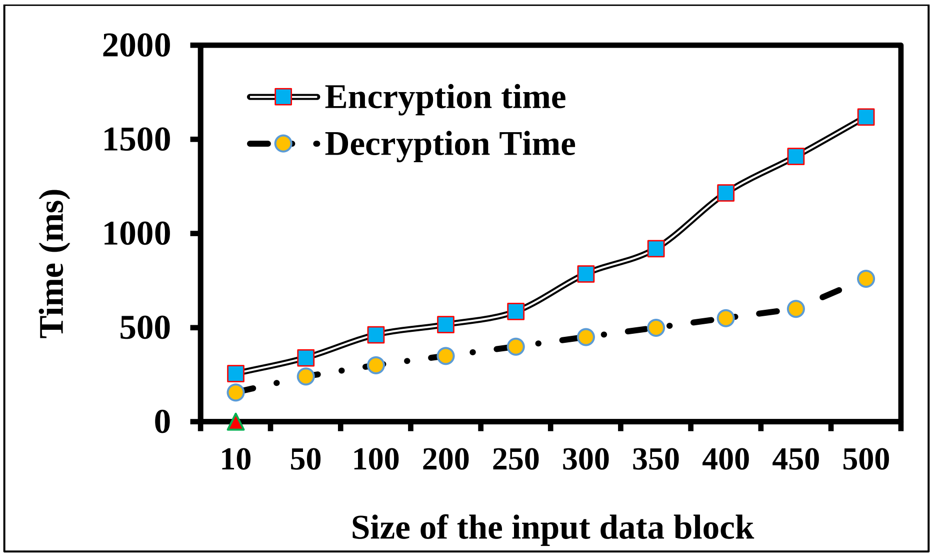

Figure 9: Time taken to encrypt and decrypt the data block using ECC algorithm

6. Conclusion

A cyber-attack is a harmful act that targets a person or an organization knowingly to break the security system. Cyber-attacks of various kinds are occurring in several industries. The security aspects of WSN are highlighted in this paper. Any company's employee must be knowledgeable of the most recent technological trends if it is to be protected against cyber-attacks.

The application of machine learning is a significant component. As this paper explained, it is commonly recognized that machine learning today plays a crucial role in the advancement of many fields, including Cyber Security. Machine learning and deep learning techniques are used in WSN to detect cyber-attacks. The suggested methodology of cyber-attack detection using machine learning and deep learning techniques yields the Node level security of WSN. Artificial intelligence can be incorporated into the suggested methodology to detect and drop attack packets that attempt to reach the WSN, thus preventing a cyber-attack.

A cryptographic technique enables network-level security, and Koblitz encoding with ECC is suggested to offer better security. Comparing the suggested encryption method to the current system, the new method produces better results. With the suggested methodology, security at the node and network levels is achieved in terms of Confidentiality and Integrity.

References

[1] H. S. Lallie, K. Debattista, en J. Bal, "A review of attack graph and attack tree visual syntax in cyber security", *Comput. Sci. Rev.*, vol 35, no 100219, bl 100219, Feb 2020.

[2] S. Chen, Z. Wu, en P. D. Christofides, "Cyber-attack detection and resilient operation of nonlinear processes under economic model predictive control", *Comput. Chem. Eng.*, vol 136, no 106806, bl 106806, Mei 2020.

[3] M.RiahiManeshen N. Kaabouch, "Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions", *Comput. Secur.*, vol 85, bll 386–401, Aug 2019.

[4] M. Z. Gunduzen R. Das, "Cyber-security on smart grid: Threats and potential solutions", *Comput. netw.*, vol 169, no 107094, bl 107094, Mrt 2020.

[5] Priya R. L., Lifna C. S., D. Jagli, en A. Joy, "Rational unified treatment for web application vulnerability assessment", in 2014 *International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), Mumbai, Maharashtra, India*, 2014.

[6] N.&. Nageswaran, &. Seshan, en V. S. Sriram, SCO-RNN: A Behavioral based Intrusion Detection approach for Cyber Physical Attacks in SCADA Systems. 2019.

[7] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, en H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study", *J. Inf. Secur. Appl.*, vol 50, no 102419, bl 102419, Feb 2020.

[8] A.Sivaprasad, "Secured proactive network forensic framework", in 2017 *International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, India*, 2017.

[9] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, en H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study", *J. Inf. Secur. Appl.*, vol 50, no 102419, bl 102419, Feb 2020.

[10] R. Coulter, Q.-L. Han, L. Pan, J. Zhang, en Y. Xiang, "Code analysis for intelligent cyber systems: A data-driven approach", *Inf. Sci.* (Ny), vol 524, bll 46–58, Jul 2020.

[11] D. Wang, X. Wang, Y. Zhang, en L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning", *J. Inf. Secur. Appl.*, vol 46, bll 42–52, Jun 2019.

[12] Á. M. Guerrero-Higueras, N. DeCastro-García, en V. Matellán, "Detection of Cyber-attacks to indoor real time localization systems for autonomous robots", *Rob. Auton. Syst.*, vol 99, bll 75–83, Jan 2018.

[13] M. Shafiq, Z. Tian, Y. Sun, X. Du, en M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city", *Future Gener. Comput. Syst.*, vol 107, bll 433–442, Jun 2020.

[14] S. Agarwal, A. Tyagi, en G. Usha, "A deep neural network strategy to distinguish and avoid cyber-attacks", in *Advances in Intelligent Systems and Computing, Singapore: Springer Singapore*, 2020, bll 673–681.

[15] H. Malhotra, M. Dave, en T. Lamba, "Security analysis of cyber attacks using machine learning algorithms in eGovernance projects", in *Futuristic Trends in Networks and Computing Technologies, Singapore: Springer Singapore*, 2020, bll 662–672.

[16] M.Kalech, "Cyber-attack detection in SCADA systems using temporal pattern recognition techniques", *Comput. Secur.*, vol 84, bll 225–238, Jul 2019.

[17] M.Swarnkaren N. Hubballi, "OCPAD: One class Naive Bayes classifier for payload based anomaly detection", *Expert Syst. Appl.*, vol 64, bll 330–339, Des 2016.

[18] G. E. Dahl, J. W. Stokes, L. Deng, en D. Yu, "Large-scale malware classification using random projections and neural networks", in 2013 *IEEE International Conference on Acoustics, Speech and Signal Processing, Vancouver, BC, Canada*, 2013.

[19] P. Raghu Vamsi en A. Chauhan, “A hybrid model for detecting anomalous ozone values”, in *Futuristic Trends in Networks and Computing Technologies, Singapore: Springer Singapore,* 2020, bll 419–430.

[20] M. I. Tariq et al., “A review of Deep Learning security and privacy defensive techniques”, *Mob. Inf. Syst.*, vol 2020, bll 1–18, Apr 2020.

[21] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, en G. Cao, “Deep learning aided interval state prediction for improving cyber security in energy internet”, *Energy* (Oxf.), vol 174, bll 1292–1304, Mei 2019.

[22] M.Yousefi-Azar, V. Varadharajan, L. Hamey, en U. Tupakula, “Autoencoder-based feature learning for cyber security applications”, in 2017 *International Joint Conference on Neural Networks (IJCNN), Anchorage, AK, USA*, 2017.

[23] A.Gawareen S. B. Dhonde, “A survey on security attacks in wireless sensor networks”, in *3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi*, 2016, bll 536–539.

[24] W. Du, R. Wang, en P. Ning, “An efficient scheme for authenticating public keys in sensor networks”, in Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing - MobiHoc ’05, Urbana-Champaign, IL, USA, 2005.

[25] J. Goodman en A. P. Chandrakasan, “An energy-efficient reconfigurable public-key cryptography processor”, *IEEE J. Solid-State Circuits*, vol 36, no 11, pp. 1808–1820, 2001.

[26] Abirami, S. (2019). A Complete Study on the Security Aspects of Wireless Sensor Networks. In: Bhattacharyya, S., Hassanien, A., Gupta, D., Khanna, A., Pan, I. (eds) *International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems*, vol 55. Springer, Singapore. https://doi.org/10.1007/978-981-13-2324-9_22

[27] L. Tan, S. Zhang, Y. Sun, en J. Qi, “Application of wireless sensor networks in energy automation”, in 2009 *International Conference on Sustainable Power Generation and Supply, Nanjing,* 2009.

[28] A. Rani en S. Kumar, “A survey of security in wireless sensor networks”, in 2017 3rd *International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, India,* 2017.

[29] P. N. V. Ravi Kishore Kodali1, Red, “ECC Implementation Using Koblitz’s Encoding”, in *Proc. Int. Conf. On Communication Engineering and Network Technologies, Warangal: ELSEVIER*, 2012.

[30] V.D.Gligor (2006), “Emergent Properties in Ad-Hoc Networks: A Security Perspective,” *Proc. ACM Symp. Information, Computer------- LSM And Comm. Security* (ASIACCS ’06), P. 1, 2006.

[31] Mauro Conti Et Al (2011), “Distributed Detection of Clone Attacks in Wireless Sensor Networks,IEEE Transactions On Dependable And Secure Communication, vol.8,no. 5, September/October .

[32] M.Dong (2016), “LSCD:A Low Storage Clone Detection Protocol for Cyber Physical Systems”, *IEEE Transactions on Computer Aided Design of Integrated Circuits And Systems,*vol.35, no.5,May.

[33] Xiaoyong Li (2016), “LDTS:A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks”, *IEEE Transactions on Information Forensics and Security*, vol.8, no.6 June.

[34] W.Heinzelman, A. Chandrakasan And H. Balakrishnan (2000), "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," *Presented atThe 33rd Hawaii Int. Conf. On System Sciences* (HICSS ‘00), January.

[35] Samer A. B. Awwad, Chee Kyun Ng, Nor K. Noordin,Mohd. Fadlee A. Rasid , *Cluster Based Routing Protocol for Mobile Nodes in Wireless Sensor Network, © Springer Science+Business Media, LLC,* 2010.