International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 13, No.1 (Jan-2023)

http://dx.doi.org/10.12785/ijcds/130110

Detecting Network Traffic-based Attacks Using ANNs

Sanad Malaysha[1], Mohammed Moreb[1] and Ali Zolait[2]

[1] *Computer Science Department, Birzeit University, Ramallah, Palestine*
[2]*College of Information Technology, University of Bahrain, Bahrain*

Received 28 Oct. 2021, Revised 15 Dec. 2022, Accepted 12 Jan. 2023, Published 31 Jan. 2023

Abstract: Nowadays, data security is a significant challenge for computer networks, especially on internet-based systems and the internet of things (IoT). Many possible network attacks and intrusions need to stop and treat, but the first step is to stop the attack to discover it and understand its type. More specifically, active ones such as Denial of Service (DOS), Masquerade, Replays, Penetration, Placement, and unauthorized access. An attractive and practical field to satisfy attack detection and prediction is Machine Learning (ML), which has techniques such as Artificial Neural Networks (ANNs) that take the data transmission request vectors and rely on them to classify the attacks. ANNs have many structure options so selected the most appropriate structure for the article context: the Feed-Forward Back-Propagation structure. Hence, introducing the ANN technique and applying it to an international dataset will discover how the experimental results would prove a significant acceptable accuracy of attack detection. Moreover, the article margin discussed two of the standard techniques for fighting the attacks to give recommendations for best practices, which are the Digital Signature and the Cryptography functions, these methods that can decrease and harden the attacks, then the role of the ML techniques would be more specific and determined..

Keywords: Security Attack, Artificial Neural Networks, Machine Learning, Digital Signature, Cryptography.

1. Introduction and Overview

The increasing expansion in the computer network systems and, on the top, the internet has grown the risk of information security for the transmitted and requested data over the networks, which led to a massive number of network attacks and intrusions in different ways and for many reasons [1]. Educational environments are facing many challenges [2] on Internet protection, and there's an increase in cyber-attacks, it is a need to focus on the protection of educational environments and ensure that they have a good security infrastructure. Some time for the entertainment of the hackers, other times for financial wise, and more could be security, curiosity, or lousy competition. Those attacks will lead to breaking the security of the data and this means loss or forgery that could affect human lives or losing tons of dollars, which may spoil even a country or corporation or on the small level business. Many types of attacks over the network and the internet could be from outside or inside the targeted system, such as DoS [3], phishing attacks, malware attacks, password attacks, spy attacks, spacious attacks, and many other web attacks to mention [3]. ML techniques helped the machine have learning, prediction, and classification skill, there are many ML algorithms that can be used for classification identified in [4]. It could apply to the network data to train the algorithms and let them detect and classify in case any data vectors have an attack pattern. Moreover, many types and techniques for ML can be classified as shown in Figure 1. Mainly supervised learning [4], semi-supervised learning, unsupervised learning, reinforcement learning, and finally, Deep Learning (DL) [1] [3] [5] [4]. The research is interested in the supervised learning track, where input and goal mapping are available in the international dataset, combining the considered attribute of the network attack with the request status, to decide if there is normal use or a real attack. The most common and effective techniques in the ML for the prediction are ANNs [5] [6] [4], and though will use the network data to train, test, and evaluate the different structures for the ANNs until reaching the most accurate output for detecting and classifying the malicious records in the network transmitted data. Moreover, below introduces some of the related works that utilize the ML techniques to detect and classify network attacks and intrusions.

A. Artificial Neural Networks ANNs

It is ML technique that mimics the human brain's works, so it is represented per the illustrated structure in Figure 2. As inputs vectors are summated and processed at transformation function in the artificial neuron, then its output moves to the next level of neurons, which is very similar to the last concept of trying to understand the brain's actual neural network work [1]. So below will brief some of the ANNs applications for detecting and

E-mail address: sanad.ahmed2000@gmail.com, Dr.moreb.mohammad@gmail.com, azolait@uob.edu.bh

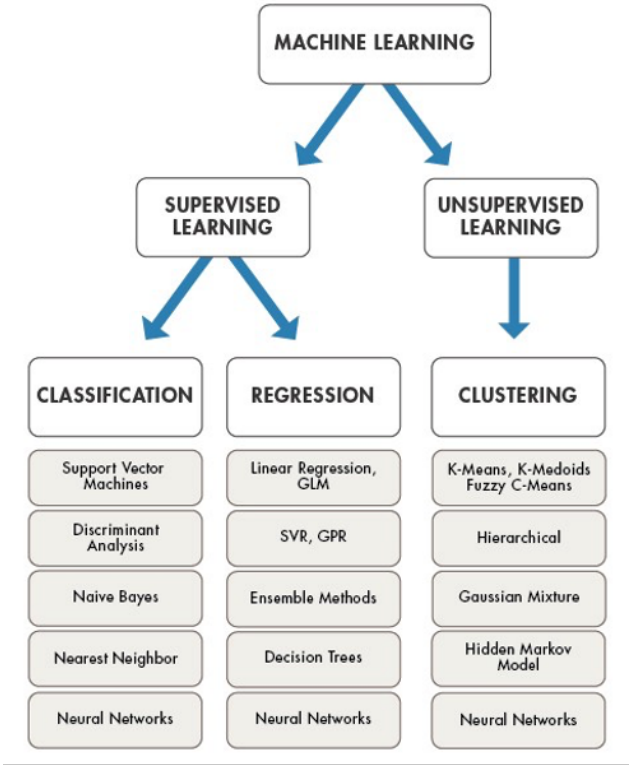

Figure 1. Machine Learning Types

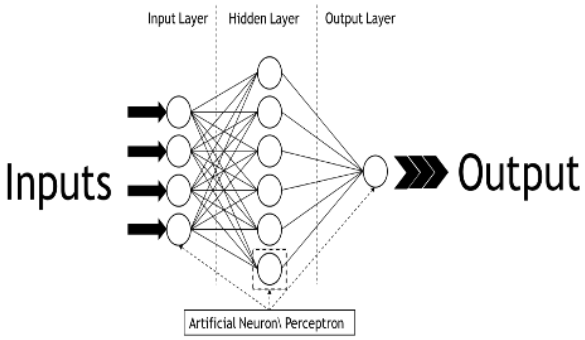

Figure 2. Artificial Neural Model

predicting the different network-based and internet security attack. For example, Output = Sigmoid ((Input X Weight). It represents the summation of the multiplication of each input value Ii with its corresponding weight Wj. A. Bivens et al. [1] introduced a ML method for intrusion detection based on network traffic data, for the classification used the self-organizing map (SOM) and the ANNs Multi-Layer Perceptron MLP for the detection because the attacks have different labels (ways) for the detection. Also, M. Moradi et al. [3] utilized the ANNs Multi-Layer Perceptron MLP in offline analysis for multiclass network data records. After trying various structures, it reached an accuracy of around 90% of detection.

A feed-forward ANNs Multi-Layer Perceptron MLP with a back propagation-training algorithm applied to computer network traffic for internet-based intrusion detection. This Multi-Layer was exercised by J. Shum et al. [5], with around 80% correct classification in the experimental results. Moreover, O. Al-Jarrah et al. [6] used the Time Delay Neural Network (TDNN) version of the ANNs to increase the rate of recognition in the network attacks from the host sweep or port scan shows the requested services to analyze the unauthorized and unwanted access. More options for utilizing ML and more exactly in the ANNs done in [7], where they utilized the recurrent version of the ANNs in the network intrusions and attack detection. They have introduced another version of the commonly known Intrusion Detection Systems (IDS), especially the ones built for the networks for the increasingly high connectivity services over the internet and the intranets. J. Skaruz et al. [8] worked on the specific version of the attack detection, which is the SQL attacks, by using Jordan and Elman networks in the recurrent ANNs that is RNN. They divided the SQL requests into tokens and let the model predict the next token to differentiate between the normal and attacker queries. It proved acceptable performance where Elam outperformed Jordan network. In research conducted by Maleh et al. [9], researchers focused on the Wireless Sensor Networks WSNs, such as the attack on the air transmission level. They composed a lightweight Intrusion Detection System IDS from the Support Vector Machine (SVM) algorithm with additional support from signature rules set to predict the attack behavior. The model simulation results showed a successful detection rate for malicious events. DL is practiced in [10] by using the Deep neural network (DNN) as a comparison with the SVM in intrusion detection, that is, for identifying and preventing the attacks for securing the data in the network systems. The detection in their study supported by the level of classification of either the attack from inside or outside the network system, and categorized attacks into mainly four types which are DOS, Probing, Unauthorized access to the root user privileges (U2R), and Unauthorized access from a remote machine (R2L). In addition, the outputs proved 99% as the expected results. Moreover, F. Jiang et al. [11] introduced a novel method in information security and, more specifically, attack detection; they utilized the ML techniques using the ANNs. It used the hydride of multichannel and RNNs of long short-term memory. The model Fig2. Artificial Neural s applied on a collected dataset simulating the behavior of the system user as data vectors, so both training, testing, and evaluation phases run on the vectors to assure the quality and accuracy, which reached 98.9% accurate outputs. Additionally, Smys [12] research worked on a specific common network attack: the Distributed Denial of Service (DDOS), especially in telecommunication networks. Therefore, the authors used a combination of the ANNs and the SVM to accurately and efficiently identify and classify the DDOS attacks. The DDOS could have several volumes-based, protocol-based, and application-based classes. However, their works proved acceptable results similar to the previous ones

because the ML methods are adaptive to the changeable attack format, proving promising results for automating the detection and treatment. More combined techniques are done in [13], where they integrated the Correlation-based Feature Selection CFS and ANNs for detecting the attacks specifically. Since they targeted the detailed classification for the types though that led to an accuracy of 96.44%. They used the same dataset applied in this article. Their targeted attack types were probe, DoS, U2R, and R2L. The efforts done in [14] even used the convolutional neural networks CNNs, where it applied to the networks traffic as if it were a two-dimensional image to detect any attack. It's a novel idea but still didn't outperform the other reviewed techniques and our proposed method, as the CNNs achieved 95.90% of detection accuracy. Table 1 briefly summarizes the introduced related works in section 1 where they are explained well, here it gives a quick review to have a clear idea about each used technique and with the highest accuracy it reached, those ten articles used the major ML methods for the same goal of this paper. The primary goal of all these efforts is to utilize the best technique that fits the attack's detection case with minimal error.

B. Security Techniques

As introduced, researchers will briefly describe two recommended techniques that harden and reduce security attacks. Then, the Digital Signature [15] and Cryptography Functions [16] were selected to be introduced in the following sections for their effective results in fighting the attacks. Finally, researchers will compare the different techniques of the mentioned two concepts and recommend the best per the general reviews. Most of the cyber-crimes are attacks using malicious URLs [2] designed by attackers to fool the users and steal their sensitive information or effect resources, result [2] shows how digital signature can be used to detect the malicious URLs as the first level, for advance users they can use ML ANNs to detect maliciously URLs effectively.

C. Digital Signature to Reduce Intrusions

The ML would help detect the network intrusion and treat it in the right way regardless of the source or the class, while the best if it can prevent the intrusion from occurring in the system. Digital signatures [15] [2] is another form of the cryptography system that could help at least to decrease the attacks by increasing the security using the verification of the correctness and originality of the transmitted data over the network system. The digital signature will use the sender's private key to sign the message and then send both. The receiver side will use the sender's public key to verify the signature and the message to assure the safety and security of the message [16]. This concept, the digital signature, could have multiple techniques and schemes for implementing it. This research mentioned a few of the forms in Table 2, with a few suggestions for improvements.

TABLE II. Selected Digital Signature Schemes Review

Scheme	Algorithm	Weaknesses
ElGamal [15]	x: user private key y: user public key m: message p: large prime number k: 0 ¡= k ¡= p-1, gcd(k,p-1)=1 α: primitive element r= α^{k} mod p $\alpha^{m}= \alpha^{xr}\ \alpha^{ks}$ mod p	To keep changing r if m is already similar sent message, and to change m with additional digits if same already sent with notifying the addition size in the message
Elliptic [17]	Q=2^m Fq: finite fields seed E: <= 160 bit string a and b: define Elliptic equ. (xG,yG): finite point P: point of prime order d (private key): 0¡=d¡=n-1 Q(Public key)=dP Signature generation Signature Verification	The used equation for the curve better to be more complex than $y^2 = x^3 + ax + b$
Schnorr [18]	p, q: prime numbers GCD(q, p-1) =/ 1 a^{q} mod p = 1 s(private): <q v(public) = a^{-s} mod p Signature generation Signature Verification	It uses the exponentiation and Euclidean as mathematical signing and verification which requires long computing time and that need to optimize by changing to better performance wise such as modulo
DSA [19]	y: public key x: secret key r(public)= (g^{k} mod p) mod q k: secret value s=k^{-1} (H(m)+xr) mod q signature (r, s)	One of the weaknesses is using the same private key all the time as the algorithm is not changing or recalculating them, that makes it possible to predict them, thought better to add a recalculation criteria by depending on random generated numbers

D. Cryptography Hashing For Securing the Messaging

In order to guarantee the availability and security of the transmitted data over the computer networks and internet, there is a need for cryptography and encrypting data to protect it while transmitting and storage. In addition, the hashing helps in reducing the transmitted data, which enhances the performance of message delivery between the different endpoints across the communicators [16]. Using ML techniques can help detect the attacks, but avoiding the attack is more efficient than detecting it; therefore, the hashing is a phase to protect the data by minimizing and hardening the attacks. This technique makes it harder to analyze the data and injects the poison [20].], a set of algorithms [21] that are considered suitable for work in the IOT environment called lightweight algorithms, the simulation results showed that the algorithms provide significant security over several rounds of cryptography. Data integrity

TABLE I. The Attacks Detection Accuracy Resulted in the Summarized Efforts

Methodology	Accuracy
Self-Organizing Map SOM and the Artificial Neural Networks ANNs [1]	91%
Artificial Neural Networks ANNs Multi-Layer Perception MLP [3]	90%
Feed-Forward Artificial Neural Networks ANNs Multi Layer Perception MLP [5]	80%
Recurrent Neural Networks RNNs [7]	98%
Support Vector Machine SVM [9]	97%
Deep Neural Networks DNN [10]	99%
Recurrent Neural Networks RNN Long Short-Term Memory LSTM [11]	98.9%
Artificial Neural Networks ANNs and Support Vector Machine SVM [12]	90%
Correlation-based Feature Selection CFS and ANNs [13]	96.44%
Convolutional Neural Networks CNN [14]	95.90%

is a critical point in data communication that can be fulfilled in the hash functions, which apply cryptography algorithms and criteria [22]. This study will traverse three of the most common crypto hash functions, such as Tiger hash function [23], SHA [24], and MD5 [25]. In addition to the recommendation for the most practical and efficient choice among the three, the Tiger [23].

1) Tiger

Hashing function digests 512-bit data message to produce a 192-bit hashed value, which will keep and assure the data security in a ciphered way. Support both 32-bit and 64-bit machines which makes it three times faster than SHA. It consists of two phases Key Schedule and State Transformation, where it goes through three rounds each use eight lookups to create a strong nonlinear avalanche, in addition to register operation for hardening the diffusion and attacks [18] [26]. The rounds block is calculated per the following [27]:

1) A, B, and C are words of the block. X is the message
2) C = C $\oplus$ X
3) A = A - even(C)
4) B = B + odd(C)
5) B = B $*$ (constant), constant $\in$ {5, 7, 9}
6) Round again

And though the values of A, B, and C shifted as cycle each round to be at first round moved to B, C, and A [27].

2) SHA [24]

A crypto hash function adopted mostly by the government after the industries especially in the digital signatures, also use in security protocols such as pseudorandom number generation, key agreement, and user authentication. It generate 160-bit hash for message of length less than 2^64, the input message digested into blocks of size 512-bit, and the following cycle goes for each block:

Initial Value IV = (A_0, B_0, C_0, D_0, E_0) = (0x67452301, 0xefcdab89, 0x98badcfe, 0x10325476, 0xc3d2e1f0)

TABLE III. NSL-KDD dataset records

Total Records	Normal	Attack
77,289	47,911	29,378

Divided into 16 words (M_0, $M_1 \ldots M_{15}$), each of size 32-bit

1) Each mi = ($M_{i-3} \oplus M_{i-8} \oplus M_{i-14} \oplus M_{i-16}$) $\gg$ 1.
2) Ai = (Ai−1 ¡¡5) + fi (Bi−1, Ci−1, Di−1) + Ei−1 + Mi−1 + Ki
3) Bi = Ai−1
4) $C_i = B_{i-1} \gg 30$
5) Di = Ci−1
6) Ei = Di−1

Then re-round again, but each round uses a different function and constant so it makes the attack and analysis harder [24]. The above-summarized SHA version SHA1, where there are many optimizations on this crypto function that leads to harder crack and collisions.

2. Methodology

A. NLS-KDD Dataset

For simulating the security attack classification and prediction using the ANNs, one of the common datasets called NSL-KDD for security attacks research purposes was divided into three parts: training 80%, validation 10%, and testing 10%. The NSL-KDD is a dataset created to study internet problems [28], including security intrusions and attacks. The original dataset size is explained below.

Moreover, the classification process for predicting an attack from normal ones covered three types of attacks:

- Denial of service
- Probing
- Unauthorized access

The dataset has 41 column inputs, all of them included in ANNs training and testing because the more increased

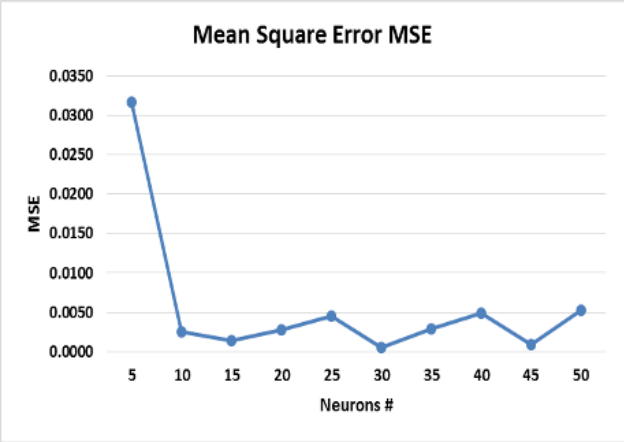

Figure 3. The MSE results behavior for trying a cumulative increment of five neurons until reach 50 neurons

the columns, the better the results since found all of them related to the attacks contexts, some of them are mentioned in the below list:

- Protocol type
- Service
- Source bytes
- Destination bytes
- Number of failed logins

B. *Proposed Method*

The ANNs selected structure is Tow-Layered Feed-Forward back-propagation with Levenberg-Marquardt training algorithm, Gradient Descent learning function, and the Hyperbolic Tangent Sigmoid as a transfer function, all the structure details are illustrated in Table 5. The experiment started with five neurons for the hidden layer and continued increasing five neurons every try until they reached 50 neurons. The Mean Square Error (MSE) is used as the performance evaluation function.

C. *Results*

As listed in Table 4 and illustrated in Figure Figure 3 the scenario with 30 neurons proved to have the least MSE "0.001", which shows the accuracy is almost 100% (99.9%) for detecting an attack from a normal user request.

In addition, the 45 neurons try has low MSE close to the 30 neurons case, but for sure, even if both are equal in performance, have to choose the one with the minimal computation and complexity for reducing resources, time, and cost consumption, which is the 30 neurons scenario. Table 4 explains how the probing among the MSE values, that's by trying increasingly neuron numbers and every three runs to have actual average MSE because there is a randomization possibility in the ANNs weights initialization

TABLE V. The selected ANNs structure layers and functions

ANN Property	Value
Type	Feed-Forward backpropagation
Training Function	Levenberg-Marquardt LM
Learning Function	Gradient Descent GD
Performance Function	Mean Square Error MSE
Transfer Function	Hyperbolic tangent sigmoid
Number of Layers	2

and selection. So this average view will give more accurate and fair comparisons. These results were reached by applying the proposed technique to the NSL-KDD dataset mentioned in 2.A section.

TABLE IV. The experiment MSE results as tabular values per the increment in the neurons

Try #	MSE1	MSE2	MSE3	MSE Average	Neurons#
1	0.0344	0.0311	0.0297	0.0317	5
2	0.00387	0.000555	0.00325	0.0026	10
3	0.00294	0.000915	0.00015	0.0013	15
4	0.00115	0.00404	0.00315	0.0028	20
5	0.0118	0.000173	0.00157	0.0045	25
6	0.000129	0.000785	0.00075	0.0006	30
7	0.00452	0.00143	0.00251	0.0028	35
8	0.00522	0.00371	0.00583	0.0049	40
9	0.000597	0.000004	0.00199	0.0009	45
10	0.00299	0.0073	0.00545	0.0052	50

There are many options for the ANNs, which can be used in this experiment or other experiments. Still, the utilized one in the article Tow-Layered Feed-Forward back-propagation proved the best results in the initial research and running of the experiment. Through continued to collect the results as the research's goal is to find a methodology for detecting the attack from the normal use network and internet requests with minimal close to zero errors, which is the optimal goal to have almost 100% accuracy of detection. So, our work achieves better results than the other reviewed works. The highest reviewed efforts are per done in [10] that achieved 99%, and also [11] that achieved 98.9%, where both used the ANNs. This article effort detects the attack regardless of the type, which makes it easier to cover and utilize more data, also needs less training because only high-level classification helps to stop the attack at first. Then the other studies can be applied to the result of this research, that's when it goes to the detailed detection of the attack type.

3. Conclusion

The network-based and internet-based systems are exponentially increasing, especially in cloud computing, IoT, and 5G. This certainly increases the network attacks and intrusions, as they become an attractive goal for the huge

amount of valuable data that is communicated over the networks. On the other side, the research and potential for defeating these attacks would require more effort and evolution to protect communication confidentiality, integrity, and availability. The ML is a promising field for fighting the network-based attack as it has the power to predict the attack from the normal use attack. This is shown in the introduced experiment that reached an accuracy of almost 100%, but the researchers believe that this result accuracy comes from utilizing only a specific dataset, NSL-KDD. Though for future works, it is recommended to utilize more datasets and try different structures of the ANNs to prove and evaluate the prediction abilities in varied possibilities, as the attacks methods also evolve, so the detection and defense methods must not stop evolving.

References

[1] A. Bivens, C. Palagiri, R. Smith, B. Szymanski, and M. Embrechts, "Network-based intrusion detection using neural networks,," *Intell. Eng. Syst. through Artif. Neural Networks*, vol. 12, no. 1, p. 579–584.

[2] Y. Salem, M. Moreb, and K. S. Rabayah, "Evaluation of information security awareness among palestinian learners," in *2021 International Conference on Information Technology (ICIT)*, July 2021, pp. 21–26.

[3] M. Moradi and M. Zulkernine, "A neural network based system for intrusion detection and classification of attacks,," in *Proceedings of the IEEE international conference on advances in intelligent systems-theory and applications*, p. 15–18.

[4] M. Moreb, T. A. Mohammed, and O. Bayat, "A novel software engineering approach toward using machine learning for improving the efficiency of health systems," *IEEE Access*, vol. 8, pp. 23 169–23 178, 2020.

[5] J. Shun and H. Malki, "Network intrusion detection system using neural networks,," in *2008 Fourth International Conference on Natural Computation*, vol. 5, p. 242–246.

[6] O. Al-Jarrah and A. Arafat, "Network intrusion detection system using neural network classification of attack behavior,," *J. Adv. Inf. Technol. Vol*, vol. 6, no. 1.

[7] J.-S. Xue, J.-Z. Sun, and X. Zhang, "Recurrent network in network intrusion detection system,," *Cybernetics (IEEE Cat*, vol. 4, no. 826, p. 2676–2679.

[8] J. Skaruz and F. Seredynski, "Recurrent neural networks towards detection of sql attacks,," in *2007 IEEE International Parallel and Distributed Processing Symposium*, p. 1–8.

[9] Y. Maleh, A. Ezzati, Y. Qasmaoui, and M. Mbida, "A global hybrid intrusion detection system for wireless sensor networks,," *Procedia Comput. Sci*, vol. 52, p. 1047–1052.

[10] S. Roy, A. Mallik, R. Gulati, M. Obaidat, and P. Krishna, "A deep learning based artificial neural network approach for intrusion detection,," in *International Conference on Mathematics and Computing*, p. 44–53.

[11] F. Jiang, "Deep learning based multi-channel intelligent attack detection for data security,," *IEEE Trans. Sustain. Comput*, vol. 5, no. 2, p. 204–212.

[12] S. Smys, "Ddos attack detection in telecommunication network using machine learning,," *J. Ubiquitous Comput. Commun. Technol*, vol. 1, no. 1, p. 33–44.

[13] I. Sumaiya Thaseen, J. Saira Banu, K. Lavanya, M. Rukunuddin Ghalib, and K. Abhishek, "An integrated intrusion detection system using correlation-based attribute selection and artificial neural network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, p. e4014, 2021.

[14] G. Andresini, A. Appice, and D. Malerba, "Nearest cluster-based intrusion detection through convolutional neural networks," *Knowledge-Based Systems*, vol. 216, p. 106798, 2021.

[15] E. Mohammed, A.-E. Emarah, and K. El-Shennaway, "A blind signature scheme based on elgamal signature,," in *Proceedings of the Seventeenth National Radio Science Conference. 17th*, NRSC'2000 (IEEE Cat. No. 00EX396, p. 25–1.

[16] M. Wang, M. Duan, and J. Zhu, "Research on the security criteria of hash functions in the blockchain,," in *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, p. 47–55.

[17] A. Khalique, K. Singh, and S. Sood, "Implementation of elliptic curve digital signature algorithm,," *Int. J. Comput. Appl*, vol. 2, no. 2, p. 21–27.

[18] M. Mesran, M. Syahrizal, and R. Rahim, "Enhanced security for data transaction with public key schnorr authentication and digital signature protocol,," *ARPN J. Eng. Appl. Sci*, vol. 13, no. 11, p. 3839–3846.

[19] D. Kravitz, "Digital signature algorithm."

[20] Y. Chen, Y. Wo, R. Xie, C. Wu, and G. Han, "Deep secure quantization: On secure biometric hashing against similarity-based attacks,," *Signal Processing*, vol. 154, p. 314–323.

[21] M. Shadeed and M. Moreb, "Lightweight encryption for multimedia in the internet of thing(iot)," in *2021 International Conference on Information Technology (ICIT)*, July 2021, pp. 27–32.

[22] X. Wang and H. Yu, "How to break md5 and other hash functions,," in *Annual international conference on the theory and applications of cryptographic techniques*, p. 19–35.

[23] R. Anderson and E. Biham, "Tiger: A fast new hash function,," in *International Workshop on Fast Software Encryption*, p. 89–97.

[24] X. Wang, Y. Yin, and H. Yu, ""finding collisions in the full sha-1," in annual international cryptology conference," p. 17–36.

[25] P. Gupta and S. Kumar, "A comparative analysis of sha and md5 algorithm,," *architecture*, vol. 1, p. 5.

[26] F. Mendel and V. Rijmen, ""cryptanalysis of the tiger hash function," in international conference on the theory and application of," *Cryptology and Information Security*, p. 536–550.

[27] J. Kelsey and S. Lucks, "Collisions and near-collisions for reduced-round tiger,," in *International Workshop on Fast Software Encryption*, p. 111–125.

[28] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the kdd cup 99 data set,," in *2009 IEEE symposium on*

computational intelligence for security and defense applications, p. 1–6.

Sanad Malaysha Sanad Malaysha is a Ph.D. student at Birzeit University (2022), Palestine. Earned his M.Sc. degree in Computer Science from Arab American University(2021), Palestine, and also holds B.Sc. degree in Computer Science from Arab American University(2011), Palestine. The focus of his research works is about utilizing Machine Learning Techniques is solving real worlds problems, in fields such as security, health, and NLP. Sanad was born in Nablus, Palestine, where all his education and academic activities are done.

Ass. Prof Dr. Mohammed Moreb Mohammed Moreb was born in Hebron, Palestine, in 1981. He received the B.Sc. degree in information technology from Palestine Polytechnic University, the M.Sc. degree in computer science from Al-Quds University, and the Ph.D. degree in electronic and computer engineering from Altinbas University, Istanbul, Turkey, in 2019. The focus of his research is software engineering in health informatics. He has over twelve years of experience in managing software development projects, including large government IT systems. Expertise in advance AI/ML research, specifically focusing on deep learning, with a strong publication track record. ML engineering and software engineering research management experience in building high-throughput frameworks. Dr. Moreb recently founded a new framework and methodology specialized in software engineering for machine learning in health informatics named SEMLHI, It investigates the interaction between software engineering and machine learning within the context of health systems.

Dr. Ali Zolait Ali Hussein Zolait is an Assistant Professor at the College of Information Technology – University of Bahrain. Dr. Zolait is a senior member of IEEE, obtained the Fellowship of the British Higher Education Academy, and served as a Visiting Research Fellow at the University of Malaya (2007–2010). He acted as a leader in several international conferences. Dr. Zolait's research works have been published in leading international information systems and security journals. He is the Editor-in-Chief of the International Journal of Technology Diffusion (IJTD). Currently, he is the elected Chairperson of the IEEE Bahrain Section. He is the IEEE Membership Development Officer and an IEEE Computer Society member..