JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2328 - 2336
https://publishoa.com
ISSN: 1309-3452

Enhancement of Authentication in the IoT Network

Animesh Srivastava [1]
Research Scholar [1]
Banasthali Vidyapith [1]
er.animesh10@gmail.com

Dr. Anoop Kumar [2]
Assistant Professor [2]
Banasthali Vidyapith [2]
anupbhola@gmail.com

ABSTRACT

IoT devices, however, are resource-constrained in terms of computing, memory, storage, networking, and energy, making it challenging to secure them properly. In this sense, a lot of work has gone into addressing the security of IoT networks, mostly using classic cryptographic algorithms. The solutions are ML models using backpropagation neural networks to perform network optimization of the network and reduce the overhead consumption as well as increase the network lifetime. The paper highlights ECC's use across a broad range of authentication systems and investigates its potential. They also mitigate attacks and enable IoT security systems to make adjustments in changing environments as per the requirements. In the proposed scheme, we reduce the network errors and a more resistant authentication scheme.

Keywords: Machine learning, Hidden layer, Artificial neural network, Authentication, Internet of Things (IoT)

Objectives: Analyse the authentication scheme to mitigate the effect of the attack on the IoT network. To carry out network optimization and cut down on network error for the Internet of Things by using backpropagation of neural network sensor nodes with regard to wireless sensor networks.

Methods: Solutions can be contributed to by using machine learning models where it can be used for the optimization of the network and using ECC to mitigate attacks and enable IoT security systems to make adjustments in changing environments as per the requirements.

Findings: In this paper, we talked about security attacks as well as how ECC can improve IoT device performance and security. We have to use backpropagation to reduce network errors.

Novelty: We must use backpropagation to reduce network error and the particle optimization network to improve network utilization.

1. INTRODUCTION

In the IoT network If a packet is lost in a network, the system will resend the packet. The network and system must be rebuilt as part of this procedure. We say that if there is an error, there will be a packet loss, and we will have to start over. We reduce the error by using backpropagation [1-2]. Identifying the necessary patient at the proper time to serve them in healthcare. To develop a reliable system for managing patient preferences, the dropout rate must be minimal [6]. Spectrum resources cannot be utilised optimally until network difficulties and malfunctions are resolved, and they'll be a roadblock to further IoT development. The Internet of Things (IoT) is a new technology that is expected to transform a wide range of industries. The IoT enables all physical devices in the world to connect to the Internet and share vital real-time data. The number of devices increases the computational cost of data transport between devices and internet connections. One of the founders of RSA, Ronald Rivest, lectured about cryptography and machine learning [1]. Rivest emphasised in his presentation the parallels and contrasts between machine learning and encryption. The area has flourished since Ronald Rivest spoke about machine learning and cryptography. Cryptoanalysis and machine learning have more in common than cryptography. They have a same objective: expansive search spaces. The objective of machine learning is to identify an appropriate answer from a wide range of potential options. In recent years, machine learning applications have gained prominence. The study for this application centred on the future of machine learning-based cryptosystems and cryptanalysis. Other study topics include [2–7] privacy preservation, [8, 9] quantum machine learning, and [10] quantum machine learning. This article laid the ground for future study in cryptography and machine learning. IoT (Internet of Things) authentication refers to methods of securely and conveniently accessing connected devices such as smart homes, automobiles, transportation hubs, and workplaces, as well as ensuring the integrity and security of data from sensors and

other connected devices. we have combined both concept cryptography & Machine Learning and fined the best solution for the IoT.

2. Review of Related Literature

When a computer must learn how to solve a problem based on previously provided data, machine learning happens. There are several challenges that can be solved using machine learning. For example, there is no algorithm that is 100 percent accurate when we want the computer to detect spam emails. When machine learning is fed thousands of spam and non-spam instances, it may achieve near-optimal performance [11]. As it learns more about spam emails, it will become more accurate. Today's legacy database systems are overwhelmed by 2.5 quintillion bytes [13]. Except for effectively storing and analysing enormous volumes of data, the obtained data will be meaningless. Large-data processing techniques are necessary to exploit this data in a commercial application. Machine learning can be used in a wide range of applications, including commercial, health, and even political. In classification, machine learning is widely used [12]. Banks categorize loans as low-risk or high-risk. It must be possible for the bank to accurately categorize a loan. High-risk loans have a high default rate. Low-risk loans are expected to be paid back on time and regularly. Customer data, such as credit scores, is fed into the classification software. This data will be used to train the software to produce a loan-specific rule. This rule will help the bank determine the risk level of the loan. Multiple inputs are used to solve regression problems. A government might want to predict global oil prices. This system considers global production rates, current prices, past prices, and seasons (winter, spring, etc.). This is a number derived from the inputs. However, the system must be trained to learn the impact of changes in each input element over time.
Machine learning can also discover object associations. Supermarkets, for example, can use data analysis to boost sales. By analyzing thousands of shopping baskets, the supermarket system can produce useful association data.
According to the system, 80% of soda drinkers also buy potato chips. Aisle placement can help boost sales. Consuming canned food increases the likelihood of using disposable plates. This is why bundling or putting them in the same aisle can boost sales. It can be used in machine and human learning. When there is no reference output, learning occurs solely through input. In unsupervised learning or training in unsupervised learning, clustering is common. Clustering is used to find patterns in data sets. Customer density profiles can be created using historical data. It can also be used in AI. This can be a series of actions. The correct sequence of actions is crucial. A single move in a game may not be significant, but a succession of remedial measures may be. As a public-key cryptosystem, a tree parity machine with mutual learning was proposed. The paper offers a hypothetical public-key cryptosystem based on the synchronisation state of a tree parity machine. This "key" may be publicly traded without prior warning. Synchronization demands a minimal quantity of data input/output exchange. [14]

Mutual education is advantageous for cryptography. Two parties can develop a secret key for a public channel with the aid of mutual learning. The two sides enjoy an advantage over the attacker, who can only acquire knowledge in a single manner. [15]

A machine learning encryption classification test was conducted. No IP addresses, ports, or payload information were used in this project. In this study, C4.5 outperformed RIPPER, Naive Bayesian, SVM, and AdaBoost.[17]

The classified online machine learning algorithm attacks. This also examined machine learning algorithm flaws and fixes. The paper also presented two adversary simulation models. The paper explored exploratory integrity attacks in depth. Adversaries exploit learner blind spots to hide criminal activity. Many machine learning applications can use these attacks.[16]

According to the book, steganography may be deciphered with the use of machine learning. Using machine learning, the primary objective was to determine whether or not things were stereograms or clean papers. Using a service that provides cloud computing, you may delegate the execution of machine learning algorithms [18-19]. Accelerating machine learning and data processing may be accomplished through the utilisation of high-performance computing resources, such as cloud computing.

The three different methodologies—hyperplane decision, Naive Bayesian, and decision trees—were brought together with the help of AdaBoost. The researchers developed their own internal classifiers. On medical datasets, the suggested classifiers performed quite well [20]. [Citation needed]

Side-channel assaults were carried out with the use of machine learning methods [21]. The learning method known as Least Squares Support Vector Machine (LS-SVM) was implemented in the system that was presented, with power usage serving

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2328 - 2336
https://publishoa.com
ISSN: 1309-3452

as a side-channel (AES). According to the study, machine learning algorithm parameters have a significant impact on the results.

The IoT network is dynamic and node placements within the network are not fixed. As a result, the overhead increases the risk of network collisions and the blocking probabilities, which can result in missed packets; hence, optimization is essential, necessitating a self-learning process.

With the study literature review, research gaps have been found. We focused primarily on the security challenges of the IoT. We must address the authentication issue in the IoT perception layer. The current authentication schemes are quite successful in some ways, but they are not ready for upcoming challenges. A relatively new type of cryptography called elliptic curve cryptography has not received much attention from researchers. The current paper showcases ECC's use across a broad range of authentication protocols and examines its possibilities .

3. Methodology

Authenticating a user involves having them gently ask the system to authenticate their identity, authority, or capacity so that the system may quickly and readily access whatever data they have stored in the system as a user. However, there is a persistence of the attack in the registration phase of the scheme, which can be avoided by using some cryptographical technique.

3.1 MACHINE LEARNING

In 2016, Peprnot et al. published a comprehensive study of machine learning security and privacy [26]. The paper introduces a comprehensive threat model for machine learning, as well as an adversarial framework for attacks and defenses. Training adversarial settings were divided into two categories: privacy and integrity. Inferring in adversarial settings was also divided into two types of adversaries in both the white and black boxes The study also explained how to create a machine learning model that is reliable, private, and accountable.
According to the authors, the classes identified influence the cost for both attackers and defenders. [23] The paper also provided a comprehensive review of previous attacks on machine learning systems. A spam filter called Spam Bayes is used to illustrate the taxonomy. This attack is similar to the exploratory integrity attacks discussed in section 3 in that it injects adversarial data into the machine-learning training data. The paper states that machine learning must be thoroughly tested for adversarial data resistance.[24] A statistical data leak from machine learning classifiers can occur unintentionally or maliciously. To hack other classifiers' training sets, a new meta-classifier is developed and trained. Classifier performance can be improved or trade secrets stolen from rivals using this attack technique. [25] By altering their own conduct, enemies might avoid being taught. Until recently, little study has been done on established methods of learning. A A variety of other possible applications where data-driven approaches may generate security problems were identified to examine the methodology, difficulties, and future research objectives for safe learning and learning-based security applications. So-called "spam detection," "author identification," and "copyright enforcement" are only a few examples of these kinds of applications.

II. ANN STRUCTURE
Processing units are the fundamental building blocks of an artificial neural network. Sending signals to one another is the means through which these units communicate with one another. There are elements of ANN that already exist.

1. Many processing units, e.g., neurons or cells,
2. The activation status of the unit (yk), as well as the unit output equivalent3. Interunit on the left.
3. Each link is assigned a weight.
4. A propagation rule that defines a unit's effective Sk input.
5. Function activation Fk, which calculates the new level of activation based on the effective input sk (t).
6. For each unit, the external input (along with bias and offset) oscillates.
7. Information gathering method (the learning rule) A system environment for operating and providing input signals and error signals where necessary.

III. NETWORK ARCHITECTURES
There are three network architectures:
1. Single-layer feeds network transmission: A neuronal source node is the input layer in that layer. It is a type of network feed-in.
2. Multilayer feed networks—add just one additional layer called the "hidden layer." This hidden layer produces higher levels of statistics.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2328 - 2336
https://publishoa.com
ISSN: 1309-3452

3. Recurrent network: A recurrent network has at least one feedback loop. The neuron output is returned to its input in this loop, thus increasing the capacity to learn. And performance is also increasing.

3.2 BACKPROPAGATION

The single-layer feed-forward network has several drawbacks. Because of this, we employ backpacking as a method of reducing human error. In order to calculate the hidden layer unit errors, the output layer unit errors are recursively distributed backward. Background learning rule refers to this approach. Multi-layer generalisations can also be viewed as a form of this rule.

4.1 General Delta Rule–This formula is used to calculate the delta for all network units. This generalized Delta rule applies to non-linear unit feed-in networks.

Multilayer Perceptron Network

Neural networks are networks of processing elements driven by biological neuron models capable of performing similar calculations to the human brain. Artificial neuron models have synapses, adders, and activation functions and externally

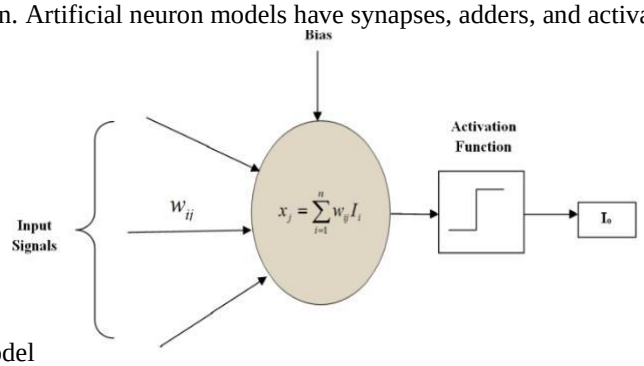

Figure1: Artificial Neuron Model

Each point called a neuron is used to create a different type of network with or without an induction activity. By altering the activation function and the interaction value, the input of each neuron has a different effect on the outcome. Self-organization, learning, flexibility, comparison, energy processing, and low counting are features of neural networks [27]. An artificial neural network is a systematic design strategy inspired by biology that may approximate the function of numerous inputs or multiple outputs. Devices built on artificial neural networks are utilised for explanation modelling, clustering period forecasting, and image processing. (FNN) is one of the most used ANN systems.

A multi-layer perceptron (MLP) is a feedforward neural network that uses gradient-based learning with a low number of hidden neurons or can utilise the BP error approach to handle a range of challenges and facilitate learning. The backbone spread of the method may be utilised to reduce the disparity between the actual output and the estimated output. In MLP, one or more hidden layers participate in the difficult process of isolating gradually the most fundamental events from connected birds. Figure 2 depicts the MLP structure utilised for the presentation analysis.

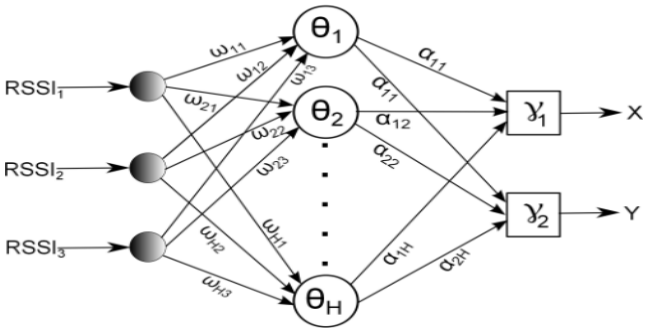

Figure 2: Multi-Layer Perceptron Network

Given the availability of noise sources in actual WSN applications during the past several years, RSS has been utilised as a strategy for zeroing nodes. Positioning technology based on artificial neural networks (ANN) may discover complex links between input and output changes and learn about these interactions [28]. Theoretical ANN studies (in the context of so-called feedforward) suggest that a single-layer network with a sigmoidal point (in the hidden layer) may be close to the function [29]. This feature enables us to anticipate that if the RSS value is at least a position with three anchors on the node measured at a particular place in a two-dimensional space (as determined by triangulation), then:then a sigmoid

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2328 - 2336
https://publishoa.com
ISSN: 1309-3452

feedforward tortious network can be created (SFFANN), which takes the RSS value measured by the anchor response when it enters and predicts the alignment of the bright point of the signal. This method has been used in some reported works.
The network input (RSSI1, RSSI2, and RSSI3 in our example), multiplied by the value of the input layer in the hidden layer, the wij represents the strength of the relationship between the hidden node and j-th input, and summarize the input to get the network access to the n-hidden node 'is:

$ni = \sum_{j=1}^{3} wijRSSI + \theta I$

Among these, θi is referred to as a gate parameter or value. The access of the hidden net node is modified by non-linearity (activation), which requires a monotonous, binding, continuous and distinctive increase. The most commonly used force functions are logical (also called sigmoid logarithmic functions):

$\sigma(x) = \frac{1}{1+e-x}$

And the hyperbolic-tangent function (tan sigmoid function):

$\sigma(x) = \frac{e^{x}-e^{-x}}{e^{x}+e^{-x}}$

Due to the symmetry of the strange function, the hyperbolic tangent function is often used as the activation function. The output of the hidden node is multiplied by the index of the αij connection string and summed by the index of the remote node to attain the i-th output of the network:

$xi = \sum_{j=1}^{H} \alpha ij\sigma(nj) + \gamma i$

If i = {1,2}, H is the number of hidden nodes, x1 = X or x2 = Y, and γ represents range / value of the output node. The network values (w, α, θ, γ) as a group (called with values for short) are started with a small value, and the input (RSSI value) is obtainable to the network to predict configurations of the transmitting node. Suppose we assume that the predicted value compares (x, y) and the actual value (X, Y). In that case, the difference among the expected value or target value is the average of the input pairs. Enter all slowly.

$E = \frac{1}{4}((X - x)2 + (Y - y)2)$

To develop the FANN model for all problems, the error function associated with E is reduced by a non-linear optimization method to attain a value and reduce the value of E in all data. These methods integrate the Widrow-Hoff study law with multilayer networks and non-uniform transfer functions, so they have been termed false backpropagation methods.
The foundation function of every neuron in the MLP network is nonlinear. In an MLP network, each neuron has a nonlinear activation function. As there is no inequality, the connection between the output parameters of a single perceptron may be streamlined. A multi-layer perceptron (MLP) network has one or more hidden layers, allowing it to learn difficult tasks by progressively removing less relevant input vector parts. It also demonstrates a strong bond. In order to construct an efficient system for position detection in wireless sensor networks, the multi-layer perceptron architecture combines the input or output of hidden layer input functions for simulation. Here are some opinions regarding MLP's position:

MLP uses a backpropagation (gradient) algorithm to modify the value of each neuron to reduce the square root error between the output value and the actual value.

$Xk+1 = Xk-\Omega kgk$

Where Xk+1 is a vector of weights and biases
gk is the gradient, ηk is the learning rate
Sigmoidal feedforward ANN has universal proximity (UAP) characteristic, which helps solve the problematic learning task. This property means that for a 3-layer network with sufficient hidden nodes, it is possible to approach the continuous operation without proper dependence by using sigmoidal inequality. Sigmoidal activity is δ function, which is continuous, continuous, and distinct, and has asymptotic properties, so that for

$x \in \mathbb{R}, \log_{x\to\infty} \delta(x) = \alpha$

$\log_{x} \delta(x) = \beta$

Where α=1 & β=0 or β= -1 where $\mathbb{R}$ is the set of all real numbers. The hidden layer nodes use the hyperbolic tangent transfer function, as shown by the following equation

$$\tan(x) = \frac{e^{x} - e^{-x}}{e^{x} + e^{x}}$$

The function of the development layer activation remains linear because the output is a two-dimensional spatial coordinate. 1. You should avoid distractions during training. 2. The rate of learning is set with adequate training. 3. Different learning algorithms to train the network.

In upcoming times, ECC will play a major role. RSA has first-mover advantages and many more, such as RSA is easier to implement, RSA is older than ECC, and the people who use RSA have paid a lot of money to use RSA. In the future, for lightweight devices and enhanced security, we have to use ECC.

Table 1: Comparison of ECC and RSA based on key size for same security level [28]

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2328 - 2336
https://publishoa.com
ISSN: 1309-3452

ECC key size (bits) ratio	RSA key size (bits) Key size	ECC better than RSA in percentage
163	1024	628%
256	3072	1200%
384	7680	2000%
512	15360	3000%

The goal of this paper is to provide ECC-based authentication and key exchange mechanisms. The suggested protocols have undergone mathematical and formal examination, demonstrating that they are secure against a variety of network threats.

4. Proposed Solution

Artificial Neural Networks (ANNs) are a method for modelling high-complexity computer machines that is both simple and effective. Using a back-propagation algorithm, this method was utilised to create a primitive mix of logic and sequence machine.A comparison of the strengths and drawbacks of the two different neural network architectures has been conducted. Highly complex coupled and sequential circuits can be implemented using ANNs. Our performance evaluation shows that our system can meet security needs without using a lot of computing power. In contrast, the suggested technique demands lower communication costs. After employing Backpropagation, we also minimise network errors, hence increasing system throughput.

5. Result & Discussion

We choose ANN for the supervised learning process since it is extremely robust and has a rapid response and reaction time, which reduces training errors and losses. A thirty-node network is used in this simulation. Throughout the entire network used as an administrator, the monitor's malicious activity is broadcast throughout the network. The simulation was done using MATLAB software.

TENC also lowers the cost of computing. The ANN reduces the overhead usage from 12.2 to 2.6. We noticed an improvement in network performance after applying the ANN.

Table 2: ANN Comparison

Parameter	Before ANN	After ANN
Consumption of Energy	220.6 mJ	2.1 mJ
End Delay	4 s	58.1 ms
Overhead Consumption	12.2	2.6

Table 1 Tabular representation of the general network If you're looking to build circuits that integrate and sequential circuitry, then an artificial neural network (ANN) is the best option. Aside from TENC, the overhead consumption is decreased to 2.6 from 12.2 using the neural network.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 2328 - 2336
https://publishoa.com
ISSN: 1309-3452

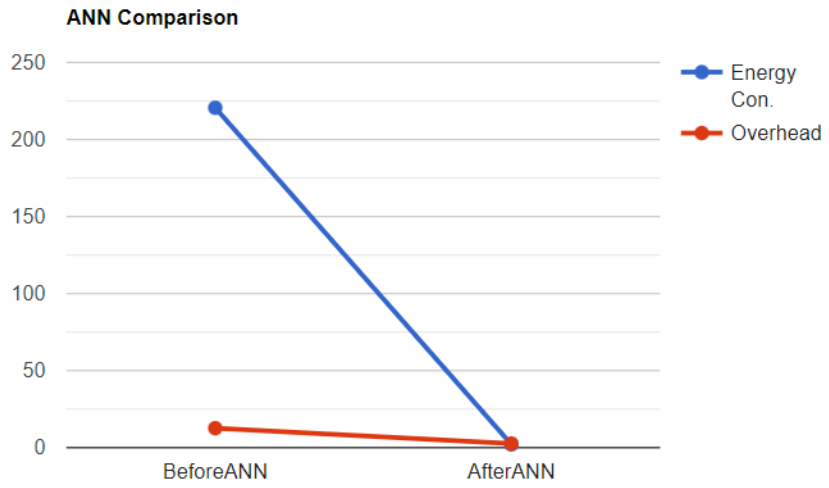

Figure 1 : ANN Comparison

Additionally, we use the ECC concepts to enhance security, so our concept should be more viable in the sense of being efficient and more secure.The principal factor while designing is to balance security & overhead.

6. Conclusion And Future Directions

This study is centered on security attacks as well as how ANN and ECC can improve IoT device performance and security. We have demonstrated that our proposed protocol can withstand attacks. Additionally, we discovered that our protocol is much more efficient regarding time and communication costs. We find that implementing the ANN improves network performance by more than 75% when compared to not using backpropagation.

In this, we proposed ECC for lightweight devices to enhance their security. which will enhance the authentication process and also reduce process time and overhead. That can be useful for IoT-based smart healthcare, creating an enhanced authentication solution for resource-constrained wearable devices.

7.1 Future Directions

In the near future, we would like to explore the following areas:

(1) Creating symmetric and asymmetric cryptosystems using machine learning algorithms Perhaps two AI-based systems will design their cryptosystems as AI advances.

(2) Making use of machine learning to train on muddled data sets.

(3) Using machine learning to improve the efficiency of existing cryptanalysis techniques (for example, differential or linear cryptanalysis).

REFERENCES

[1] Martínez-Peláez, R., Toral-Cruz, H., Parra-Michel, J. R., García, V., Mena, L. J., Félix, V. G., & Ochoa-Brust, A. (2019). An Enhanced Lightweight IoT-based Authentication Scheme in Cloud Computing Circumstances. *Sensors (Basel, Switzerland)*, *19*(9), 2098. https://doi.org/10.3390/s19092098

[2] Jong-Young Choi;Jiwoong Park;Sung-Hwa Lim;Young-Bae Ko A RSSI-Based Mesh Routing Protocol based IEEE 802.11p/WAVE for Smart Pole Networks 2021 23rd International Conference on Advanced Communication Technology (ICACT) Year: 2021

[3] Eryk Schiller, Andy Aidoo, Jara Fuhrer, Jonathan Stahl, Michael Ziörjen, Burkhard Stiller, Landscape of IoT security, Computer Science Review, Volume 44, 2022,

[4] O. Ohrimenko, F. Schuster, C. Fournet, A. Mehta, S. Nowozin, K. Vaswani, and M. Costa, "Oblivious multi-party machine learning on trusted processors.," in USENIX Security Symposium, pp. 619–636, 2016.

[5] A. Srivastava and A. Kumar, "A back propagation NN to optimize the IoT network," *2022*, pp. 1-4, doi: 10.1109/ICCCI54379.2022.9740861.
[6] P. Mohassel and Y. Zhang, "Secureml: A system for scalable privacy-preserving machine learning," in 2017 38th IEEE Symposium on Security and Privacy (SP), pp. 19–38, IEEE, 2017.

[7] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1175–1191, ACM, 2017.

[8] Y.-B. Sheng and L. Zhou, "Distributed secure quantum machine learning," Science Bulletin, vol. 62, no. 14, pp. 1025–1029, 2017.

[9] D. Ristè, M. P. da Silva, C. A. Ryan, A. W. Cross, A. D. Córcoles, J. A. Smolin, J. M. Gambetta, J. M. Chow, and B. R. Johnson, "Demonstration of quantum advantage in machine learning," npj Quantum Information, vol. 3, no. 1, p. 16, 2017.

[10] Suggestive References Istiaque Ahmed, K.; Tahir,M.; Hadi Habaebi, M.; Lun Lau, S.;Ahad, A. Machine Learning forAuthentication and Authorization inIoT: Taxonomy, Challenges andFuture Research Direction. Sensor. 2021,21, 5122. https://doi.org/10.3390/s21155122

[11] A. A. Alsadhan and M. M. A. Alani, "Detecting ndp distributed denial of service attacks using machine learning algorithm based on flow-based representation," in Developments in eSystems Engineering (DeSE), 2018 Eleventh International Conference on, IEEE, 2018.

[12] Game Theory and Machine Learning for Cyber Security", Wiley, 2021

[13] "How much data do we create every day?." https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#645fe1f960ba. Accessed: 2022.

[14] Securing Internet of Things (IoT) with machine learning. Sherali Zeadally and Michail Tsikerdekis. Int J Commun Syst. 2020;33:e4169. https://doi.org/10.1002/dac.4169

[15] Marabissi, D.; Mucchi, L.; Stomaci, A. IoT Nodes Authentication and ID Spoofing Detection Based on Joint Use of Physical Layer Security and Machine Learning. Future Internet 2022, 14, 61. https://doi.org/10.3390/fi14020061

[16] Mohammed M. Alani. "Applications of machine learning in cryptography", Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19, 2019

[17] Kathamuthu ND, Chinnamuthu A, Iruthayanathan N, Ramachandran M, Gandomi AH. Deep Q-Learning-Based Neural Network with Privacy Preservation Method for Secure Data Transmission in Internet of Things (IoT) Healthcare Application. Electronics. 2022 Jan;11(1):157. https://doi.org/10.3390/electronics11010157

[18] Jayalaxmi PL, Saha R, Kumar G, Kim TH. Machine and deep learning amalgamation for feature extraction in Industrial Internet-of-Things. Computers & Electrical Engineering. 2022 Jan 1;97:107610. https://doi.org/10.1016/j.compeleceng.2021.107610

[19] Y. Liu, J. Wang, J. Li, S. Niu and H. Song, "Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 298-320, 1 Jan.1, 2022, doi: 10.1109/JIOT.2021.3099028.

[20] Internet of Things (IoT) Authentication and Access Control by Hybrid Deep Learning Method - A Study. Dr. Joy Iong Zong Chen and Kong-Long Lai, Journal of Soft Computing Paradigm (JSCP) (2020) Vol.02/ No.04 Pages: 236-245 http://irojournals.com/jscp/ DOI: https://doi.org/10.36548/jscp.2020.4.005

[21] Attkan, A., Ranga, V. (2022). Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security. Complex and Intelligent Systems. https://doi.org/10.1007/s40747-022-00667-z

[22] Chan Suet Yan, Sharon and Wei, Alice and Bong, Jie and Teh, Quor and Sivalingam, Shanmugapiriya and Khoo, Shi & Nafy, Tahmid. (2021). Authentication of IoT device with the enhancement of One-time Password (OTP). Journal of IT in Asia. 9. 29-40. https://doi.org/10.33736/jita.3841.2021

[23] M. Azrour, J. Mabrouki, A. Guezzaz and Y. Farhaoui. (2021). New enhanced authentication protocol for Internet of Things. Big Data Mining and Analytics, 4(1):1-9. https://doi.org/10.26599/BDMA.2020.9020010

[24] Ahmad, H. S., Arshad, M. J., & Akram, M. S. (2021). Device Authentication and Data Encryption for IoT Network by Using Improved Lightweight SAFER Encryption with S-Boxes. International Journal of Embedded and Real-Time Communication Systems (IJERTCS). 12(3):1-13. http://doi.org/10.4018/IJERTCS.2021070101

[25] Amiya Kumar Sahu, Suraj Sharma, Rohit Raja, Deep Learning-based Continuous Authentication for an IoT-enabled healthcare service, Computers and Electrical Engineering, Volume 99,2022,https://doi.org/10.1016/j.compeleceng.2022.107817.

[26] N. Papernot, P. McDaniel, A. Sinha, and M. Wellman, "Towards the science of security and privacy in machine learning," 2016.

[27] Philipp Mundhenk, Andrew Paverd "Security in Automotive Networks: Lightweight Authentication and Authorization" ACM Transactions on Design Automation of Electronic Systems 2016.

[28] Zhang, Liping & Tang, Shanyu & Luo, He. (2016). Elliptic Curve Cryptography-Based Authentication with Identity Protection for Smart Grids. PloS one. 11. e0151253. 10.1371/journal.pone.0151253.