ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2023.0422

DECENTRALIZED BLOCKCHAIN WITH CONVOLUTIONAL NEURAL NETWORK MODEL FOR SECURITY ATTACK MITIGATION

C. Berin Jones[1] and D. Jeba Kingsley[2]
[1]*Department of Computer Science and Engineering, Madurai Institute of Engineering and Technology, India*
[2]*Department of Information Technology, DMI College of Engineering, India*

Abstract

In recent era, there is a demand and a need for more effective solutions based on new technologies for detection and mitigation because of the limitations and current state of the methods. In this research, we propose the design of a distributed ledger that utilises a convolutional neural network as a layer of defence against intrusions carried out by malicious actors. The result of simulation shows that the proposed method achieves a better traffic flow than the existing methods.

Keywords:

Blockchain, Convolutional Neural Network, Security, Mitigation, Passive Attacks, Traffic Flow

1. INTRODUCTION

The capability to support the autonomous operations and communications, the Internet of Things (IoT) is presently playing a pivotal role in the physical world. This is due to the fact that IoT is able to support these functions [1]. This capability is assisting in the facilitation and advancement of new services that play a significant role in the day-to-day existence of individuals. The IoT has found widespread application in a variety of industries, such as healthcare, smart cities, smart power networks, and so on, to facilitate efficient resource management and pervasive sensing [2]. This is a result of the advancements that have been made in information and communications technology (ICT) as well as the proliferation of technologies that utilize sensors.

By the year 2025, it is anticipated that there will be 75,44 billion devices connected to the Internet of Things that will be in use all over the globe. The IoT is made up of an ever-increasing number of devices, and there is an ever-increasing demand to protect these devices from being subjugated to cyberattacks. In addition, there is an ever-increasing demand to protect data that is transmitted over these devices [3].

The pervasive use of security protection methods at lower levels and the simplicity with which devices can be accessed from anywhere via the internet, existing IoT ecosystems are susceptible to a wide variety of security attacks. These attacks can be particularly damaging because they can compromise the integrity of sensitive data. The security risk associated with the IoTs ecosystem is significantly higher than that of a traditional network. This is due to the increased opportunities for malicious actors to take control of vital infrastructures like essential sensors, moving vehicles, and nuclear facilities and cause damage [4].

In the event that an adversary is successful in seizing control of a device and putting it to malicious use, the entire ecosystem of the IoTs, including the devices themselves, is vulnerable to privacy infractions. As a direct result of this, given the frequency with which attacks are launched against the environment of the IoT, there is an immediate need for research into and the development of innovative security defense strategies. This is a prerequisite that must be met immediately. Because of the ecosystem distributed structure, it is difficult to monitor and aggregate historical data from that system, which makes it difficult to develop a security attack detection mechanism that can provide optimal security and defense in the IoT ecosystem. This makes it difficult to develop a mechanism that can provide optimal security and defense in the IoT ecosystem. Because of this, it is difficult to create a security attack detection mechanism that can offer the highest possible level of protection and defense within the IoT environment [5]. The heterogeneity of the devices that make up the IoT, the complexity of the network topology, and the unpredictability of the information make it challenging to design an efficient security protection system. When it comes to detecting security breaches in the IoT, the methods that are presently available are frequently insufficient. This is due to the fact that there are many obstacles that need to be conquered [6].

The vast majority of methods for detecting lapses in network security depend on a centralized infrastructure. Specifically, detection software is typically installed on a single cloud server that is situated in the geographic center of the network. Because the environment of the IoTs contains such a large number of devices that are connected to one another, it is extremely unlikely that these methods will ever become more ubiquitous. Because there are storage limitations, expensive processing, excessive latency, and a singular point of failure, the cloud server will continue to be ineffective [7].

This research proposes the distributed ledger design using convolutional neural network (CNN) as a layer of defence against intrusions carried out by malicious actors.

2. TECHNICAL BACKGROUND

Cryptocurrencies are a form of digital commodity that are managed by a decentralized and distributed network referred to as the blockchain [8]. The distributed ledger technology, also known as blockchain, is an essential component of the cryptocurrency market fundamental infrastructure. The business of cryptocurrencies is not the only industry that stands to gain from the implementation of blockchain technology. Other industries, such as finance, healthcare, real estate, and the supply chain, also have a chance to profit from the technology [9]. There has been a recent uptick in the number of businesses looking to blockchain technology as a means to safeguard confidential customer data and verify the identities of prospective clients [10].

Private blockchains, also known as permissioned blockchains, are used by a variety of different groups as opposed to public blockchains, which are used by the bitcoin protocol and enable anyone to participate. Private blockchains are also referred to as permissioned blockchains. A blockchain is a form of digital

record that is not managed by a single entity but rather is maintained by a network of computers known as nodes. Blockchains are also known as distributed ledger technology (DLT). These computers collaborate with one another to verify information and share data in an open and honest fashion. A computer or other electronic device that is capable of storing an entire digital document is capable of functioning as a network node. A network node can be any computer.

A decentralized model governs the operation of the blockchain network, which allows individual servers to preserve their autonomy [8]. The term decentralization can be interpreted in a variety of ways [9], exist: in layman terms, blockchain is politically decentralized due to the fact that it is not governed by a central authority; in architectural terms, it is decentralized due to the fact that the failure of individual nodes does not disrupt the operation of the network as a whole; however, in a logical sense, they are centralized due to the fact that the entire system operates in the same manner as a single computer. There are three primary contributors to the significance of having one own identity, all of which work together to create this importance.

First, the capacity of the blockchain to tolerate errors grows, which improves its dependability on a diverse collection of network servers. Second, the number of nodes that make up the blockchain also grows. Second, it is resistant to attacks, which is an important quality because it is typically not cost-effective for attackers to target individual nodes within a network. This is because of the nature of the distributed nature of the internet. This is due to the interconnected structure of the system, which is why this occurred. Individuals are unable to gain an advantage at the expense of other people because they are unable to conspire with one another, which is the main factor that prohibits this [11].

3. PROPOSED MODEL

The recommended architecture utilizes a bottom-up methodology, with the sensing layer serving as the point of origin and the cloud as the destination of the process. The detecting layer is where everything gets started. Whenever the network is in operation, each CNN-enabled edge layer switch communicates the traffic traces that it has observed with the fog node that corresponds to it in the cloud layer. These traffic traces originate from the sensor nodes that are connected to it in the sensing layer. The sensor nodes that are located in the sensing layer are the source of these traffic records. In order to discover potentially harmful traffic patterns emanating from the sensor nodes, the CNN controller of the cloud node will first learn from the traffic traces and then evaluate them.

The controller determines whether or not the current traffic is malicious based on information about traffic patterns that have happened in the past. This information includes the number of attacks that have occurred and the number of features that have been utilized. After the analysis is finished, the CNN supervisor of the cloud server makes a decision about the flow of the data through the switch. The manager of the CNN will then make dynamic allocations of the flow principles to the appropriate switches after that. The CNN controller is responsible for defining the rules that must be adhered to, and the switches are responsible for reacting to those rules by performing a variety of operations in relation to the influx of information from IoT devices. These strategies might involve completely impeding the flow of traffic or just slowing it down slightly.

Additionally, in the event that a cloud node discovers any noteworthy patterns or occurrences, it will communicate this information to the CNN controller that is situated in the cloud layer. After that, the CNN controller will provide updates to the controller at predetermined intervals. As a consequence of this, the cloud-based CNN controller is in a position to form opinions regarding the flow of traffic from IoT devices regardless of their placement within the network. This is because the cloud-based CNN controller has access to data regarding events and patterns collected from numerous cloud nodes.

As a result, the CNN controller is able to search for events that are similar across different clusters and draw conclusions about impending waves of attacks on IoTs devices located across its network. Provisioning of security can now be done remotely and without the need for human intervention. It is now feasible to digitally secure devices, and users will not be required to take any additional steps as a result of this information. A traffic flow analyzer, a traffic flow classifier, a blockchain-based attack detection and mitigation module, and a blockchain-based attack mitigation module are the components that make up the CNN controller at the cloud node in the proposed architecture.

The initial two components analyze the traffic and produce a customized attack detection model for the cloud server based on any abnormal patterns they find. The blockchain technology is then utilized in the third component in order to perform dynamic updates to the attack detection model. The attack mitigation module makes use of the attack detection model in order to thwart attacks that are directed at the interface layer. This is the last and most important step.

3.1 TRAFFIC ANALYZER

While it is dynamically monitoring the traffic coming from a wide assortment of IoTs devices, the traffic flow analyzer maintains a log of the data that it collects. This information contains the total number of requests that were sent from a device, the origin of the request, and any other pertinent details. Under normal circumstances, the information that is gathered is first examined to determine whether or not it is legitimate, and then it is used to educate a system so that it can distinguish between false traffic and genuine traffic.

It is possible to identify attacks that target the environment of the IoTs with the assistance of a traffic flow analyzer that includes a directory of known IoT device vulnerabilities, attack patterns, and blacklisted source IP addresses. This makes it possible to identify threats to the security of IoT devices. Because of this, the traffic flow classification is able to take full advantage of the traffic flow analyzer comprehensive understanding of both types of traffic. This is a direct consequence of the previous point.

3.2 CNN TRAFFIC FLOW CLASSIFIER

This section helps to guarantee that the data collected from attacks on the cloud node are accurately categorized by preparing the attack detection model. Each individual cloud server will then use the data regarding the traffic that is specific to them in order to construct the trained model with the assistance of various machine learning techniques. Deep learning, a type of machine

learning classification algorithm, is put to use within the recommended architectural structure.

When we provide a deep learning model A_k with n input neurons that describe the encoding process in the first layer of the model, we obtain the following when the dataset $a=\{a_1; a_2;\ldots; a_n\}$ is not constrained:

Given an unlabeled dataset $a=\{a_1; a_2;\ldots; a_n\}$ for deep learning model, where n input neuron for the first layer of model A_k describes the encoding process as follows:

$$h_1 = F(w_1 a + b_1) \quad (1)$$

where

F - activation function and

w_1 – weight matrix,

b_1 - bias vector.

The sigmoid function, which is an activation function and can be characterized as follows:

$$F(z) = 1/[1 + \exp(-z)] \quad (2)$$

The results of the first hidden layer, which are indicated by h_1, are sent to the second hidden layer, which is denoted by h_2, and are then used to train the second set of network parameters, which are denoted by w_2 and b_2. The part that has been disassociated from the rest of the structure is denoted by h_1, which stands for the second concealed layer. It is necessary to train all the way up to the N^{th} concealed layer, which is denoted by h_N, in order to train the network parameter referred to as W_N.

The model feature A_k that was obtained at the Nth layer is what is meant when the h_N is used. The network characteristics (weight matrix and bias vector) for the N^{th} hidden layer in the deep learning model A_k are represented by the equations $w = w_1, w_2,\ldots, w_N$ and $b = b_1, b_2,\ldots, b_N$ in their appropriate places.

Both the weight matrix and the bias vector are denoted by these notations, correspondingly. During the training phase of deep learning, a method known as gradient descent is utilized to make modifications to the network parameters that are being learned. This method operation is broken down into quantitative detail in the accompanying explanation.

$$w_1^{l+1} = w^{1,l} - \beta \frac{\partial J(w_1, b_1)}{\partial w_1}, l = 1, 2, ..., L \quad (3)$$

$$b_1^{l+1} = b^{1,l} - \beta \frac{\partial J(w_1, b_1)}{\partial b_1}, l = 1, 2, ..., L \quad (4)$$

where

L - maximum iterations

β - learning rate.

J - loss function and this is minimized using the process of stochastic gradient descent.

The method described above is implemented during the training period of each attack detection model A_k, and features for all models ($f_1, f_2,\ldots, f_m$) are extracted from the final hidden layer h_N of each model. f_m stands for features for all models. Early fusion is conducted on all attack detection models ($A_1, A_2,\ldots, A_m$) using the extracted features, which results in a structure that is completely connected and characterized by two layers and one hidden layer. The values that will be used for the layer that will come after it are determined by taking a weighted average of the values that were used for the levels that came before it.

After the weight matrices have been seeded with random data at the beginning of the process, the back-propagation method is used to determine the numbers that produce the best results for both matrices.

$$H_i = \sum_{k=1}^{|f_c|} W_{1,k_i}^T f_c \quad (5)$$

where

f_c - concatenated vector and

W_1 - weight matrix.

The utilization of the softmax function is what ultimately leads to the achievement of the desired outcome Y, as below:

$$Y_i = \frac{\exp\left(\sum_{k=1}^{|H|} W_{2k_i}^T H_k\right)}{\sum_{j=1}^{d} \exp\left(\sum_{k=1}^{|H|} W_{2k_i}^T H_k\right)} \quad (6)$$

where W_2 is the weight matrix.

3.3 ATTACK DETECTION

The attack detection model is a component that is generated from the traffic flow classifier. This component automatically updates the attack detection model at the cloud node based on the attack detection model from other cloud nodes. Because we have upgraded the attack detection model, we are now able to identify attacks with a higher degree of precision and educate the CNN routers to recognize them when they occur. A novel strategy for automatically keeping the attack detection model up to date is proposed, and an illustration of this strategy can be found in Fig.1.

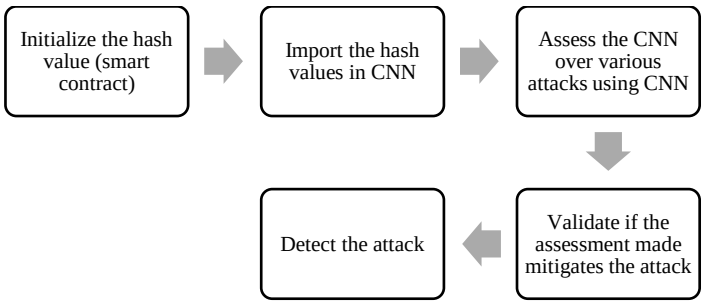

Fig.1. Attack Detection

The strategy that has been proposed includes not just one but two components: the manager and the representatives. One of the responsibilities of a manager is to create a unified defense system out of attack detection models that have been pulled from various cloud platforms. This section describes the data-driven responsibilities for attack detection, as well as the format of incoming data and the consequences that should be anticipated from attack detection models.

According to the strategy that has been proposed, each cloud node reports its anticipated accuracy for proofing the attack detection model to the central cloud server, which serves as a manager and provides a testing set of data. This is done so that the

central cloud server can evaluate the results. The model is verified as a result of the primary cloud server carrying out these actions.

This section provides an explanation of the compensation guarantees that come along with the decentralized technique for threat detection. The recommendation that is provided by the cloud server regarding the way in which to best organize the detection strategy for attacks is, in the majority of instances, the most reliable option. On the other hand, agents are accountable organizations that are charged with managing the decentralized attack detection strategy and ensuring that it is accurate. They are responsible for ensuring that the strategy is accurate.

The method that is detailed in this article is capable of employing a cloud server either in the capacity of a processing or proofing agent. Every cloud node, in its capacity as a processing agent, is accountable for independently preparing the attack detection model. This is achieved by instructing each node to run a machine learning algorithm on the data stored locally on that particular node. The validation agent ensures the accuracy of the recently developed attack detection model by subjecting it to a series of tests and conducting verification procedures.

4. RESULTS

The proposed model is tested on four different types of attacks that includes n confirmation attack, 51% attack, transaction issues and selfish mining.

4.1 51% ATTACK

Imagine for a second that there is an adversary that is armed with enough hashing power to launch a 51 percent attack. In order to add an additional layer of complication to the situation, an adversary has mined a separate chain that is longer than the primary chain, and they are broadcasting it to the network. In order to comply with the proof-of-work principle that stipulates using the chain that is the longest in length, the nodes in the network are required to use the chain that was created by the intruder.

CNN, on the other hand, is proposing a novel solution to the issue at hand with the concept that it is currently developing. CNN performs a number of tests on the information that is recommended in order to determine whether or not the solutions provided for the three puzzle blocks are accurate. Because the block height is greater than the number that was anticipated, the certification of the attacker chain has been rendered invalid as a result of this.

It is proposed that as soon as CNN recognizes an attack, it will immediately stop the node that is under attack from participating in any further network operations for a predetermined amount of blocks. In the event that none of the three blocks are able to fulfill the requirements, the mining process will have to begin again, and the three nodes that contributed to the unsuccessful blocks will be punished. In the event that none of the three blocks are able to satisfy the requirements, the mining process will have to begin again.

4.2 TRANSACTION CONFIRMATION DELAY

On average, a new block is generated by the Bitcoin network about once every ten minutes. A transaction on the Bitcoin network is not considered to be finalized until it has obtained a minimum of six confirmations; however, the more confirmations that are obtained, the more secure the transaction will be.

Due to a flaw in the Bitcoin network, the process of clearing the mempool of large transactions can take a lot longer than the process of clearing the mempool of smaller transactions that have greater fees. The reason for this is that miners prefer to make smaller deals because this enables them to include a greater number of transactions in each block, which in turn enables them to earn more benefits. Miners prefer to make smaller deals because this enables them to earn more benefits. Even after a protracted delay for large transactions with low fees to be included in a block, participants still need to wait at least six confirmations before they can consider their transaction to be secure. There is also no guarantee that a transaction will be included in the next block within a certain amount of time due to the guidelines that are presently in place for reaching a PoW consensus. These guidelines have been put in place so that a PoW consensus can be reached. It is possible that a transaction will be held in the mempool for a number of days if the selection procedure includes an element of randomness.

According to the hypothesis, the fact that CNN employs an innovative method for classifying material contributes to the solution of this problem in some way. As shown in Figure 8, there were three different groups that were successful in advancing to the sorting stage. Transactions were selected to be included in Block C based on the higher fees paid by users in order to have their transactions completed more quickly. This decision was made in order to maximize the efficiency of the blockchain. These miner transactions were also included in Block C. It was discovered, as a result of the application of a cutting-edge method for comparing and sorting the data, that of the three blocks, Block B comprised the greatest number of transactions of a significant magnitude. It is very important to keep in mind that the proposed CNN block selection procedure is not taken into consideration when calculating the transaction fees.

4.3 N CONFIRMATION ATTACK

The Zero, One, Confirmation Attack and the Miner Bribe Attack are two other techniques of attack that are similar but exploited in different ways. Throughout the entirety of this conversation, we will refer to all attacks as n-confirmation strikes. This is so that we can keep things as simple as possible. The level of sophistication of these various attacks may range, but one thing that they all have in common is that in order to circumvent the protections that are in place for the network, they all make use of the extended block confirmation interval.

The proposed CNN will address these issues by employing a method known as one confirmation, in which only a single piece of evidence is necessary for a definitive confirmation to be made. The waiting time that has been allocated protects transactions in block 2056 that are still vulnerable to attack. These transactions are still at risk of being attacked. If block 2056 is left or compromised in some other way, there is a chance that the merchant who distributed the products immediately or after the confirmation will not be paid. The research demonstrates that the proposed CNN executes all of the essential checks prior to adding a block to the main chain in its confirmed state. This, in turn, encourages transactions that are concluded in a shorter amount of

time, involve larger amounts of currency, and are transacted for a fee that is lower overall.

4.4 SELFISH MINING

The centralization that Bitcoin mining pools have brought about, miners have a substantial amount of influence over a variety of aspects relating to the altcoin network. Mining that is carried out for the purpose of one own gain is one of the variables that can contribute to a decline in the performance of a network.

According to the findings, there was a period of time during which mining pools frequently produced two or more consecutive blocks, providing evidence of their capability for egotistical mining. This was evidenced by the fact that mining pools frequently produced two or more consecutive blocks. It is exceedingly unsettling for both the other servers on the network and the users of cryptocurrencies to consider the possibility that something like this could take place.

This advantage, which is experienced by miners of all skill levels, is provided by the technique that was recommended by CNN, which helps to mitigate the negative effects that result from selfish mining. It is possible for a miner to intentionally generate blocks behind the scenes without sharing them with the rest of the network.

The miner will announce to the network any newly discovered blocks that can be added to the primary chain when he does so. The result of this is that the other miners forfeit the block and any mining rewards they had accumulated up to that point, giving the miner who is motivated by greed an advantage over the other miners.

The security technique for CNN will only work with blocks that have a height associated with them. When producing numerous blocks in a row, this prevents a miner from being able to ignore the blocks that other miners have produced as competition. The verification check for CNN that has been recommended takes into account a number of factors, one of which is the amount of time needed to generate a block of data. If this is the case, then the test will also be considered invalid for any blocks that have been concealed for a considerable amount of time. Those blocks that have been extracted within the specified amount of time are the only ones that can be considered legitimate.

From the results of Table.1, it is found that the proposed blockchain mechanism achieves higher percentage of accuracy in detecting the four different types of attacks than other methods.

Table.1. Accuracy of CNN on all attacks

Attack	Hash Value	Centralized Blockchain	Ethereum	C2C	Proposed Blockchain-CNN
NCA	10	91.19	91.73	93.01	93.87
	20	91.27	91.82	93.02	93.92
	30	91.29	91.96	93.08	94.03
	40	92.66	93.20	94.06	94.93
	50	92.66	93.21	95.00	95.92
51%	10	89.53	89.63	90.08	90.09
	20	90.06	90.17	90.61	90.62
	30	91.44	91.78	91.89	92.35
	40	92.29	92.67	92.78	93.24
	50	93.95	93.79	93.48	94.42
TI	10	91.42	92.16	93.26	94.12
	20	91.63	92.16	93.48	94.39
	30	91.87	92.40	93.72	94.63
	40	92.83	93.63	94.97	95.11
	50	93.98	94.87	95.19	96.23
SM	10	92.66	93.20	94.06	94.93
	20	92.66	93.21	95.00	95.92
	30	93.50	94.05	95.85	96.78
	40	93.50	94.05	95.85	96.78
	50	94.08	94.64	96.45	97.38

Table.2. Computational Complexity of CNN on all attacks

Attack	Hash Value	Centralized Blockchain	Ethereum	C2C	Proposed Blockchain-CNN
NCA	10	3.90	3.66	3.09	2.71
	20	3.86	3.62	3.09	2.69
	30	3.85	3.56	3.06	2.64
	40	3.25	3.01	2.63	2.24
	50	3.25	3.00	2.21	1.81
51%	10	4.63	4.59	4.39	4.39
	20	4.40	4.35	4.16	4.15
	30	3.79	3.64	3.59	3.38
	40	3.41	3.24	3.20	2.99
	50	2.68	2.75	2.88	2.47
TI	10	3.80	3.47	2.98	2.60
	20	3.70	3.47	2.88	2.48
	30	3.60	3.36	2.78	2.38
	40	3.17	2.82	2.23	2.16
	50	2.67	2.27	2.13	1.67
SM	10	3.25	3.01	2.63	2.24
	20	3.25	3.00	2.21	1.81
	30	2.88	2.63	1.83	1.42
	40	2.88	2.63	1.83	1.42
	50	2.62	2.37	1.57	1.16

From the results of Table.1, it is found that the proposed disturbed blockchain mechanism achieves reduced computational complexity in detecting the four different types of attacks than other methods.

5. CONCLUSION

In this article, we propose the design of a distributed ledger that utilises a convolutional neural network as a layer of defence against intrusions carried out by malicious actors. The proposed method is tested on four different types of attacks that include n

confirmation attack, 51% attack, transaction issues, and selfish mining. The result of simulation shows that the proposed method achieves better traffic flow than the existing methods. It is possible to identify attacks with a higher degree of precision and educate the CNN routers to recognize them when they occur.

REFERENCES

[1] A. Hassanzadeh, R. Stoleru and J. Chen, "Efficient Flooding in Wireless Sensor Networks Secured with Neighborhood Keys", *Proceedings of International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 119-126, 2011.

[2] E. Fadel, V.C. Gungor, L. Nassef, N. Akkari, M.A. Malik, S. Almasri and I.F. Akyildiz, "A Survey on Wireless Sensor Networks for Smart Grid", *Computer Communications*, Vol. 71, pp. 22-33, 2015.

[3] M. Shobana and S. Ramya, "An Optimized Hybrid Deep Neural Network Architecture for Intrusion Detection in Real-Time IoT Networks", *Transactions on Emerging Telecommunications Technologies*, Vol. 33, No. 12, pp. 4609-4614, 2022.

[4] R. Ch and S. Ramachandran, "Robust Cyber-Physical System Enabled Smart Healthcare unit using Blockchain Technology", *Electronics*, Vol. 11, No. 19, pp. 3070-3074, 2022.

[5] Y. Kumar and S. Gupta, "Effectiveness of Machine and Deep Learning for Blockchain Technology in Fraud Detection and Prevention", *Proceedings of International Conference on Applications of Artificial Intelligence, Big Data and Internet of Things in Sustainable Development*, pp. 287-307, 2023.

[6] A. Bhandari and F. Kamalov, "Machine Learning and Blockchain Integration for Security Applications", *Proceedings of International Conference on Big Data Analytics and Intelligent Systems for Cyber Threat Intelligence*, pp. 129-173, 2023.

[7] K.T. Selvi and R. Thamilselvan, "Privacy-Preserving Healthcare Informatics using Federated Learning and Blockchain", *Proceedings of International Conference on Healthcare 4.0*, pp. 1-26, 2022.

[8] R. Chaganti and V. Ravi, "A Survey on Blockchain Solutions in DDoS Attacks Mitigation: Techniques, Open Challenges and Future Directions", *Computer Communications*, Vol. 78, pp. 1-13, 2022.

[9] R. Akter and D.S. Kim, "Iomt-Net: Blockchain Integrated Unauthorized UAV Localization using Lightweight Convolution Neural Network for Internet of Military Things", *IEEE Internet of Things Journal*, Vol. 87, No. 1, pp. 1-14, 2022.

[10] Q. Abu Al-Haija, "Detection of Fake Replay Attack Signals on Remote Keyless Controlled Vehicles using Pre-Trained Deep Neural Network", *Electronics*, Vol. 11, No. 20, pp. 3376-3383, 2022.