Vol. 06, No. 4 (2024) 1551-1560, doi: 10.24874/PES06.04.014

Proceedings on Engineering Sciences

www.pesjournal.net

CULTIVATING RESILIENCE: A TRANSFORMATIVE APPROACH TO ENHANCING CLOUD DATA SECURITY WITH TRANSFORMER-BASED TECHNIQUES

Gantela Prabhakar [1]
Bobba Basaveswara Rao

Received 12.04.2024.
Received in revised form 24.09.2024.
Accepted 09.10.2024.
UDC –004.056.5:004.76

Keywords:

Data Centres, Blockchain Technology, Healthcare System, Analytic Neural Process (ANP), Cyber-Attacks

A B S T R A C T

Data centres have grown drastically in size and in number as the digital economy has proliferated. For the advancement of society and the economy, data centres are becoming increasingly important. But even a little period of data centre downtime can be extremely harmful. Secure management of the physical infrastructure of data centres is essential to resolving this problem. A decentralized approach to healthcare systems is also made possible by blockchain technology, which gets rid of some of the drawbacks of centralized systems like single points of failure. Currently, a number of enhanced resilience security solutions using blockchain and ANP (Analytical Neural Processes) techniques have been presented to improve the security of transformation-based technologies. ANP finds false data and recognizes harmful data measured by medical sensors. For the Internet of Things (IoT) and Cyber Physical Systems (CPS), the development of defences against diverse cyber threats is advancing. Leveraging cloud environments to discover harmful code may not be a practical strategy in the future as malicious code grows in prevalence and there are no established techniques for identifying malicious code. Therefore, before the fog layer processes the data, transformation-based systems can identify and stop cyber-attacks. Additionally, it makes use of a blockchain network at the fog layer to guarantee data integrity and privacy by preventing data modification. Experimental findings demonstrate that the ANP and block chain models deliver what is promised. Additionally, the Transformer Neural Network (TNN) model's accuracy is 99.99% according to the F1 score accuracy indicator.

1. INTRODUCTION

In the fast-evolving digital environment, cloud services will be widely used by 2024, ushering in a time of convenience and innovation for all sectors of society. However, the urgent task of securing cloud-based data security also comes with this innovation (Praneetha et al., 2024). Protecting sensitive information has become crucial as businesses use cloud computing for data analysis, distant operations, and other uses. To improve cloud data security and uphold the confidentiality and integrity of important data assets, the proposal

[1] Corresponding author: Gantela Prabhakar
Email: gantelaprabhakar@gmail.com

investigates a novel strategy for utilizing cutting-edge deep learning technology, particularly transformers.

The construction of new infrastructure has recently been fuelled by the explosive growth of the digital economy, big data, and information technology. When we talk about new infrastructure, we mean infrastructure that is supported by technical advancement (Almalki et al., 2022), like 5G base stations (Alsulami et al. 2022), which are built on information networks. The new infrastructure will increase the connection between the physical and digital worlds, as opposed to the present infrastructure, which connects physical areas (Kumar & Sharma, 2022). It serves as the cornerstone of the digital economy and is crucial to high-quality development and digital transformation in conventional industry (Skrodelis & Romanovs, 2022). With rising worldwide investment in digital infrastructure and accelerated digitalization of conventional industries becoming more significant in many countries, there is growing interest in new infrastructure, especially in the post-COVID-19 era. Data centres are a crucial component of new infrastructure because digitalization is one of its fundamental components (Maray et al., 2022). Statistics and projections indicate that by 2025, there will be 163 ZB of global data, raised from 16.1 ZB in 2016 (Alsulami et al., 2022). Economic activity depends more and more on data centres, and even brief disruptions can cause significant losses in revenue (Fu et al., 2023; Zhang et al., 2022). Unplanned data centre downtime costs $8851 per minute on average (Meng et al., 2023). Therefore, it is more crucial than ever that data centres run safely and efficiently (Martins et al., 2022). Several researches have been done to improve IoT security utilizing various technologies, including blockchain and machine learning (Somasekaram et al., 2022). Non-map learning, map learning, and reinforcement learning are three machine learning categorization techniques that researchers frequently use. The alternative to map learning is non-map learning because we are unsure of the model's outcome. Additionally, non-map learning's output classes are not labelled during training. Intrusion Detection Systems (IDS) are frequently used to scan data and separate the good from the bad using a binary classification technique (Shah & Pareek, 2022). In contrast, Industrial Control systems (ICS) are used to identify cyber-attacks types by detecting different data types. Machine learning models built on blockchain and artificial neural networks can be used to reduce cyber-attacks on IoT devices.

There are a few studies on infrastructure security management in industrial systems and urban construction, but there aren't many on data centres infrastructure, which needs more attention (Susanti et al., 2023). Data centre infrastructure management (DCIM) systems are a subject of interest to some researchers. Most current research is on rating and managing authentication across topological layers. The traditional security management paradigm, which emphasizes dependability and availability, cannot satisfy security needs since there are uncertainties in managing complex infrastructure systems in data centres. There is a need for evaluation and optimization techniques that include fault tolerance and recovery in addition to general data centres infrastructure assessment, classification, and risk prevention (Schlippe et al., 2023).

As a result, we use the resilience concept to control the infrastructure's security. Infrastructure research is currently making consistent use of resilience theory. The definition of resilience is dynamic, and so are the theoretical foundations that support it (Firoz et al., 2023). The greatest criterion for safety is resilience theory, which is positioned as a new research paradigm for safety scientific study and practice. The main methods used nowadays for qualitative analysis of infrastructure resilience are interviews, questionnaires, etc. with the aid of expert scoring techniques, analytic hierarchy processes, entropy weight methods, etc. to create an infrastructure evaluation index system, or using other measurement techniques. The following is a summary of this paper's significant contributions.

To distinguish between harmful data (cyber-attacks) and healthy data (real-world data) gathered from medical sensors, take resilience-building procedures using ANP.

To improve data integrity and privacy, use block chain-based non-financial application solutions to replicate block chain operations on fog nodes.

We suggest a security framework that combines block chain and ANP's strengths. The usage of ANP boosts the ability to capture data injected during hacks. Block chain ensures data privacy and integrity so that transferred and stored data cannot be altered.

2. METHODOLOGY

2.1 Data Infrastructure Resilience Framework

The following presumptions concerning the data centres' physical infrastructure are made in this study based on Walid Mokhtar Bennaceur's (2020) review of the literature and industry consensus: (a) The electrical subsystem that generates and distributes power, including generators, power transformers, backup power supplies, and other related devices. (b) The temperature-regulating thermal subsystems, such as coolers, ducting, and cooling towers. (c) Systems for management and control that track different types of data. The infrastructure of the data centre is powered by energy that is constantly flowing through it and supporting the IT and cooling systems. The thermal system receives the surplus heat produced by the network system, recycles it for space heating, and returns it to the network system. The cooling subsystem relies on both the electrical and the cooling subsystems to function

effectively, and the electrical subsystem is also necessary for the network subsystem to function. Ecological resilience, traditional engineering resilience, and resilience have all evolved since resilience was first proposed. Four key characteristics of resilience are regarded to be robustness, redundancy, flexibility, and agility. Figure 1 displays the schematic diagram. The combined capacity of an infrastructure system to absorb, resist, recover, and adapt can be used to measure its resilience. The system's capacity to absorb energy is what allows it to get rid of dangers and stop disasters. The system's capacity to lessen the effects of disasters to cut down on system losses is provided by its resistors and capacitors. When a calamity strikes, resilience refers to the capacity to quickly change the environment in order to maintain normal operations. After a tragedy, adaptation aims to improve the system's internal structure in order to better withstand future unstable events.

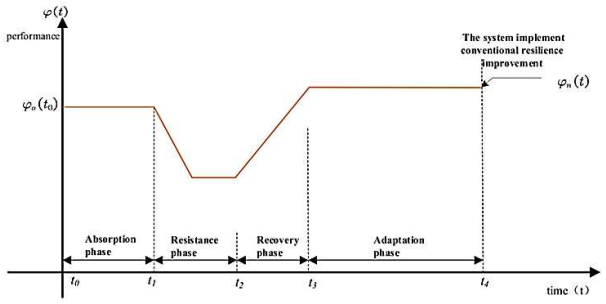

Figure 1. Resilience state diagram

2.2 Transformer Model

Transformer models employ an encoder-decoder structure just like the majority of competing neural sequence conduction models. The decoder outputs the provided continuous representation sequence as (y1 y2 ym), while the encoder maps the input symbol representation sequence (x1 x2 xn) to the continuous representation sequence z (z1 z2 zn). The model's stages are all autoregressive. This means that, with the exception of the input to the first encoder at the bottom of the encoder stack, the output produced by each encoder or decoder serves as the input for the subsequent encoder or decoder. The goal of the converter model is to transform the input feature sequence into the appropriate vector representation. The self-attention mechanism, which uses attention matrices rather than recurrent connections, is the primary distinction between Transformer and RNN.

2.3 Secure cloud for malware worms detection

Data management, communications, media services, storage, computing, artificial intelligence, machine learning, developer tools, security, and other services are quickly becoming part of the new paradigm. Figure 3 shows the different cloud publishing services, models, and users. You can access your data with cloud computing services from any device, at any time, and anywhere. On the other hand, this access option is extremely risky because viruses can be accessed with ease. Cloud malware has the potential to lead to major security problems such login credentials theft, system corruption, virtual device hijacking, identity theft, and system corruption.

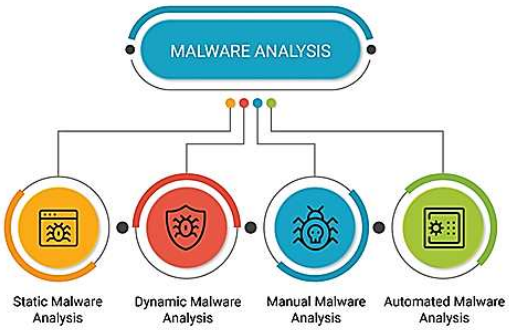

Figure 2. Malware Analysis

According to Inter-cloud, the malware is capable of operating inside virtual devices and stealing user privacy. With methods based on behaviour, signatures, and machine learning, malware in the cloud can be located. Google, Azure, and Amazon Web Services (AWS) are a few of the main cloud service providers (CSPs) that provide cloud-based malware detection and prevention services (Schlippe, 2023). A threat detection service called Amazon Guard Duty monitors activity related to dangerous software detection. Google is currently releasing new techniques to identify risks.

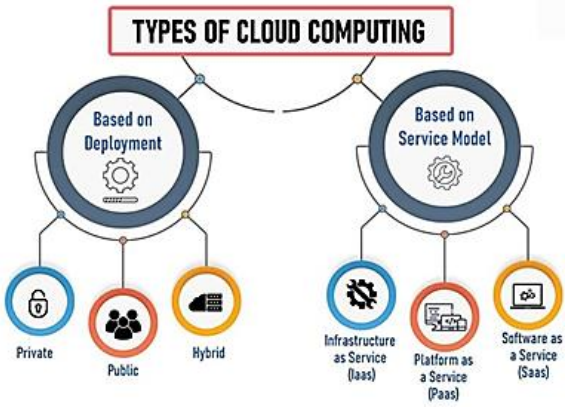

Figure 3. Technologies and services of cloud computing

The process for locating malware at the cloud level is shown in Figure 4. Other methods of data acquisition are widely used by people, including email, HTTP, media, instant messaging, P2P, PCs, mobile phones, and the Internet of Things. These users get file reports and cloud storage for their files. Cloud-based signature-based detection systems identify malware by comparing observed patterns. While quickly and effectively detecting known malware, signature-based approaches are unable to identify brand-new malware.

Malware is identified based on its behaviour using anomaly-based detection techniques. This approach has the potential to discover new dangerous software, but it also increases the risk of false positives. Machine learning-based malware detection techniques have been studied in the past, and this approach has shown to be highly effective. Machine learning-based malware detection techniques use LSTM (Firoz et al., 2023), support vector machines, and parse trees among other algorithms. This strategy will only be effective if the model can be trained with enough data and strong accounts. On the other side, scaling problems exist with machine learning-based malware detection methods.

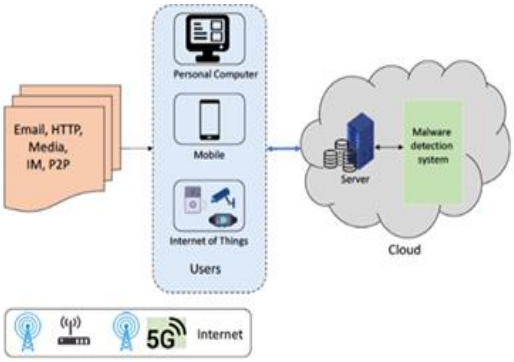

Figure 4. Cloud-based malware detection system

3. BLOCKCHAIN

This study makes use of block chain technology. This is because it uses cutting-edge technology to address difficulties with centralization, privacy, and trust. Block chain is the recognized technology for the Bit coin and other crypto currencies. Block chain can be compared to a database that stores transactions decentralized and without the involvement of third parties using a peer-to-peer (P2P) network. The block chain's distributed architecture reduces the likelihood of single points of failure while increasing system availability and reliability. The block chain model used in this investigation is depicted in Figure 5. Variable-length data are encrypted with fixed-length encrypted data using the mathematical operation of hashing. In order to replace trust in already functional systems, hashes are utilized. As a result, we only have data from the prior block. On order to ensure that the data on fog nodes cannot be altered, block chain technology uses the block chain hash function to create safe links between blocks. The longest legitimate block chain will often be chosen by a computer when it tries to join a block chain network. Because an attacker can raise the number of blocks created to draw in more members, controlling block growth is crucial. For precisely this reason, we use the Proof of Work (PoW) algorithm to raise the mining difficulty and employ a mining difficulty that causes the creation of new blocks to proceed more slowly. Controlling the rate of block mining is essential as a result. An arbitrary number called a nonce is what miners use to calculate a hash. Additionally, since the nonce is only used once, check the hash. Transactions are actions produced by system users. In addition, depending on the block size, each block contains a huge number of transactions, ranging from 1 to N. A transaction is broadcast to all network nodes after it has been started. When a new transaction is received, every node confirms it and records it in the ledger.

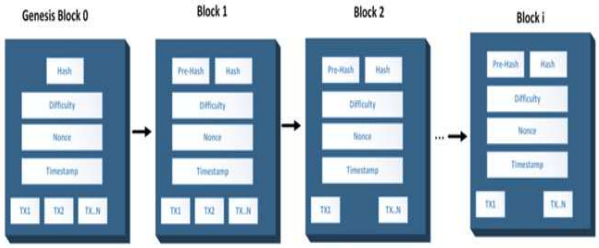

Figure 5. Blockchain Scheme

3.1 Blockchain Scheme

This section explains how the blockchain system was used in this investigation. Python is used to implement BlockchainMain(), BlockchainClass(), and BlockClass() algorithms. We introduce the primary functional stages of the blockchain model used in this work, based on the fundamental paradigm of public blockchain architecture first presented in Algorithm 1. Declare two lists, rows, and blocks first. According to the number of IoMT devices used in the blockchain network, the block list stores record fragments, whilst the row list keeps entire dataset entries. The number of simulated IoMT devices determines the value of the chunk_size variable, which is set to N. The dataset's CSV file should now be loaded. After that, the data is separated into pieces. The fundamental steps of blockchain technology may then be seen in the loop that runs from line 7 to line 14. Line 8 invokes the Algorithm 2 blockchain class. Line 10 invokes the Algorithm 3 device class. For the device object, a new thread is created on line 12. Line 13 finally stops additional thread calls until the thread that is now processing is finished.

Algorithm 1: BlockchainMain()

1: Create the variables' initial values given as rows and chunk as empty list. Declare the chunk_size variable as N.
2: From the Comma Separated Values file, the rows are copied into the rows list.
3: Share the values in the rows variable into numerous percentages depending on the chunk_size.
4: for each of the chunk perform the following:
(i) Call BlockchainClass as Blockchain = BlockchainClass().
(ii) Call device class as Device object = DeviceClass(blockchain,chunk).
(iii) Start a new device object low-weight process (LWP).
(iv) Look out for the completion of each device LWP.

5: End for
6: End

The blockchain class's implementation is shown in Algorithm 2. At first, only one crucial section of the code may be accessed at once, thanks to an object lock established as a thread's lock. Then create a list of the blocks that contain the block values. The list's first block, the Genes block, is stored first; therefore its previous hash value is zero. Make a transaction list containing the transactions for each block that follows. The transaction list is then updated by the Broadcast_transaction function, locking it to prevent concurrent access. The new_block object is created by the mine_block function and contains the list of transactions, the hash of the previous block, and the degree of difficulty. The next step is to invoke the mining function, which is covered in Algorithm 3. The algorithm finally outputs a new_block object.

Algorithm 2: BlockchainClass()

1: Create an entity "lock" with LWP system
2: Set the difficulty = 1
3: Initialize the blocks list = [Genesis_block,…]
4: Initialize the transactions list as empty
5: add_block (block)
6: if block.previous_hash == blocks[last].hash
    (i) add the block to the blockslist
    (ii) return True
7: else
    (i) return False
8: broadcast_transaction (transaction)
9: Use thread lock object
10: transactions = [transaction]
11: mine_block ()
12: new_block = BlockClass (transactions, blocks[last].hash, difficulty)
13: new_block = mine ()
14: return new_block

Algorithm 3 represents the blockclass() used to produce a block in the network. These characteristics apply to the class:

- Data: Information contained in the block.
- Previous_hash: the block chain's previous block's hash value.
- Hash: the block's current hash value.
- Difficulty: The level of challenge involved in mining the block.
- Once: An arbitrary number that is used to modify the block's hash value while it is being mined.
- The block's timestamp indicates when it was mined.

The mining function expands the blockchain network with new blocks. Old hashes are required to link new blocks with old ones in this process.

Algorithm 3: BlockClass()
1: Initialize the entities such as statistics, data, previous_hash, hash, difficulty, nonce, and timestamp
2: mine ()
    (i) Calculate hash using sha256

The categories of devices are described by Algorithm 4. The device class replicates the simultaneous operation of numerous devices by deriving from the thread function. The device must generate blocks with at least 35 transactions per block (customizable). However, the block will be mined when there are 35 transactions.

Algorithm 4: DeviceClass()

1: Define a class named "device" that inherits from the algorithm1 with the function thread
2: Use the following object: blockchain, rows
3: Initialize pending_transactions = 0
4: create a dictionary called transaction[]
5: run()
8: for each row in rows
    (i) if pending_transactions < 35
        transaction = [data]
        broadcast_transition (transaction)
        pending_transactions += 1
    (ii) else
        block = mine_block()
        pending_transactions = 0
9: End

4. EVALUATION INDEX MODEL BASED ON ANP METHOD

AHP (Analytical Hierarchy Process), SD (System Dynamics) modelling, Bayesian networks, DEMATEL-ISM approach, and ANP (Analytical Network Process) are some of the techniques used for recovery resilience evaluation. Relationships in complicated, interdependent adaptive systems are typically studied using SD. However, it is challenging to simulate system heterogeneity across infrastructures and vast volumes of internal data are needed to calibrate the model's many parameters and traits. Even though Bayesian networks efficiently calculate the likelihood of executing an assessment, they do not consider relationships between overlapping elements, and AHP is ineffective at explaining complicated interconnected systems, which raises the danger of inaccurate risk estimates. When compared to methods like AHP, the ANP method can more correctly reflect the dependency and influence within the reference group in the network structure model. Some internal operational data is challenging to collect since a data centre's physical infrastructure comprises connected infrastructure subsystems. In this situation, the ANP method is appropriate for physical infrastructure resilience assessment models for data centres since it clearly and concisely describes the interaction between components. In academics, there are lots of examples of success. The assessment of infrastructure resilience especially that of

interconnected critical infrastructure, resilient urban infrastructure, and resilience to both local earthquakes and urban floods, has made substantial use of the ANP technique. The subjective weights are established using the ANP approach. The top-down dependencies of the analytical hierarchy process (AHP) are replaced by the dependency between elements in the network analysis technique (ANP), and the original single hierarchical structure is replaced by a feedback network between internal elements, making it easier to handle. The following are the precise steps for solving scientific decision-making issues in complex systems: (a) Create a model for the structural layers based on the relationship between the components of the control layer (goals and standards) and the network layer (indicators), experts create a network relationship diagram. A one-way or two-way arrow denotes each relationship. (b) Setting regional priorities and creating a judgment matrix: Based on the structural hierarchical model, the expert group assesses a pairwise comparison matrix of the link between various factors. Conduct a consistency check after collecting the decision matrix findings, and the check coefficient Cr is less than 0.1:

$$CI = \frac{\lambda_{max} - n}{n-1} \quad (1)$$

$$CR = \frac{CI}{RI}$$

The consistency index (CI), maximal eigenvalue (max), judgment order (n), and random consistency index (RI) are all used in the formula.

Using the criteria of evaluation of the control layer elements in super matrix calculations, the sub-criteria of each element in the element group Bj are used to create the weight matrix Fij. The control criterion as is then used to obtain the super matrix Fs.

$$F_{ij} = \begin{bmatrix} f_{i1}^{(j1)} & f_{i1}^{(j2)} & \cdots & f_{i1}^{(jn_j)} \\ f_{i2}^{(j1)} & f_{i2}^{(j2)} & \cdots & f_{i2}^{(jn_j)} \\ \vdots & \vdots & \ddots & \vdots \\ f_{in_i}^{(j1)} & f_{in_i}^{(j1)} & \cdots & f_{in_i}^{(jn_j)} \end{bmatrix}$$

$$F_s = \begin{bmatrix} F_{11} & F_{12} & \cdots & F_{1n} \\ F_{21} & F_{22} & \cdots & F_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ F_{n1} & F_{n2} & \cdots & F_{nn} \end{bmatrix}$$

$$\overline{F_S} = (\overline{F_{ij}}), \overline{F_{ij}} = m_{ij}(F_{ij}), i = 1, 2, \ldots, n$$

$$\overline{F_S}^{\infty} = \lim_{t \to \infty} \overline{F_S}^{t} \quad (2)$$

where $\left[f_{i1}^{(jl)}, f_{i2}^{(jl)}, \ldots, f_{in_i}^{(jl)}\right]^T$. The elements of the normalized weighting matrix Ms of the factor group judgment matrix under the control criterion are illustrated by the normalized eigenvector generated by contrasting each element in the element group Bj.

Calculation for group decision-making: We calculate the final result by geometrically averaging the findings of many specialists in order to ensure the accuracy of the results. The ultimate priority value can be calculated by taking the geometric mean of each indication.

5. RESULT AND DISCUSSION

Our remedy blends blockchain and ANP models. ANP is in charge of identifying cyber-attacks using information gathered by medical sensors. The blockchain concept disseminates and stores data, identifying and counteracting cyber-attacks at the fog layer. Therefore, before sending common or normal data to the blockchain model, the ANP model will first detect and delete harmful data. In other words, after filtering the data with the ANP model, we manage and store the regular or common data, CSV (Comma Separated Values) files extracted from the dataset, using the blockchain method. To determine the ANP model's correctness, evaluate it using a confusion matrix.

The figure depicts the confusion matrix's overall form. An accurate positive (TP) indicates that the ANP correctly identified typical sensor data. Real talk indicates that ANP may classify malicious data as an anomaly. False positive (FP) indicates that ANP misclassifies benign sensor data as normal. FN (false negative) describes the situation where ANP misclassifies malicious data as good data.

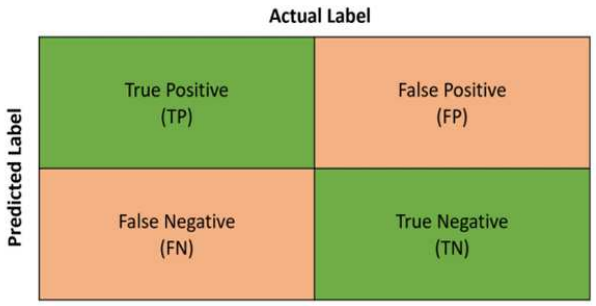

Figure 6. Confusion matrix

5.1 Measurement Model: Reliability and Validity

The PLS output produced by the measurement model is seen in Figure 7. We used composite reliability values in addition to the reported Cronbach's alpha values to evaluate the measurement model's internal consistency. The composite reliability values, which ranged from 0.818 to 0.968 for all constructs, showed acceptable levels of internal consistency. Due to low factor loadings, two resilience items (RE2 and RE4) and supervisor support items (e.g., SS4) were eliminated. The setup with an elasticity value of 0.548 was the only one to not achieve factor loadings over the 0.600 cut-off. For this project, the average variance extracted (AVE) stayed at acceptable levels.

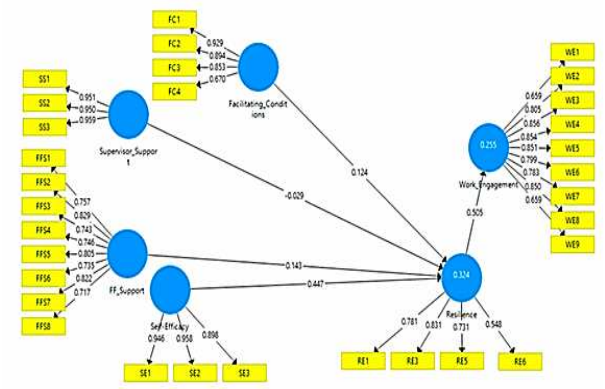

Figure 7. Measurement model

Researchers frequently base their conclusions only on categorization accuracy. Therefore, equation (4) is used to determine the F1 score. Calculating precision and recall before calculating the F1 score is straightforward and is demonstrated in equations (2) and (3). Determine the ANP model's precision rate, recall rate, and F1 score index. The model earned an F1 score of 98.63%, a precision of 99.72%, and a recall of 98.46%.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \times 100$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \times 100$$

$$\text{F1-score} = \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \times 100 \quad (3)$$

On the basis of the afore-mentioned accuracy indicators, we can see that the TNN model has acquired a high level of accuracy. TNN can therefore be applied as a detection model for these studies. We contrasted our findings with those of (Alsemmeari et al., 2023) to ensure that the TNN model was performing as expected. In order to assure a fair comparison, we chose to compare our findings with those of (Alsemmeari et al., 2023), whose authors used the same dataset as this work. Table 3 displays various detection models for cyber-attacks that have been created using machine learning algorithms. Comparing the suggested TNN to the other detection models, it produced the best results in terms of classification accuracy metrics. In terms of classification accuracy, precision, and F1 score outcomes, Naive Bayes (NB) scored the worst whereas TNN performed the best across the board. TNN's findings were closely matched by KNN (K-Nearest Neighbour's), Random Forest (RF), Ada boost (AB), Logistic Regression (LogR), and Decision Tree (DT). TNN performs better than other ML models overall, according to Table 3's metrics for precision, recall, and F1 score. The RF is the model that performs the best for us.

Table 1. Accuracy in comparison with other security techniques

Detection model	Accuracy	Precision	Recall	F1-score
NB	52.24	79.72	98.75	67.51
KNN	98.64	98.68	98.69	98.59
RF	98.53	98.74	98.8	98.65
AB	98.53	98.53	98.45	98.47
DT	98.52	95.28	9.35	93.71
TNN	98.51	98.64	98.3	98.64
Proposed ANP	99.84	99.72	98.46	98.63

Examples of two successive blocks of a block chain network recorded in Python are displayed in Figures 8 and 9 as JSON output. JSON, short for JavaScript Object Notation, is a text-based format for transferring and storing data. Any programming language can communicate data between computers using the language-neutral data type JSON. JSON can be used to facilitate peer-to-peer data sharing and enhance system compatibility. Figure 8 displays the data that was taken from the CSV file and filtered using the ANP model. The fundamental public block chain design paradigm that Satoshi Nakamoto first described in his article "Bitcoin: A Peer-to-Peer Electronic Cash System" is the foundation upon which the actual block chain ecosystem and its implementation are built. Figure 8 shows an example block with the transaction parameters, difficulty, nonce, hash, and prior hash. The size of blocks affects both the volume and the kind of transactions. In this example, each block can process up to 35 transactions; however the user can alter this depending on the ability of their IoMT device. Figure 9 depicts the second block sample. Because both blocks are sampled at the same time, it is clear that the Previous_hash parameter correlates with the hash value in Figure 8.

```
{
'hash':'09g245cv6dfs6hd76jdjd88423e8j44jsbd67
jdwk345sjnadr87ssmmxz23kwift92laksb12l'
'previous_hash':
'45iiuw76bkjfkjd34akjdjj22khkhk87jbjbkw08knci
h12bkebf44bwefkj23jhbfkd65kjbqwk9g'
'difficulty':1,
'nonce':6,
'timestamp':6473827362.73728291
Transactions:[
                {
                        TX(1)
                }
                …       ….      ….
                {
                        TX(N)
                }

        ]

'
```

Figure 8. Example 1 denoting the Evidence of a Block in the Block chain

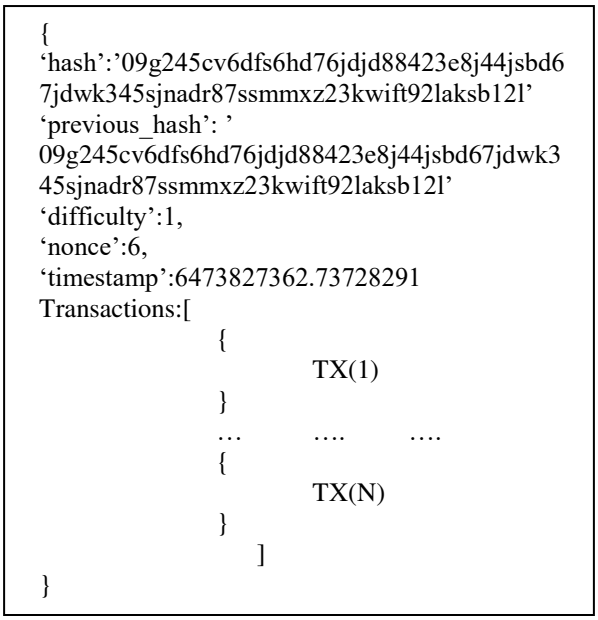

Figure 9. A Block sharing the data from the previous Block

6. CONCLUSION

The complexity of IoT systems and their security flaws, which make them susceptible to hacker attacks, make cloud data security a crucial issue. By combining block chain with ANP (Analytical Neural Processes) models, we suggest strong security architecture in this article. With regard to assaults on sensor data, the ANP model is specifically utilized to recognize malicious data as well as to detect and stop them. We employ the fog layer's block chain model after ANP testing to make sure the data stored on the device is accurate. The findings demonstrate that the ANP model performs superior to more established techniques like NB, KNN, RF, AB, and TNN, reaching high accuracy, accuracy, and F1 score indicators as well as flawless replication performance. Additionally, the proposed block chain-based simulation system has produced the anticipated results and allows for the customization of its settings. Trade-offs' proposed block chain-based solution prioritizes security over performance. Future research will compare the system's performance against private block chain implementations.

References:

Almalki, J., Al Shehri, W., Mehmood, R., Alsaif, K., Alshahrani, S. M., Jannah, N., & Khan, N. A. (2022). Enabling blockchain with IoMT devices for healthcare. *Information*, *13*(10), 448. https://doi.org/10.3390/info13100448

Alsemmeari, R. A., Dahab, M. Y., Alsulami, A. A., Alturki, B., & Algarni, S. (2023). Resilient Security Framework using TNN and blockchain for IOMT. *Electronics*, *12*(10), 2252. https://doi.org/10.3390/electronics12102252

Alsulami, A. A., Abu Al-Haija, Q., Alqahtani, A., & Alsini, R. (2022). Symmetrical simulation scheme for anomaly detection in autonomous vehicles based on LSTM model. *Symmetry*, *14*(7), 1450. https://doi.org/10.3390/sym14071450

Alsulami, A. A., Abu Al-Haija, Q., Tayeb, A., & Alqahtani, A. (2022). An intrusion detection and classification system for IoT traffic with improved data engineering. *Applied Sciences*, *12*(23), 12336. https://doi.org/10.3390/app122312336

Firoz, N., Beresteneva, O. G., Vladimirovich, A. S., Tahsin, M. S., & Tafannum, F. (2023, February). Automated text-based depression detection using hybrid ConvLSTM and Bi-LSTM model. In *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)* (pp. 734-740). IEEE..https://doi.org/10.1109/ICAIS56108.2023.10073683

Fu, H., Zhu, H., Xue, P., Hu, X., Guo, X., & Liu, B. (2023). Eye-tracking study of public acceptance of 5G base stations in the context of the COVID-19 pandemic. Engineering, Construction and Architectural Management, (ahead-of-print). https://doi.org/10.1108/ECAM-10-2021-0946

Kumar, R., & Sharma, R. (2022). Leveraging blockchain for ensuring trust in IoT: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(10), 8599-8622. https://doi.org/10.1016/j.jksuci.2021.09.004

Maray, M., Alghamdi, M., & Alazzam, M. B. (2022). Diagnosing cancer using IoT and machine learning methods. *Computational Intelligence and Neuroscience, 2022*, 9896490. https://doi.org/10.1155/2022/9896490

Martins, J. B., Carim Jr, G., Saurin, T. A., & Costella, M. F. (2022). Integrating Safety-I and Safety-II: Learning from failure and success in construction sites. *Safety science*, *148*, 105672. https://doi.org/10.1016/j.ssci.2022.105672

Meng, J., Zhu, Y., & Han, Y. (2023). Can 'new'infrastructure become an engine of growth for the Chinese economy? *Journal of Chinese Economic and Business Studies*, *21*(3), 341-362. https://doi.org/10.1080/14765284.2022.2036571

Praneetha, N., Rao, S. S., Maheswara Rao, V. V. R., Silva Rao, I S.., & Brahmanandam, P. S. (2024). Identity-based privacy-preserving anonymous authentication access control for secure cloud computing. *Proceedings on Engineering*, *6*(3), 1327-1336. doi: 10.24874/PES.SI.24.03.015

Schlippe, T., Stierstorfer, Q., Koppel, M. T., & Libbrecht, P. (2022, July). Explainability in automatic short answer grading. In *International conference on artificial intelligence in education technology* (pp. 69-87). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-8040-4_5

Shah, N., & Pareek, J. (2022, November). Automatic evaluation of free text answers: A review. In *International Conference on Advancements in Smart Computing and Information Security* (pp. 232-249). Cham: Springer Nature Switzerland.https://doi.org/10.1007/978-3-031-23095-0_17

Skrodelis, H. K., & Romanovs, A. (2022, October). Synthetic network traffic generation in iot supply chain environment. In *2022 63rd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)* (pp. 1-5). IEEE. https://doi.org/10.1109/ITMS56974.2022.9937126

Somasekaram, P., Calinescu, R., & Buyya, R. (2022). High-availability clusters: A taxonomy, survey, and future directions. *Journal of Systems and Software*, *187*, 111208. https://doi.org/10.1016/j.jss.2021.111208

Susanti, M. N. I., Ramadhan, A., & Warnarsa, H. L. H. S. (2023). Automatic essay exam scoring system: a systematic literature. *Procedia Computer Science*, *216*, 531-538.. https://doi.org/10.1016/j.procs.2022.12.166

Zhang, C., Zhang, M., & Xiao, C. (2022). From traditional infrastructure to new infrastructure: a new focus of China's Belt and Road Initiative diplomacy?. *Eurasian Geography and Economics*, *63*(3), 424-443. https://doi.org/10.1080/15387216.2022.2039740

Gantela Prabhakar
Department of Computer Science Engineering,
Acharya Nagarjuna University,
Guntur, Andhra Pradesh,
India
gantelaprabhakar@gmail.com
ORCID 0000-0001-9167-8842

Bobba Basaveswara Rao
Department of Computer Science Engineering,
Acharya Nagarjuna University,
Guntur, Andhra Pradesh,
India
Bobbabrao62@gmail.com
ORCID 0000-0003-4287-0891