iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: V Month of publication: May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71451

Cyber Security Framework to SME Applications using Block Chain Integrated Convolution Neural Network for Authorizing and Classifying Level of Access to Distributed Data

Aravinda Kumar Appachikumar
Independent Researcher

Abstract: Small and medium size enterprises are becoming critical in driving innovations and economic growth in digital economy. However SME growing reliance on digital technologies exposes to cybersecurity attacks such as data breaches and phishing attacks and ransoms ware attack leads to greater financial loss, reputational challenges and business closure. In order to protect the SME business operation and their process data against cyber security attacks, many researchers applies emerging technologies such as Artificial intelligence and blockchain. Despite of many advantages of the implementing blockchain towards decentralization and transparency while artificial intelligence approaches towards predicting and classifying attacks, it is mandatory to establish an integrated solution to enhance security of the distributed servers of the SME. In this paper, blockchain integrated convolution neural network is designed to predict and classify the user with user level to secure access of data in blockchain enabled distributed servers. Initially Blockchain is established to business process data of the SME with immutable ledger for fostering trust and transparency. Convolution Neural Network establishes access control mechanism to blockchain distributed server to authenticate user against unauthorized access and predict the user level of access to data. In Blockchain, trusted nodes can validate the transaction and request for data access through generation of new transaction by user. User request is logged in blockchain which leads to data transparency and support detect the malicious user to retrieve data in the blockchain. Convolution Neural Network processes the log data of blockchain which contain user request. The user requests were processed in the convolution layer to extract the spatial temporal features. Extracted feature were embedded as spatial embedding and temporal embedding and applied to Max pooling layer. Max pooling layer reduces spatial dimension of the feature map. Spatially reduced feature map is applied to fully connected layer which contains activation function and softmax function to authenticate user and categorize the user with level of access to the data. Experimental analysis of the model is performed in the blockchain platform named as hyperledger which enables convolution neural network for authenticate user and categorize level of user towards data access. Performance analysis of the model proves that model is more secure and accurate against detecting authorized user and classifying user on their level access to data.

Keywords: Blockchain, Artificial intelligence, Convolution Neural Network, Hyperledger Block chain, Small and Medium Enterprise (SME), Business Transformation, Access Control.

I. INTRODUCTION

Small and Medium Enterprise drives more innovation, employment and economic growth of many economies worldwide. Due to exploration of technologies, SME has started adapting to digital technologies to reach global market on increase their operations and improving customer expectations. Especially technologies like cloud computing, Internet of Things, Blockchain and Artificial Intelligences benefits SME to more extent. However growing reliance of SME’s on digital technologies will give rise to various cybersecurity attacks which impacts in larger financial loss and business closure. Traditionally many researchers has employed machine learning and deep learning architectures to detect and prevent attacks and blockchain technologies provides increased security to their outsourced business data with greater transparency separately[1].

Blockchain is classified into public blockchain, private blockchain, consortium blockchain and blockchain as a service. Hence it leads to more complexity in verifying data integrity and challenges in establishing strong trust and privacy[2]. Type of blockchain is as follows

- Public Blockchain: It is permission less system which allows to download blockchain code and make modification and to utilize according to requirement.
- Private Blockchain: It is organized by organization which is permissioned system where user and participants are preapproved for read and write operations
- Consortium Blockchain: It is organized and operated by group of organization
- Blockchain as a service: Cloud service providers are increasing focusing on the blockchain and it allows its user to utilize according to requirement

Artificial intelligence aims to build cyber security architecture to data center. Machine learning is subset of the AI uses statistical methods to detect and classify the cyber-attacks. It builds models based on input and makes prediction without any explicitly programmed function to the specified attack. Deep learning is a subset of machine learning which involves neural network with several layers enabling more complex attack pattern to be distinguished[3]. Thus, it becomes mandatory to integrate blockchain and AI to provide increased trust and reduced complexity in verifying data integrity.

In this paper, a new blockchain integrated convolution neural network model is designed to store business data of SME in the blockchain ledger and to predict and classify the user with different user level to secure data access of ledger information[4]. Blockchain enabled to SME business data with immutable ledger for fostering trust and transparency and Convolution Neural Network[5] enabled to offer access control mechanism to secure data access through various layer of the model. Further trusted user or node in blockchain can validate the transaction and request for data access through generation of new transaction. Generated new transaction is logged in blockchain which help to detect and classify the trust user or node for data access through convolution neural network layers.

Rest of the article is organized into following sections; section 2 represents review of literature on blockchain enabled cyber security frameworks and AI enabled cyber security frameworks with its functional steps and performance results has been analyzed with its benefits and challenges, section 3 defines a new integrated design of blockchain and convolution neural network towards storage of the business data and to predict and classify the user with different user level to secure data access in blockchain ledger. Section 4 mentions experimental analysis and performance analysis of the proposed model against the conventional approaches. Finally section 5 concludes the article with major findings and future direction to research followers.

II. RELATED WORK

In this section, review of literature on blockchain enabled cyber security frameworks and AI enabled cyber security frameworks with its functional steps and performance results has been analyzed with its benefits and challenges is as follows

A. Blockchain enabled cyber security frameworks to SME

Blockchain enabled cyber security frameworks has been modeled and implemented in large extent by many researchers.

- Kamran habib Khan et.al presented a Blockchain enabled zero trust architecture towards continuous authentication across entities for virtual environment. Particular architecture decentralizes and imposes authentication intensity of communication transparently which computes intrusion accurately[8]. Detection accuracy is 93.1%
- Ahmed Didouh et.al presented blockchain architecture for management of vehicle communication towards road safety[7]. Particular architecture decentralizes and imposes authentication intensity of vehicle transparently which computes real time traffic accurately. Detection accuracy is 93.1%

B. Artificial Intelligence enabled cyber security architecture to SME

Artificial Intelligence enabled Cyber security architectures to SME has been modeled and implemented in large extent by many researchers.

- Guangming Xian et.al presented a large scale semi supervised deep learning architecture based on local and non-local regularization[6]. Architecture analyzes the cyber traffic data in layer of the model and predicts the attacking traffic and mitigates it from reaching data server. Model detection accuracy is 94.2%
- Ozgur et.al presented a recurrent neural network for detection and classification of the phishing attack in network[9]. RNN uses the hidden layer for process the network data to classify attack and normal traffic to the data server. Model detection accuracy is 93.2%

III. PROPOSED MODEL

In this section, new integrated design of blockchain and convolution neural network towards storage of the business data and to predict and classify the user with different user level to secure data access in blockchain ledger has been performed. Architecture is as follows

A. Blockchain

Blockchain is a decentralized distributed digital ledger which ensures data integrity and transparency. Each block contain list of transactions of SME operations which are linked and secured through cryptographic techniques. Every node in the blockchain contains public and private key pair to encrypt and sign the transactions. Figure 1 represents the architecture of the Blockchain integrated convolution neural network for secure data access against cyber-attacks.

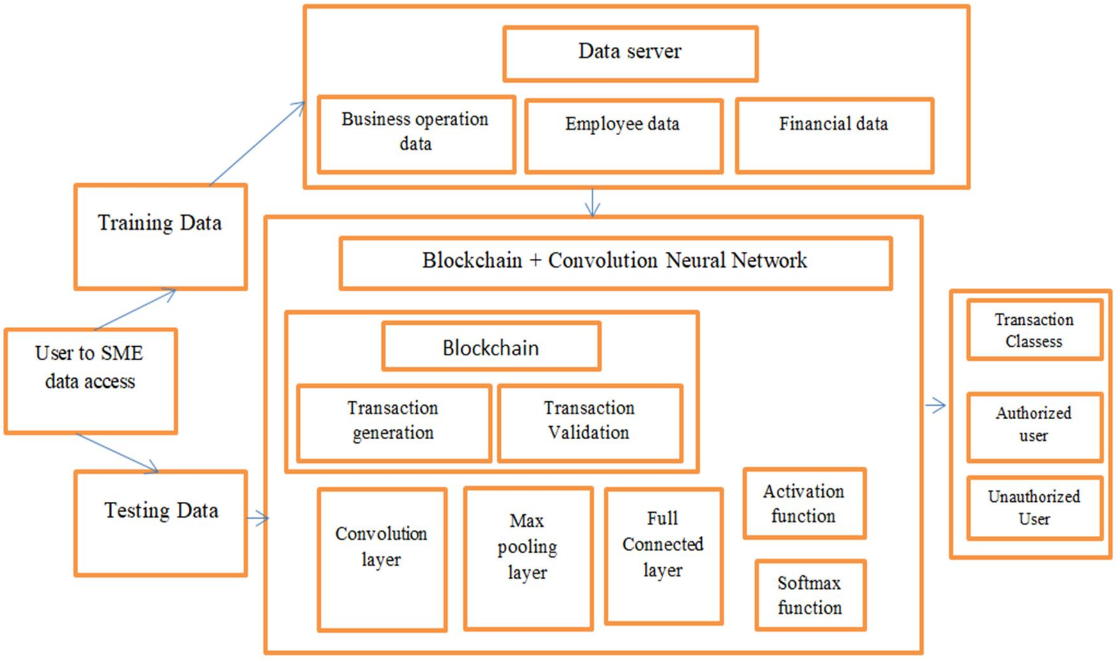


Figure 1: Blockchain Integrated Convolution Neural Network for Secure data access

For acquiring access to data upon user request, blockchain authenticates the user and determines the level of access by modeling and incorporating CNN architecture. It sends results to storage for obtaining access link which is eventually shared with the user. Table 1 represents the entities of the blockchain.

Table 1: Entities of the Blockchain

Entities of Blockchain	Operation
User	Employee of SME who makes request for storing and retrieving SME business data
Storage	Distributed Server where Data of the SME business operation is stored by user
User node	Generate transactions
Validator Node	Trusted entity which Run protocols build using CNN to verify user and its transactions to validate for generating block to be added in block chain
Block	Ledger which stores transaction of the data access
Blockchain	Linking of validated user generated transaction to storage server using cryptographic technique
Types of transaction	New Node creation, request access to data, link to user, log user access to data, input to smart contract
Smart Contract	It is to trigger the validator node to verify the user and verifies user permission to data access

1) *Convolution Neural Network- AI model*

Transactions are verified by nodes within the network and recorded data in block could be changed while alteration of subsequent blocks. In this work, Blockchain as a service is used to store data and allow participant to access it. Blockchain platforms[10] support convolution neural network towards facilitating model execution. Model execution in blockchain will trace data sources of the SME business operations stored in the blockchain ledger. Convolution Neural Network operation is as follows

- Convolution layer

Convolution layer uses kernel function and activation function to extract the user request log of the transaction to access the data transaction of each block in blockchain. It extract the spatial and temporal features of the user request log and those spatial feature is embedded as spatial feature map and temporal feature is embedded as temporal feature map[11]. Extraction and embedding of the spatial and temporal feature are as follows

Spatial feature S_f= Spatial_Kernel (User Request Log)

Spatial Features Vector $S_f(v)$ = {Source IP address, Destination IP Address, user Public key, block chain network topology, Request Info}
Temporal Feature T_f= Temporal Kernel (User Request Log)
Temporal features $T_f(v)$ = {date, time , }

- Max pooling layer

Max pooling layer reduces spatial dimension of the spatial embedding feature map. It reduces the dimension of extracting high level features[12]. Further max pooling performs aggregation of the spatial reduced features and temporal features in unified feature vector. Aggregated feature vector for the data access authorization is as follows

High Level Spatial Feature $HS_f = \sqrt{\sum_{i=0}^{n} s_f}$

Aggregated Feature Vector $F_v = H\sum_{i=0}^{n} s_f(i) + \sum_{i=0}^{n} T_f(i)$

- Fully Connected layer

Unified feature vector is applied to fully connected layer which contains activation function and softmax function along loss function to authenticate user and categorize the user with level of access to the data.

- ❖ Activation function: It linearizes the non-linear feature vector to linear feature vector using ReLu activation function.

  $AF_v = \text{ReLu}(F_v)$

- ❖ Softmax function: It employ classifier function of the naive Bayes to classify the user into authorized user and unauthorized user. Further authorized user is sub classified into various categories on basis of access level to data. Feature vector is transformed into distributions which are further analyzed in form of posterior probability and prior probability. Finally posterior probability is determined through likelihood estimation to determine the access level and prior probability is determined through conditional independence to be authorized user. Classification rule is mentioned as

  $y= \text{argmax}_y\ p(X|y)$

- ❖ Loss function: It employs cross entropy function to reduce overfitting and underfitting situation of the model.

  $F= p(x)\log p(x)$

B. Integration of the CNN on block chain consensus

Consensus mechanism uses proof of authority on employing convolution neural network to produce new block in blockchain to data access and validate the transactions. A smart contract which is self-executing contracts is written in form of code on leverage Consensus mechanism using CNN to establish a terms of agreement. Smart contract is executed in blockchain. Terms of agreement are set of rules to certain conditions[13]. Results sent to storage, storage process the result and responds with access link, timestamp, and nonce which is encrypted with user key. Encrypted information is the shared through blockchain to user.

```
Algorithm: Blockchain Integrated Convolution Neural Network
Input: SME Business Data
Output: User Authorization and Level of Access
Process ()
Distributed Storage (SME Business Data )
         Blockchain Ledger (Transaction of Data access to business data )
Blockchain nodes= {Validator node and user node}
     User node is automated participant managed by user
           User Node generates transaction for data access with public key and private key to encrypt and sign the transaction
Consensus_Proof of Authority(CNN)
       Validator Node Validates the Transaction of user node towards data access
   Convolution layer()
     Extract spatial features and Temporal Features
Max pooling Layer ()
     Reduce spatial features
         Aggregate spatial and temporal features as feature vector
Fully Connected layer ()
       Softmax function_Naive Bayes (Aggregated Feature Vector)
               Authorizes User and Classifies User levels to data access (user permissions)
Validator node generate block after successful of user validation and add block with block chain
         Validation node sends validated node results to the storage to obtain access link
              Access link is shared to user by blockchain to access the data on the storage server
                Storage server sends transaction for the blockchain to log the access
```

IV. EXPERIMENTAL RESULTS

In this section, experimental analysis of the newly integrated blockchain with convolution neural network for secure data access against cyber-attack is performed using python through popular Tensorflow and keras libraries. Convolution neural network is built using python programming in Jupiter notebook to establish a smart contract and consensus mechanism. User public key and private key is generated using hashlib libraries to encrypt the user information and user signatures. Further component of the blockchain such data structures, mining, transactions, networking and consensus algorithm is generated using python and JavaScript. Qualitative data representing business processes data of SME industries is transferred to data server.

Pretrained model of CNN is obtained from kaggle[14] process user identification id and data id to be accessed to provides values for all possible operations requested for the specific data. CNN architectures provide access to data on user validations. Model is trained with multiple user cases containing user without registration for access the blockchain and request for data which not stored in data server. Model process the 200 user and corresponding transactions are registered to blockchain

A. Performance Analysis

Performance analysis of the model proves that model is more accurate against detecting authorized user and classifying user on their data access levels. It is evaluated using confusion matrix on test data containing both attributes of the authorized user and unauthorized user. Confusion matrix[15] generates the values to the true positive, false negative, true negative and false positive parameters.

1) Precision Analysis

Precision analysis is performed to determine no of user features correctly classified as authorized user among the total no of the user features. Precision analysis represented on parameter of confusion matrix is as follows

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

Figure 2 represents precision analysis of the Blockchain integrated CNN model against conventional approaches using either blockchain or deep learning model to secure data access against cyber attacker. It represents model ability towards adaption to different types of attack.

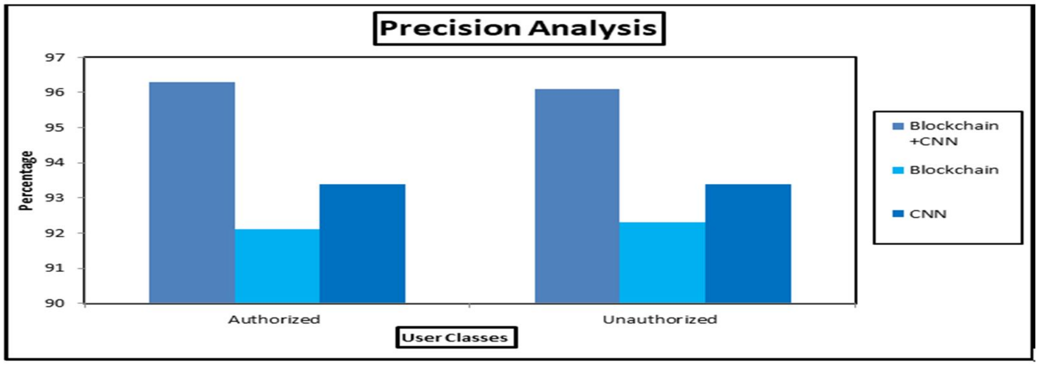


Figure 2: Precision Analysis

2) Recall Analysis

Recall analysis is performed to determine no of features incorrectly classified as authorized user among the total no of the user features. Recall analysis represented on parameter of confusion matrix is as follows

$$\text{Recall} = \frac{\text{TN}}{\text{TP+FP}}$$

Figure 3 represents Recall analysis of the Blockchain integrated CNN model against conventional approaches using either blockchain or deep learning model to secure data access against cyber attacker. It represents model ability towards adaption to different types of attack.

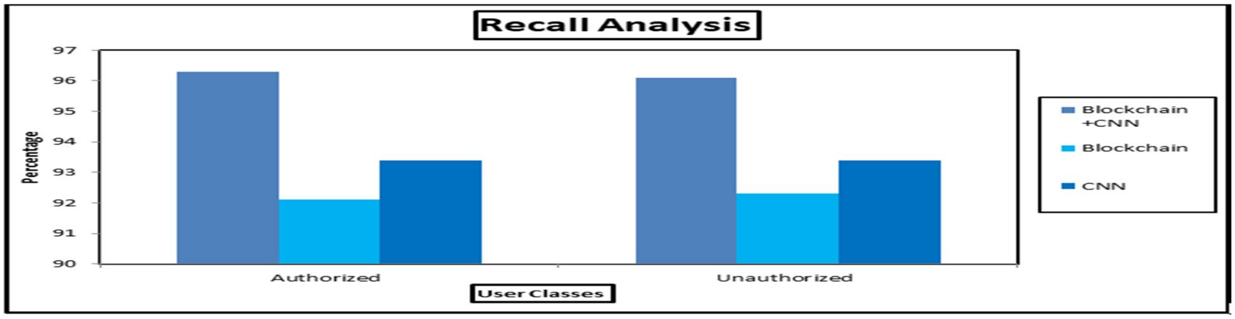


Figure 3: Recall Analysis

3) F-Measure Analysis

F-measure analysis is performed as aggregation of recall and precision towards detecting authorized user among total user for data access. F-Measure analysis represented on parameter of confusion matrix is as follows

$$\text{F-Measure} = \frac{TP+TN}{TN+FN+TP+FP}$$

Figure 4 represents F-Measure analysis of the Blockchain integrated CNN model against conventional approaches using either blockchain or deep learning model to secure data access against cyber attacker. It represents model ability towards adaption to different types of attack.

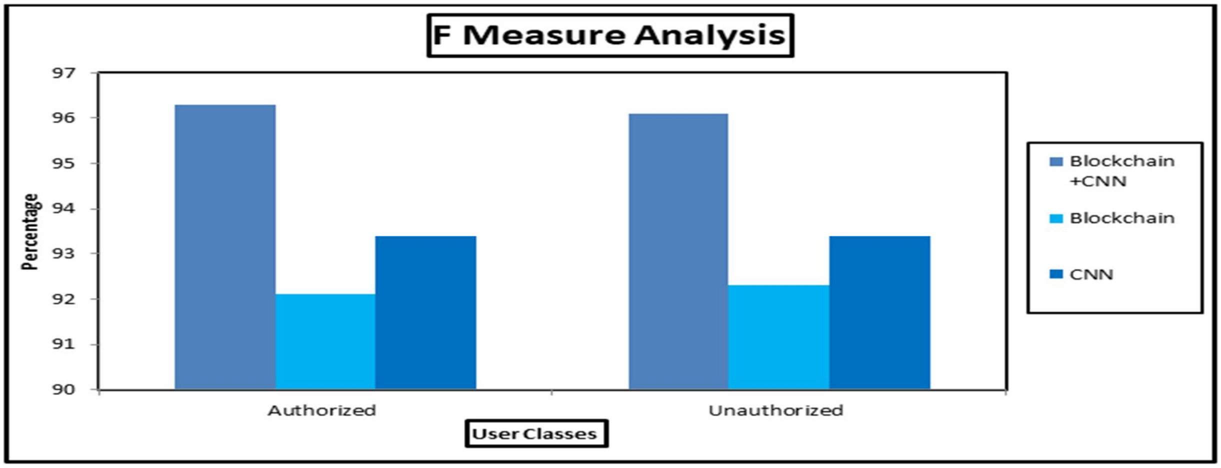


Figure 4: F-Measure analysis

On performance analysis, blockchain integrated CNN architecture performs better with detection accuracy 96.1.4% on compared to conventional approaches. Table 2 mentions the performance evaluation of the cyber security architectures towards secure access

Table 2: Performance Evaluation of cyber security architecture toward secure data access

Technique	Classes	Precision	Recall	F-Measure
Blockchain + CNN	Authorized User	96.6	94.2	96.1
	Unauthorized user	96.2	94.5	96.2
Blockchain	Authorized User	93.3	91.5	93.8
	Unauthorized user	93.7	91.6	93.4
CNN	Authorized User	91.2	90.2	91.7
	Unauthorized user	92.8	90.7	91.7

B. Security Analysis

Security analysis of the model proves that model is more secure against unauthorized user and authorized user with different access levels to data. Security strength of the model is confirmed on following aspects

- Confidentiality of the data: Confidentiality is ensured on request exchanged between the user and storage servers through blockchain are encrypted. It prevents attacker and unauthorized user from comprehending the content of a transactions or a request.
- Integrity: Integrity is ensured with signature on which user sending a request to sign the content with private key remains unmodified.
- Prevention against Replay Attacks: Nonce is randomly generated token to user request and access link shared to user by blockchain. It ensures that malicious user cant able to access previously shared link.
- Detection against malicious activity: Blockchain log user request to access data and user permission to access data as malicious request is detected easily.

V. CONCLUSION

In this paper, a new blockchain integrated convolution neural network is designed and implemented to secure data access among authorized and unauthorized user along predict and classify the user with user level to secure access of data in blockchain enabled distributed servers. Especially convolution neural network is enabled in blockchain on smart contract and consensus mechanism to validate the user and their access level to the data. On experimental and performance analysis, proposed model is found to be better compared to conventional approaches on securing data access and detecting the authorized user. As a future work, security of the secure access can be enhanced on employing federated architectures.

REFERENCES

[1] J. Abou Jaoude and R. G. Saade, “Blockchain applications–usage in different domains,” IEEE Access, vol. 7, pp. 45 360–45 381, 2019

[2] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” Telematics and informatics, vol. 36, pp. 55–81, 2019

[3] R. Zou, X. Lv, and J. Zhao, “Spchain: Blockchain- based medical data sharing and privacy-preserving ehealth system,” Information Processing & Management, vol. 58, no. 4, p. 102 604, 2021

[4] M. N. Nobi, R. Krishnan, Y. Huang, M. Shakarami, and R. Sandhu, “Toward deep learning based access control,” in Proceedings of the Twel- veth ACM Conference on Data and Application Security and Privacy, 2022, pp. 143–154

[5] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, et al., “A survey on blockchain technology: Evo- lution, architecture and security,” IEEE Access, vol. 9, pp. 61 048–61 073, 2021

[6] Guangming Xian"Cyber Intrusion Prevention for Large-Scale Semi-Supervised Deep Learning Based on Local and Non-Local Regularization"IEEE access, Vol.8,Page(s): 55526 - 55539, 2020

[7] Ahmed Didouh; Anthony Bahadir Lopez; Houda Labiod; Yassin El Hillali; Atika Rivenq; Mohammad Abdullah Al Faruque"TileChain: A Blockchain-Based Framework for Security Service Management for Vehicular Communications" IEEE Transactions on Vehicular Technology, Volume: 74, Issue: 1, pp:1335 - 1351, 2025

[8] Ikram Ud Din; Kamran Habib Khan; Ahmad Almogren; Mahdi Zareei; Jesús Arturo Pérez Díaz"Securing the Metaverse: A Blockchain-Enabled Zero-Trust Architecture for Virtual Environments"IEEE Access, Volume: 12, PP: 92337 - 92347,2024

[9] Ozgur Koray Sahingoz; Ebubekir BUBEr; Emin Kugu"DEPHIDES: Deep Learning Based Phishing Detection System"IEEE access, Vol.12, PP:8052-8070,2024

[10] B. M. Yakubu, M. I. Khan, A. Khan, F. Jabeen, and G. Jeon, ‘‘Blockchainbased DDoS attack mitigation protocol for device-to-device interaction in smart home,’’ Digit. Commun. Netw., vol. 9, no. 2, pp. 383–392, Apr. 2023.

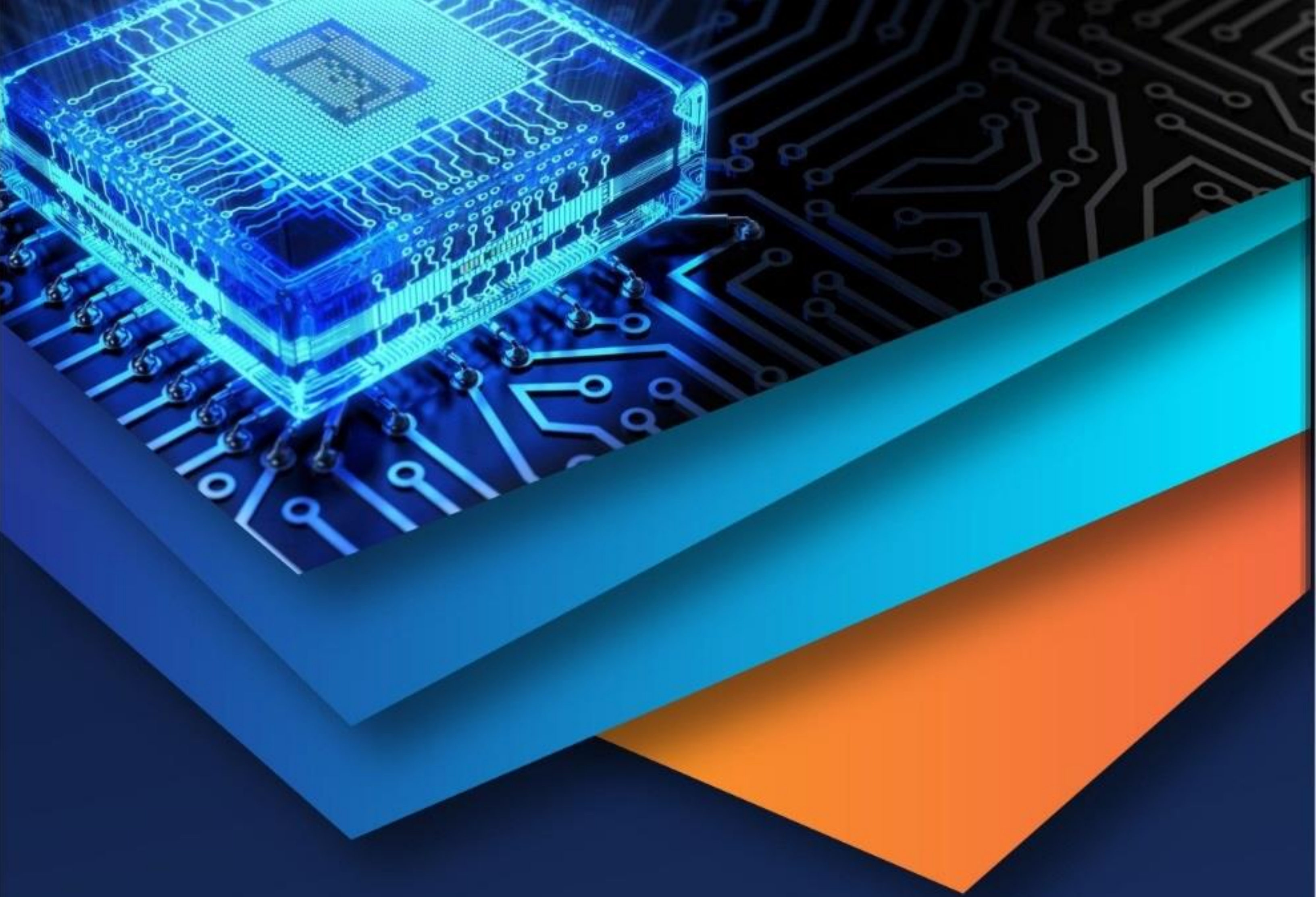
[11] E. S. Babu, S. Bkn, S. R. Nayak, A. Verma, F. Alqahtani, A. Tolba, and Mukherjee, ‘‘Blockchain-based intrusion detection system of IoT urban data with device authentication against DDoS attacks,’’ Comput. Electr. Eng., vol. 103, Oct. 2022

[12] M. A. Cheema, H. K. Qureshi, C. Chrysostomou, and M. Lestas, ‘‘Utilizing blockchain for distributed machine learning based intrusion detection in Internet of Things,’’ in Proc. 16th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS), May 2020

[13] T. M. Ghazal, M. K. Hasan, S. N. H. S. Abdullah, K. A. A. Bakar, and H. Al Hamadi, ‘‘Private blockchain-based encryption framework using computational intelligence approach,’’ Egyptian Informat. J., vol. 23, no. 4, pp. 69–75, Dec. 2022

[14] H. N. Abishu, A. M. Seid, Y. H. Yacob, T. Ayall, G. Sun, and G. Liu, ``Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the internet of electric vehicles," IEEE Trans. Veh. Technol., vol. 71, no. 1, pp. 946_960, Jan. 2022.

[15] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, and X. Du, ``Blockchain-assisted secure device authentication for cross-domain industrial IoT," IEEE J. Sel. Areas Commun., vol. 38, no. 5, pp. 942_954, May 2020.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY