FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 3 | Pages 536-543 | e-ISSN: 2347-470X

An Intelligent Secure Monitoring Phase in Blockchain Framework for Large Transaction

Sk. Khaja Shareef[1], R. Sridevi[2], V. Rama Raju[3] and K.S. Sadasiva Rao[4]

[1] *Research Scholar, CSE Dept, JNTUH &Associate Professor, CSE Dept MLR Institute of Technology Hyderabad*
[2] *Professor, Computer Science & Engineering, JNTUH College of Engineering Hyderabad*
[3] *Professor, Computer Science & Engineering, CMR College of Engineering & Technology Hyderabad*
[4] *Professor, Department of MCA, Chaitanya Bharathi Institute of Technology, Hyderabad*

***Correspondence:** Sk. Khaja Shareef ; khaja.sk0822@gmail.com

ABSTRACT- Blockchain is the key concept for security purposes for digital applications. But, in some cases, the effectiveness of the malicious behavior has degraded the security function of the blockchain. So, to enrich the blockchain process prediction and to neglect the malicious event from the data broadcasting medium is very important. So, the current research article intends to develop an efficient monitoring strategy based on incorporating deep features. Hence, the designed paradigm is termed as Lion-based Convolutional Neural Model (LbCNM) with serpent encryption. Before performing the encryption process, the novel LbCNM parameters have been activated to monitor the data process channel in the blockchain environment. Here, the malicious behaviors were estimated by incorporating the known and unknown user behavior in the Lion fitness model. During the execution, the fitness formulation of Lion is acted in the classification layer of the convolutional model. Once the present malicious characteristics have been detected, it is neglected from the data broadcasting channel. Hereafter, the transactional data has been encrypted and stored in the specific cloud. The planned strategy is verified in the python platform. The successful performance of the LbCNM with serpent has been analyzed with some key parameters like confidential rate, accuracy, data overhead, and processing time.

Keywords: Blockchain, Encryption, large transaction, malicious behaviour, data overhead.

ARTICLE INFORMATION

Author(s): Sk. Khaja Shareef, R. Sridevi, V. Rama Raju and K.S. Sadasiva Rao
Received: 16-07-2022; **Accepted**: 20-08-2022; **Published**: 30-08-2022;
e-ISSN: 2347-470X;
Paper Id: IJEER1607-09;
Citation: 10.37391/IJEER.100322
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100322.html

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

The emerging field in cloud computing is blockchain strategy, which is also termed bitcoin [1]. Introducing the blockchain model in the cloud paradigm is to secure the data from third parties [2]. Moreover, the blockchain approach is termed in two-three classes that are custom, private and public blockchain [3]. All records were kept public in a public blockchain that is accessible for all users [4]. In the private blockchain, the stored records' control belonged to a single person or organization [5]. Also, the control process is managed by a group of specific organizations for the custom blockchain. At the introduction of the blockchain, decentralized network application is utilized [6]. Hence, the main process of the blockchain model is decentralization, security, and immutability. The blockchain concept is the crypto process that has converted the original text into an unreadable way to prevent data theft [7]. In addition, several homomorphisms approaches were also implemented with the blockchain strategy to afford the security for a long duration [8]. Besides all those things, designing the monitoring mechanism is important to offer the continuous monitoring function throughout the data transaction [9].

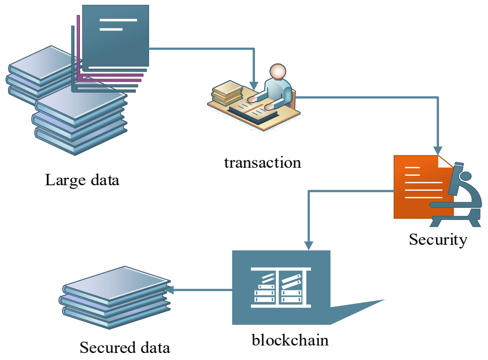


Figure 1: Blockchain fundamentals

The key motive of this blockchain usage is to transfer and store large data securely [10]. Hence, the blockchain approach has been followed under two types of crypto strategies: symmetric and asymmetric encryption schemes [11]. In addition, the has function is used to find the initial hash of the trained data [12]. Then, the encryption function has 2 is measured from the encrypted data [13]. Hereafter, the zoomorphism is applied to verify the process, whether the data is injected or not [14]. Hence, the blockchain strategy has many advances. However, it lacks in third-party continuous monitoring process [15]. The fundamentals in blockchain security are diagrammatically described in *figure 1.*

Several blockchain models, such as the blockchain model for the offline application [24], centralized and decentralized blockchain strategy [25], etc., have been executed in the past for several online applications. But, still, the security threats were not ended because of large complex data [19,20]. So the present article has planned to create a novel efficient strategy for the threat monitoring process in the blockchain-based data transaction system. Finally, the designed model is verified by launching an efficient attack. Hereafter, the parameters were calculated and compared with other models. This research work's main focus is to enhance the blockchain facilities to enrich the advances and security of online applications.

The current article's research arguments are organized as follows. The *2nd Section* has detailed the associated works of blockchain security in various sectors and challenges. The usual Blockchain system in large transactions with problems is illustrated in *Section 3*. The designed novel solution for the discussed problem is highlighted in *4th Section*. Moreover, the working performance of the designed monitoring-blockchain strategy is summarized in *5th Section* and the research discussion and achievements are concluded in *Section.6*.

2. RELATED WORK

To advance the blockchain facilities, Ikechi SaviourIgboanusi *et al [24]* have designed a blockchain model for the offline application to transfer the data. This method aims to help the smart contract whenever the connection is lost. Finally, the blockchain has transferred the data without the usage of internet connection with a high confidential rate. However, this strategy is only applicable for the specific applications.

Online education became worldwide in today's life scenario hence content ranking for the student's performance is more important. But the content ranking became thrust worth there is no replication content. For that, Anuj Garg *et al.* [25] have designed the centralized and decentralized blockchain strategy for the online education system. Finally, the content ranking has been performed with high trust behavior. But, it needs more time to execute.

The network called as delay-tolerant is used for large data transaction system. To secure this large data transmission, a blockchain strategy has been introduced by Xin Cong et al [26] called Token Negotiation blockchain. In addition, the mining procedure has been implemented to extract the replicated falsie data. Finally, the performance of the designed model is validated in terms of throughput, confidential rate and data transfer. However, the packet drop issues in the delay-tolerant model are not end.

Regression analysis was introduced in blockchain system by WeiHong *et al* [27] for analyzing the user behavior continuously. Here, the normal user's behavior was updated in the regression rules. During the encryption process, if there is any unmatched user behavior, it makes an alarm. The dataset known as food safety info has been taken as a Database to check the reliability score of the proposed model functions. However, it has required more resources to execute the process.

.Jianguo Chen *et al* [28] have introduced an efficient blockchain technology based on the deep networks for the vehicular-Adhoc application. Here, the deep network-based blockchain strategy is verified with both a centralized and decentralized environment. Here, the treat are detected neglected in the asynchronous manner. However, it has need more power usage to execute the process continuously based on vehicle moving.

The key contribution of this present study was summarized as follows,

- Initially, the bank dataset was collected and imported to the python system
- Consequently, the Lion-based Convolution Neural model (LbCNM) was designed with the Serpent Encryption model.
- Here, the fitness of the lion has provided continuous monitoring for the data transmission channel
- When, the malicious behavior was found, then it is neglected by the hunting behavior of the lion optimization
- Hereafter, the encryption strategy has been performed to hide the data from the third users
- Moreover, the incorporation of the lion fitness in the convolution model will provide the finest attack detection and prevention results
- Finally, the robustness of the proposed scheme is analyzed by confidential score, data integrity, processing time and data overhead.

3. SYSTEM MODEL WITH PROBLEM

In the large transaction system, the main two problems that have to be considered are attack vulnerability and data overhead [16]. These, two problems were addressed by controlling the security functions in the blockchain system [17,18]. However, blockchain is the more important paradigm to transact the large data. Moreover, this blockchain is mainly utilized for the bank transaction application.

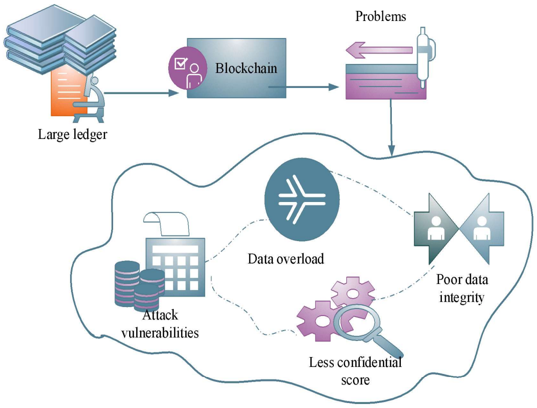


Figure 2: System model with problem

Hence, the chief problems that have often been raised during the large data broadcasting are illustrated in *figure 2*. The previous models' problems are poor data integrity, data overload, attack vulnerability, and less confidential score.

4. PROPOSED LBCNM FOR BLOCKCHAIN SECURITY ENHANCEMENT

The technology blockchain has been elaborated in many applications, but providing security is a crucial task and more difficult. So, the present research article has planned to design a continuous monitoring system for blockchain applications. Moreover, a novel technique is named LbCNM and is utilized for the encryption serpent model. Finally, the functioning performance of the proposed model is measured by applying the designed technique in the credit card database.

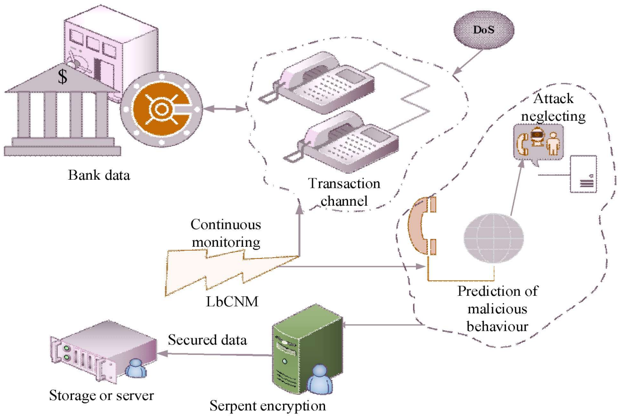


Figure 3: Proposed LbCNM with serpent architecture

Finally, the key metrics are measured and validated with recent associated works and the percentage of the improvement rate has been noted. The proposed LbCNM with serpent model is blockchain is described in *Figure 3*.

4.1 Design of LbCNM layer

The planned security model is the hybrid algorithm-generated with dual lion optimization procedures [23] and convolution neural model [22]. Here, the finest solution of the lion is hunting characteristics. This research objective is utilized to find the malicious behavior, neglect malicious events, and offer continuous monitoring. In addition, the neural convolution model is discussed for enabling the training and testing function for the trained database.

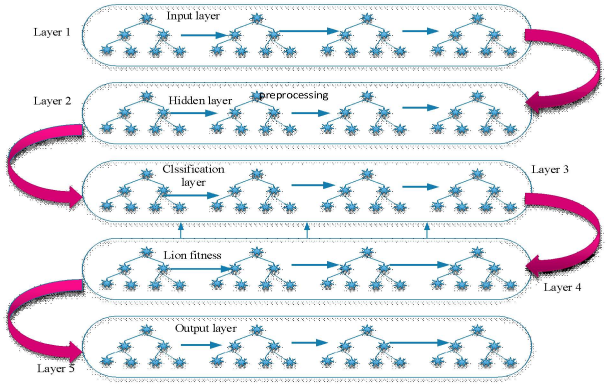


Figure 4: Layer of LbCNM

Moreover, the LbCNM contains six five layers, the first input layer, where the databases are trained to the model. The second is the hidden layer here; it is functioning as the preprocessing phase. Consequently, the error-free data is imported to the classification phase's third layer. The feature analysis parameters have been designed based on normal and malicious users. Moreover, the parameter of the classification module is tuned by the 4th optimal layer. In addition, the prediction and the neglecting process have been processed. Finally, the malicious free data transaction medium has been obtained, described in *figure 4*. The designed security mechanism is suitable for handling large data; hence, the layers of the LbCNM have included some features like preprocessing, storing, prediction layer, and optimum value setting layer.

$$f(b_d) = 1,2,3,4,5.....,n \tag{1}$$

Here, the trained credit database is determined as b_d and $1,2,3...,n$ is the each credit card details. Consequently, the pre-processing function has been performed using Eqn. (1). The function pre-processing is common for all ML models to gain the finest predicted results. Because the noisy data has reduced the prediction exactness score

$$p(b_d) = \frac{gf - nf}{tf} \tag{2}$$

Here, tf is the total features in the trained database; good features were determined as gf, nf is the noise variable or features and p is the pre-processing variable. Hence, the pre-processing function was performed by Eqn. (2)

$$L_f = \begin{cases} user & if(user = 0) // normal \quad user \\ user & if(user \neq 0) // malicious \quad user \end{cases}$$

(3)

The behavior of the malicious and normal user has been found by eqn. (3)

$$Lh = \begin{cases} rand(2*mu - Pb) & (2*mu - Pb) < mu \\ rand(mu,(2*mu - pb), & (2*mu - pb) > mu \end{cases} \tag{4}$$

Here, the unknown or malicious behaviors are found by the fitness of the lion function that is denoted as Lh, and Pb is the malicious activity detection variable. Also, mu it represents malicious users. Hence, eqn.(4) is utilized to enable the continuous monitoring function.

$$Lh = \begin{cases} rand(Pb, mu) & Pb < mu \\ rand(mu, Pb) & Pb > mu \end{cases} \tag{5}$$

In blockchain, the transaction proc4ss in performed in a random direction, which is not similar. Hence, to offer data protection in all directions of transactions, Eqn. (5) has been used. Consequently, the neglect of the malicious events proceeds by Eqn. (6)

$$Lh = \frac{normal \quad user - mu}{total \quad transactions} \tag{6}$$

After setting the monitoring modules, the serpent encryption [21] procedure has been initiated to encrypt the data and broadcast the transaction details securely.

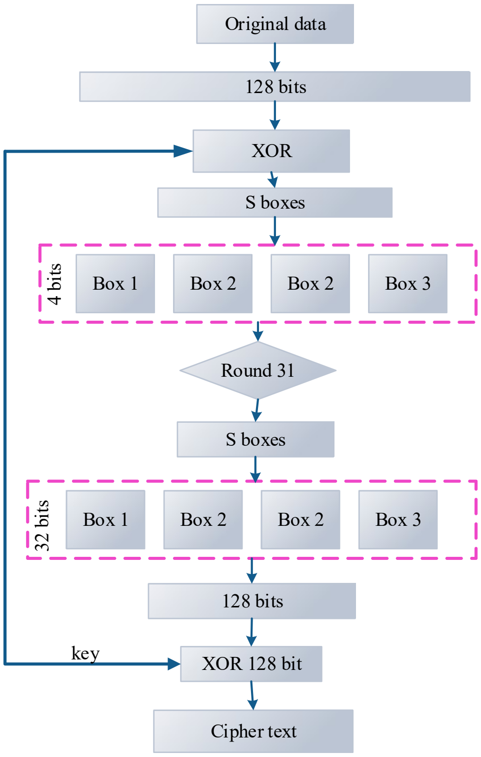


Figure 5: serpent blockchain

The usual encryption process by functioning the serpent model is detailed in *Figure 5* here; the bits take for encryption at a single time is 128 bits. Here, the process of encryption is performed based on the XOR operations.

Algorithm.1 LbCNM with serpent

```
start
{
    $int\, b_d$ ;
    // database initialization
    Reprocessing module ()
    {
        $int\ gf, nf, tf;$
        // initializing pre-processing variables
        $p(b_d) \rightarrow gf - nf$
        // error-free data was obtained
    }
    Malicious events prediction ()
    {
        $int\ Lf;$
            // updating lion fitness
            $if\ (user = 0)$
            {
            Normal user
            }else (malicious user)
            // fixing the prediction parameter based on if conditions
    }
    Continuous monitoring ()
    {
            $int\ pb, mu, Lh;$
            $Lh(Pb) \rightarrow rand(mu)$
            // setting random prediction of malicious users in all transaction direction using eqn.(5)
    }
    Malicious event rejection()
    {
            $Lh \rightarrow (normal \quad user) - mu$
            // the malicious users has been neglected
    }
    Serpent encryption Blockchain()
    {
            User credit card details $\rightarrow encrypt$
            } data sharing (transactions)
}
Stop
```

The proposed LbCNM procedure is described in the *algorithm.1* and *Figure 6*. Consequently, specific codes were written in python for each algorithm step, and execution functioned for the credit card bank database. Finally, the designed model function has been verified with DoS malicious behavior. It has produced abnormal activities by causing traffic flow in the communication medium.

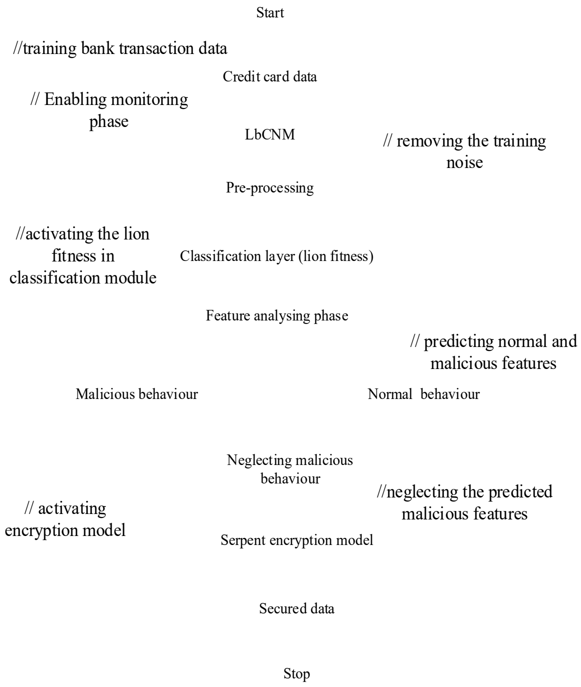

Start
//training bank transaction data
Credit card data
// Enabling monitoring phase
LbCNM
// removing the training noise
Pre-processing
//activating the lion fitness in classification module
Classification layer (lion fitness)
Feature analysing phase
// predicting normal and malicious features
Malicious behaviour
Normal behaviour
Neglecting malicious behaviour
//neglecting the predicted malicious features
// activating encryption model
Serpent encryption model
Secured data
Stop

Figure 6: Flow model of LbCNM with serpent

5. RESULTS AND DISCUSSION

To measure the successful performance of the designed LbCNM with serpent model, the database was gained from the Kaggle site, which is related to bank transactions. Hence, the total size of data 150Mb; also, it contains several attributes like class status, amount, time, and transactions count. Moreover, the novel LbCNM with serpent blockchain system is executed in the Python platform 3.8, pycharm community, and running in windows-10 environment. Hence, the successive rate was validated by measuring the key metrics.

5.1 Case study

The characteristics of the obtained credit dataset are detailed in *figure 7***.** Here, the user behavior in the trained credit databases is measured up to 175000s. This graph validation is termed as transaction period versus amount.

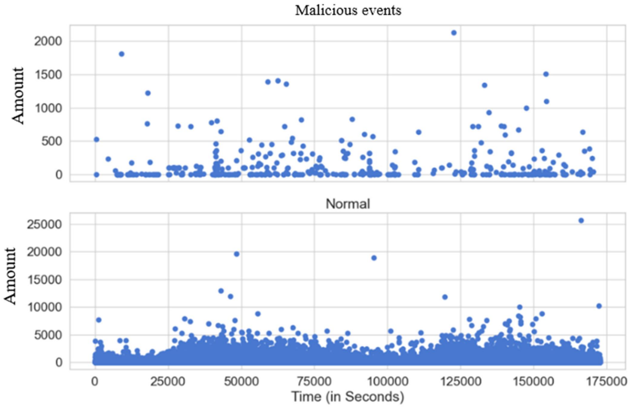
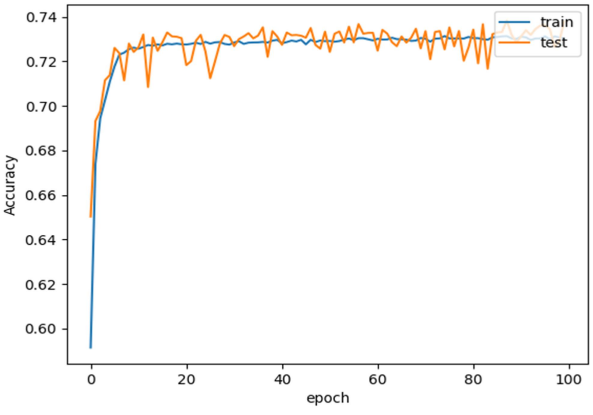
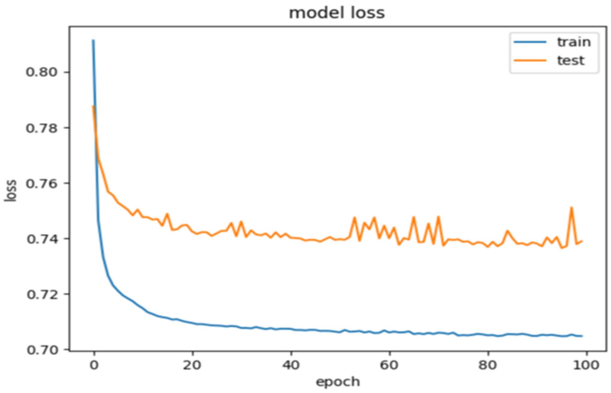


Figure 7: Credit Card Database Features

Moreover, the metrics loss function is validated for the train and test function elaborated in *Figure.* Moreover, user behavior has been measured in dual cases that are false and true cases. Based on those class results, the accuracy of the metric has been validated. The scalability score of the proposed LbCNM scheme has been verified by the training results performance, which is detailed in *Figure 8.* Here, accuracy measure has been valued in test and train cases in dual sectors.



(a)



(b)

Figure 8: Training results validation: (a) accuracy, (b) loss

The total size of the trained data is 15Mb in that 80% is utilized for training, and 20% data is utilized for testing. Moreover, several metrics were measured and validated with other associated models for the testing cases.

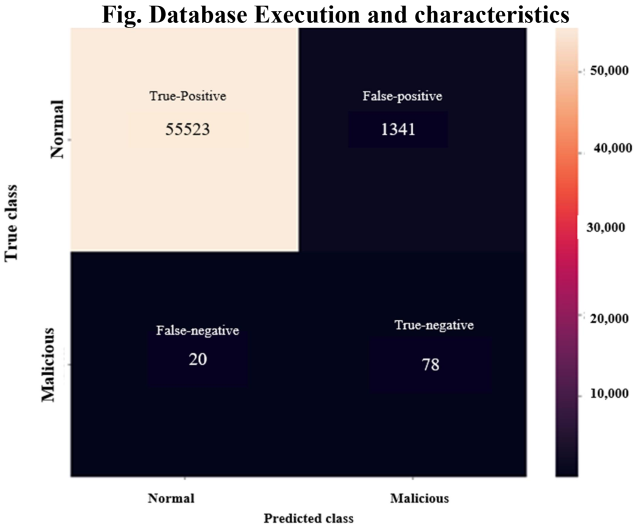


Figure 9: Confusion Matrix

The parameter confusion metrics have measured the exactness of malicious behavior findings based on true and false cases. Here, the total credit card data is 284808; the detected true-positive is 55523, and false-Positive is 1341 for normal classes. Moreover, for the class malicious, the predicted false-negative is 20 and true-negative is 78, which is represented in *figure 9*.

5.2 Performance and comparison evaluation

The working stability of the proposed model is analyzed by measuring the key parameters such as data integrity, confidential score, processing time, and data overhead. Moreover, the success rate of the designed LbCNM with serpent scheme is proved the successive score against the DoS attack.

5.2.1 Confidential rate and data integrity

For all the trust worthy application, measuring these two metrics is crucial to measure the stable status of the developed system. Also, to note the percentage of improvement over the other model, few past works have been obtained that are Radial based Kernal Model (RKM) [30] and Lamport-Merkle model (LMM) [31].

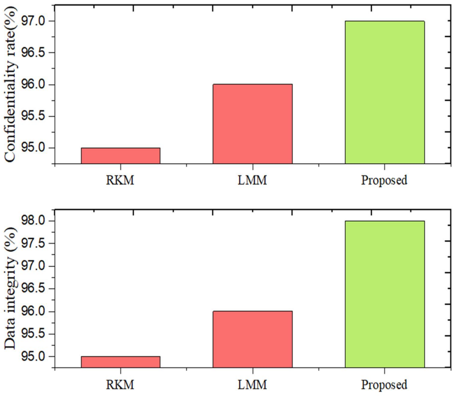


Figure 10: Confidential and data integrity comparison

Here, the RKM scheme has recorded the confidentiality score as 95%, LMM has yielded the confidential score as 96%, and the proposed LbCNM with serpent has earned 97% confidential rate. Hence, the assessment of data integrity and the confidential score is illustrated in *figure 10*. This has proved the successive rate in privacy preserved by a novel monitoring blockchain strategy. In addition, the parameter confidentiality rate is measured by eqn. (7)

$$confidentiality = {}^{rd}\!/_{td} \qquad (7)$$

Here, rd determined successful transaction and total transaction is described as td .

5.2.2 Attack prediction accuracy

After designing the proposed LbCNM with a serpent blockchain system, the privacy range of the designed platform has to be checked by some attack vulnerabilities. For that, DoS attack has been launched in the system then the working function of the novel LbCNM with serpent has been estimated by evaluating the parameters.

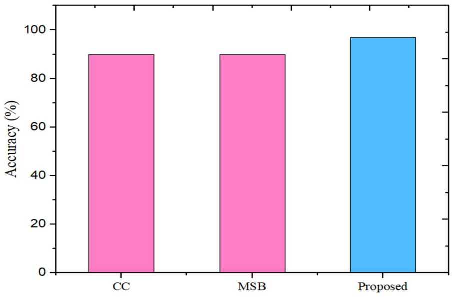


Figure 11: Validation of accuracy

Moreover, to check the detection behavior of the LbCNM model, the metric accuracy has been evaluated for attack detection. Here, the proposed LbCNM with serpent has reported the finest attack prediction exactness score than the existing models like Collaborative Clustering (CC) [34] and Master-Slave-Blockchain MSB [29]. Here, the CC and MSB has measured the accuracy rate as 90%. However, the proposed LbCNM with serpent has recorded a wide range of accuracy as 97%; those statistics are illustrated in *figure 11*.

$$Accuracy = \frac{A_b}{T_b} * 100 \qquad (8)$$

Eqn has valued the metrics accuracy of this application. (8), where, A_b is the normal behavior and T_b is the total behavior. Here, the metric accuracy has been described by taking the average of authenticated characters and total behavior.

5.2.3 Processing time

In cloud platform or application measure, the data processing duration is the most required task to value each technique performance. Moreover, the processing duration is defined as the entire system execution time to complete the single transaction.

Table 1: Assessment of processing time

Processing Time Validation			
Methods	**RKM**	**LMM**	**Proposed (LbCNM-serpent)**
Processing time (ms)	52	35	15
Processing time (s)	0.052	0.035	0.01499

The duration taken to execute the function is 15ms; simultaneously, the LMM has recorded the maximum duration as 35ms, and the model RKM has obtained 52ms for execution; those validation is tabulated in *Table 1.*

5.2.4 Data overhead

Data overhead is the key issue in big data and cloud application; that paradigm can process a large amount of data at a time. Hence, if the data load is over than the capacity of the server node, then data overhead has been recorded. In addition, achieving the overhead data rate might degrade the confidential score. Also, the high data overhead may lead to data collision in the communication medium that has maximized the attack vulnerabilities.

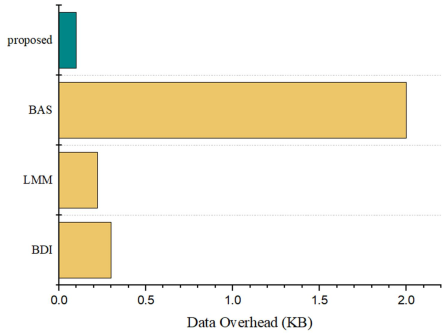


Figure 12: Data Overhead Comparison

To evaluate the improvement score of the data overhead reduction, some of the recent existing works have been considered into an account, such as Blockchain data-integrity (BDI) [32], Blockchain agent system (BAS) [33], and LMM. The proposed LbCNM with serpent has minimized the overhead data range as 0.1KB. Simultaneously, the model LMM has reported 0.22KB, BAS has obtained 2KB, and BDI has recorded 0.3KB; those statistics are described in *figure 12*.

5.3 Discussion

The designed LbCNM with serpent has reported the finest outcome from performance and comparison validation by gaining a wide range of attack perdition exactness score, high confidentiality, and data integrity. Also, it has noted less data overhead and processing time.

Table 2: Overall performance evaluation

Overall evaluation	
Metrics	**Proposed LbCNM with serpent**
Data integrity	98
Confidential rate	97
Accuracy	97
Processing time (ms)	15
Data Overhead (KB)	0.1

The overall Proposed LbCNM with serpent performance is described in *Table 2*. In all cases, it has earned the better outcome that verified the scalability of the designed scheme. Hence, the planned design is suitable for the blockchain area as the monitoring model.

6. CONCLUSION

The main novelty that has been introduced in this research article is the monitoring mechanism in the blockchain. The monitoring phase module has been designed by a novel LbCNM approach. Moreover, in this monitoring phase, dual functions were performed to predict malicious characteristics and neglect those predicted malicious events. Consequently, the encryption function is activated to hide the data from the third parties then the encrypted data is transferred or stored in the specific server or cloud. Hence, the working performance of the novel LbCNM has been measured by validating the crucial parameters. The proposed LbCNM has recorded the maximum data integrity rate as 98%. Comparing the past associated works has maximized the score of data integrity up to 3%. In addition, the measured confidential score of the novel LbCNM scheme is 97%; when compared to other recent work, it has enriched the privacy range up to 2%. Moreover, the estimation of the malicious characteristic has earned 97% accuracy, which shows an improvement rate up to 7% than the compared schemes. Hence, in all aspects, it has described the finest outcome that verified the proposed LbCNM is sufficient for the secure blockchain concept.

REFERENCES

[1] Niranjanamurthy, M., B. N. Nithya, and S. J. C. C. Jagannatha. "Analysis of Blockchain technology: pros, cons and SWOT." Cluster Computing 22.6 (2019): 14743-14757.

[2] Perez, Maria Rona L., Bobby Gerardo, and Ruji Medina. "Modified sha256 for securing online transactions based on blockchain mechanism." 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management (HNICEM). IEEE, 2018.

[3] Madaan, Lakshit, Amit Kumar, and Bharat Bhushan. "Working principle, application areas and challenges for blockchain technology." 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT). IEEE, 2020.

[4] Mao, Dianhui, et al. "Novel automatic food trading system using consortium blockchain." Arabian Journal for Science and Engineering 44.4 (2019): 3439-3455.

[5] Puthal, Deepak, et al. "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems." IEEE Consumer Electronics Magazine 7.4 (2018): 6-14.

[6] Aggarwal, Shubhani, and Neeraj Kumar. "A consortium blockchain-based energy trading for demand response management in vehicle-to-grid." IEEE Transactions on Vehicular Technology 70.9 (2021): 9480-9494.

[7] Durach, Christian F., et al. "Blockchain applications in supply chain transactions." Journal of Business Logistics 42.1 (2021): 7-24.

[8] Sladić, Goran, et al. "A Blockchain Solution for Securing Real Property Transactions: A Case Study for Serbia." ISPRS International Journal of Geo-Information 10.1 (2021): 35.

[9] Jung, Hyunjun, and Dongwon Jeong. "Blockchain Implementation Method for Interoperability between CBDCs." Future Internet 13.5 (2021): 133.

[10] Berdik, David, et al. "A survey on blockchain for information systems management and security." Information Processing & Management 58.1 (2021): 102397.

[11] Nanayakkara, Samudaya, et al. "A methodology for selection of a Blockchain platform to develop an enterprise system." Journal of Industrial Information Integration 23 (2021): 100215.

[12] Javaid, Mohd, et al. "Blockchain technology applications for Industry 4.0: A literature-based review." Blockchain: Research and Applications (2021): 100027.

[13] Vacca, Anna, et al. "A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges." Journal of Systems and Software 174 (2021): 110891.

[14] Kouhizadeh, Mahtab, Sara Saberi, and Joseph Sarkis. "Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers." International Journal of Production Economics 231 (2021): 107831.

[15] Cucari, Nicola, et al. "The impact of blockchain in banking processes: the Interbank Spunta case study." Technology Analysis & Strategic Management (2021): 1-13.

[16] Esposito, Christian, Massimo Ficco, and Brij Bhooshan Gupta. "Blockchain-based authentication and authorization for smart city applications." Information Processing & Management 58.2 (2021): 102468.

[17] Garg, Poonam, Bhumika Gupta, Ajay Kumar Chauhan, Uthayasankar Sivarajah, Shivam Gupta, and Sachin Modgil. "Measuring the perceived benefits of implementing blockchain technology in the banking sector." Technological Forecasting and Social Change 163 (2021): 120407.

[18] Rajnak, Viktoria, and Thomas Puschmann. "The impact of blockchain on business models in banking." Information Systems and e-Business Management 19.3 (2021): 809-861.

[19] Raddatz, N., Coyne, J., Menard, P., & Crossler, R. E. (2021). Becoming a blockchain user: understanding consumers' benefits realisation to use blockchain-based applications. European Journal of Information Systems, 1-28.

[20] Khalil, Mahmoona, Kausar Fiaz Khawaja, and Muddassar Sarfraz. "The adoption of blockchain technology in the financial sector during the era of fourth industrial revolution: a moderated mediated model." Quality & Quantity (2021): 1-18.

[21] Shah, Tariq, Tanveer Ul Haq, and Ghazanfar Farooq. "Improved SERPENT algorithm: Design to RGB image encryption implementation." IEEE Access 8 (2020): 52609-52621.

[22] Valueva, Maria V., et al. "Application of the residue number system to reduce hardware costs of the convolutional neural network implementation." Mathematics and Computers in Simulation 177 (2020): 232-243.

[23] Geetha, Karuppaiah, Veerasamy Anitha, Mohamed Elhoseny, Shankar Kathiresan, Pourya Shamsolmoali, and Mahmoud M. Selim. "An evolutionary lion optimization algorithm-based image compression technique for biomedical applications." Expert Systems 38, no. 1 (2021): e12508.

[24] Igboanusi, Ikechi Saviour, et al. "Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture." ICT Express 7.3 (2021): 327-334.

[25] Garg, Anuj, et al. "Blockchain-based online education content ranking." Education and information technologies (2021): 1-23.

[26] Cong, Xin, Lingling Zi, and Ding-Zhu Du. "DTNB: A blockchain transaction framework with discrete token negotiation for the delay tolerant network." IEEE Transactions on Network Science and Engineering (2021).

[27] Hong, Wei, et al. "Public cognition of the application of blockchain in food safety management—Data from China's Zhihu platform." Journal of Cleaner Production 303 (2021): 127044.

[28] J. Chen, K. Li and P. S. Yu, "Privacy-Preserving Deep Learning Model for Decentralized VANETs Using Fully Homomorphic Encryption and Blockchain," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3105682

[29] Ekanayake, Omeshika AS, and Malka N. Halgamuge. "Lightweight Blockchain Framework using Enhanced Master-Slave Blockchain Paradigm: Fair Rewarding Mechanism using Reward Accuracy Model." Information Processing & Management 58.3 (2021): 102523.

[30] Yuvaraj, N., and P. Mohanraj. "Radial kernelized regressive merkle–damgård cryptographic hash blockchain for secure data transmission with IoT sensor node." Peer-to-Peer Networking and Applications (2021): 1-13.

[31] Alzubi, Jafar A. "Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare." Computer Communications 170 (2021): 200-208.

[32] Wang, Huaqun, et al. "RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks." Journal of Parallel and Distributed Computing 152 (2021): 1-10.

[33] Wei, PengCheng, et al. "Blockchain data-based cloud data integrity protection mechanism." Future Generation Computer Systems 102 (2020): 902-911.

[34] Liang, Wei, et al. "Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems." IEEE Internet of Things Journal (2021).

AUTHORS PROFILE

Sk. Khaja Shareef is a Research Scholar at Jawaharlal Nehru Technological University Hyderabad, Telangana in the area of Information Security and he is working as Assistant professor in MLR institute of Technology. He received his B.Tech. in Information Technology from Kakatiya University and M.Tech in Information Technology from JNTU Hyderabad. Presently he is working as Associate Professor in the department of IT at MLR institute of Technology, Hyderabad, Telangana. He is having a good number of Publications in reputed Journals.

Dr. R Sridevi received her B.Tech from Madras University, Chennai in Computer Science and Engineering and M.Tech in Computer Science and Engineering from Andhra University, Andhra Pradesh and PhD in CSE from JNTUH College of Engineering Hyderabad. She has around 16 years of teaching experience from JNTUHCEH. She works as Professor in CSE & Coordinator, Centre of Excellence in Cyber Security, JNTUH College of Engineering Hyderabad, India. She has published more than 20 papers in refereed journals and conference proceedings, . Her research interests include Computer Networks, Information Security, and Network Security.

Dr. V. Rama Raju received his Post-B.Tech from Central University of Hyderabad (HCU), in Computer Science and Engineering and M.Tech in Computer Science and Engineering from JNU New Delhi and PhD in Neurology & Biomedical Engineering from Nizam`s Inst of Medical Sciences (NIMS) University Hyderabad. He has around 35 years of teaching experience from reputed Engineering Institutions. He working as Professor in the CSE Department, CMR College of Engineering Hyderabad, India. He has published 3 books and more than 200 papers in refereed journals and conference proceedings, having 300 citations. His research interests include **Computer Science & Engineering/ Information Technology** Currently working on wireless sensor – Vehicular Adhoc Networks. Artificial Intelligence- Computational & Cognitive system, AI, Natural Language Speech & Auditory Processing, Machine Translation, Lexical computation, specification design & devt of computational lexicon & Neuro-Linguistics, Pattern Recognition & feature extraction

- **Biomedical Engineering** – Biomedical Instrumentation and Signal Processing and Multichannel Electrode Recordings (Micro, surface, induced, intramuscular, intra/extra cellular microelectrodes)
- **Neuroscience** - Neurology/Functional Neurosurgery – Neurodegenerative Parkinson`s Disease/ MER with DBS Electrode Implantation in PDs, Dystonia Writer`s Cramp and other Movement Disorders, Neuromuscular diseases, Cognitive science
- **Biomedical Signal processing**-Neuro-Muscular Human Motor Control system, EMG Writer`s and Musician`s Cramp, Dystonia.

Dr. K. S. Sadasiva Rao received his PhD from JNTUH Hyderabad, in Computer Science and Engineering He has around 20 years of teaching experience from reputed Engineering Institutions. He working as Professor in the MCA Department, Chaitanya Bharathi Institute of Technology, Hyderabad, India. He has published more than 20 papers in refereed journals and conference proceedings. His research interests include working as Professor in the MCA Department, Chaitanya Bharathi Institute of Technology, Hyderabad.