ISSN: 2182-2069 / E-ISSN: 2182-2077

Blockchain Integrated Cloud Security: Novel AI-based Traffic Record Transaction for Financial Sectors

K. Balaji[1*], Vaibhav Kaushik[2], M. Ulagammai[3], Lovish Dhingra[4], Ashish Kumar Kaushal[5], and Mohit Sharma[6]

[1*]Associate Professor, Department of Commerce and Management, Amrita Vishwa Vidya Peetham, Deemed University, Mysuru Campus, India. kbalaji@my.amrita.edu, https://orcid.org/0009-0002-1441-5154

[2]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. vaibhav.kaushik.orp@chitkara.edu.in, https://orcid.org/0009-0001-0234-3205

[3]Associate Professor, Saveetha Engineering College, Chennai, India. ulagammaimeyyappan@gmail.com, https://orcid.org/0000-0002-4771-1593

[4]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh, India. lovish.dhingra.orp@chitkara.edu.in, https://orcid.org/0009-0004-2848-0859

[5]Assistant Professor, Department of Jindal Global Business School, O P Jindal Global University, Sonepat, Haryana, India. ashishkiitd89@gmail.com, https://orcid.org/0009-0005-6330-505X

[6]Associate Professor, Symbiosis Law School, Noida, Symbiosis International (Deemed University), Pune, India. mohit9826@gmail.com, https://orcid.org/0000-0001-7576-2200

Received: April 09, 2025; Revised: May 24, 2025; Accepted: July 16, 2025; Published: August 30, 2025

Abstract

Today's world places more emphasis on smart device transactions for the financial sector, which configures a large number of programs that are capable of processing massive volumes of data effectively in response to the expanding requirement for service facilities from network edges. These enormous increases have led to addressing issues with the security of the system and the functionality of smart devices regarding critical transaction records for financial transactions. Service centers currently exchange transaction records across many platforms, recognition to blockchain technology. In this paper, research developed a Distributed Blockchain-learning cloud (DistB-Learning Cloud) architecture to address these problems for financial sectors. It combines blockchain technology, properties of cloud computing and machine learning (ML) to provide secure information transfers in peer-to-peer systems and efficient data-sharing services. There are four design models in this methodology. Initially, an attack detection approach uses a Support Vector Machine (SVM), using a transaction network-based anomalous traffic detector to locate the attack in the financial sector. Second, to manage risks and confirm the process of identity verification for secure transactions, a novel model for a blockchain transaction network is created using a Crypto-Aware Elliptic Curve (CAEC) and encryption. The ML model is then trained for the output prediction by logistic regression (LR) of the large-scale transaction record. In conclusion, a cloud assessment model facilitates the management of transaction records that are maintained and

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 50-61.
DOI: *10.58346/JISIS.2025.I3.004*

*Corresponding author: Associate Professor, Department of Commerce and Management, Amrita Vishwa Vidya Peetham, Deemed University, Mysuru campus, India.

accessible sharing of services that each service center has access to several cloud platforms. The results of the experiments show that the DistB-learningCloud performs higher than existing schemes in terms of achieving more transactions in each block for the financial sector.

Keywords: Blockchain, Machine Learning (ML), Cloud Service, Security Attacks, Transaction Network, Financial Sectors.

1 Introduction

Cloud computing is viewed as a key facilitator of Information technology (IT) sector innovation in the linked world of today. In addition to a variety of on-demand financial services, this approach provides users with network utilization of a collective database of physical resources, including processing power and storage. Customers at present utilize commodity gear, such as a laptop, linked to the internet, rather than having to buy pricey technology to access these services, enabling them to solve challenging issues (Rahman et al., 2023). The issues faced by financial institutions in maintaining network security (Krishna & Tyagi, 2020) have become more intense due to the growing interconnectivity of systems, the widespread use of mobile devices, the Internet of Things (IoT) and the growing use of cloud computing (Kumari et al., 2020). The cyber attacks could have a large financial impact on financial organizations (Elankavi et al., 2017), resulting in large losses and harm to their reputation. An analysis conducted, for example, discovered that cash holdings might rise from a starting position of 23% of assets to 26.87% as a result of cyber attacks. Companies are moving to reduce the financial impact of potential cyber attacks, as demonstrated by this rise in cash holdings (Liu et al., 2022). According to research, further consequences of reputational harm include a decline in company value, a poorer performance in the stock market, a decline in operating performance, a drop in the number of mergers and acquisitions, a loss of clients and an increase in financing costs. This demonstrates the serious impact that a cyber attack might have on an organization's finances and standing (Li et al., 2020). Despite offering layered security, protections that follow the defence-in-depth approach and conventional perimeter defences have proven inadequate in dealing with complex internal and external threats. When threats breach network perimeters, these models are not able to handle them effectively and frequently find it complex to dynamically adjust to shifting threat environments (Daah et al., 2024). To solve these issues, the Distributed Blockchain-learning Cloud (DistB-learning Cloud) architecture was created and suggested in this work. It integrates ML, blockchain (Vij & Prashant, 2024) technology and the foundations of cloud computing to provide safe data transfers in peer-to-peer networks and efficient data-sharing services.

The article's portions are separated as follows: Portion 2 presents a related work. The explorations of the proposed methodology are provided in portion 3. The simulation findings and discussions were determined in portion 4. Conclusions are provided in portion 5.

2 Related Works

Hemamalini et al., (2024) presented a cloud-based architecture that integrates blockchain, IoT and Artificial Intelligence (AI). The proposed architecture provided a stable and secure foundation for data analysis and interchange, enabling the development of intelligent algorithms that improve productivity and efficiency while raising living standards. (Ayaz, 2019; Kumar et al., 2023) proposed this vacuum by characterizing the uses and advantages of blockchain-enabled, integrated AI systems across several business verticals. (Saba et al., 2023) protected financial transactions using software-defined network (SDN) architecture's intelligent services by presenting an efficient blockchain architecture for high-end

processing in a huge information setting. (Wong et al., 2021) used large data processing and analytics, scalability, as well as technical sustainability. The use of the suggested technology architecture for real-time marine risk management identification to achieve technically sustainable development was illustrated through a case study. (Nguyen et al., 2020; Huang, 2024) proposed decentralization, data privacy and network security. Blockchain offered novel ways to solve problems in this context, and the cloud of things provided scalability and elasticity to improve the effectiveness of blockchain operations (Huang, 2024; Kim et al., 2022) described a security mechanism that uses data collection and anomaly detection to identify harmful occurrences. (Awotunde et al., 2023) presented a hybrid convolutional neural network (CNN) with Kernel principal component analysis (KPCA) enabled by blockchain to offer security and privacy to users and systems in smart cities. (Yang, 2024; Hemamalini et al., 2024) presented a revolutionary method of cybersecurity analysis based on blockchain technology for fuzzy machine learning and smart cloud computing (Leema, et al., 2024), both rooted in electric car technology. (Philip & Saravanaguru, 2023) presented a revolutionary method of cybersecurity analysis based on blockchain technology for fuzzy machine learning and smart cloud computing, both rooted in electric car technology. (Selvarajan et al., 2023) preserved the privacy and security of IIoT systems, creating a lightweight blockchain security model (AILBSM) driven by AI was the project's objective (Rakesh et al., 2024). The study made a unique contribution by combining enhanced security operations and a streamlined process with the benefits of lightweight blockchain and Convivial Optimized Sprinter Neural Network (COSNN) based AI techniques. (Shahbazi & Byun, 2021) anticipated taxi demand pick-up and drop-off information, as well as reducing the opportunity for unregistered individuals to exploit taxi services for fraudulent activities. It was thought that this issue was resolved by combining Machine learning (ML) methods with the blockchain infrastructure. (Krishna & Tyagi, 2020) used the innovative idea of blockchain technology to defend IoT-based intelligent transportation systems (ITS). By putting out a unique solution known as PChain using Blockchain Technology (BT), we were able to greatly enhance the applications of ITS. (Alkadi et al., 2020) provided smart contracts on a privacy-based blockchain and security using IoT network distributed intrusion detection and suggested a deep blockchain framework (DBF). Unal et al., (2021) suggested utilizing blockchain technology to protect Federated learning (FL) algorithms running in Internet of Things (IoT) systems form attack. The utilization of blockchain and FL combined to safeguard the validity of trained models and prevent simulation-related concerns.

3 Proposed Method

A secure cloud computing architecture called Dist B-Learning Cloud was created to defend transaction networks from financial intrusions. To guarantee data availability, efficiency and integrity, it integrates blockchain, machine learning and cloud computing technologies. The design detects system security vulnerabilities using an anomalous traffic detector for the financial sector based on support vector machines (SVMs). Additionally, it employs blockchain technology's encryption and Diffie-Hellman key exchange function (CAEC) to verify identities and thwart transaction assaults. To gather comprehensive transaction data and predict transaction outcome, the ML model is repeated several times, as shown in Figure 1.

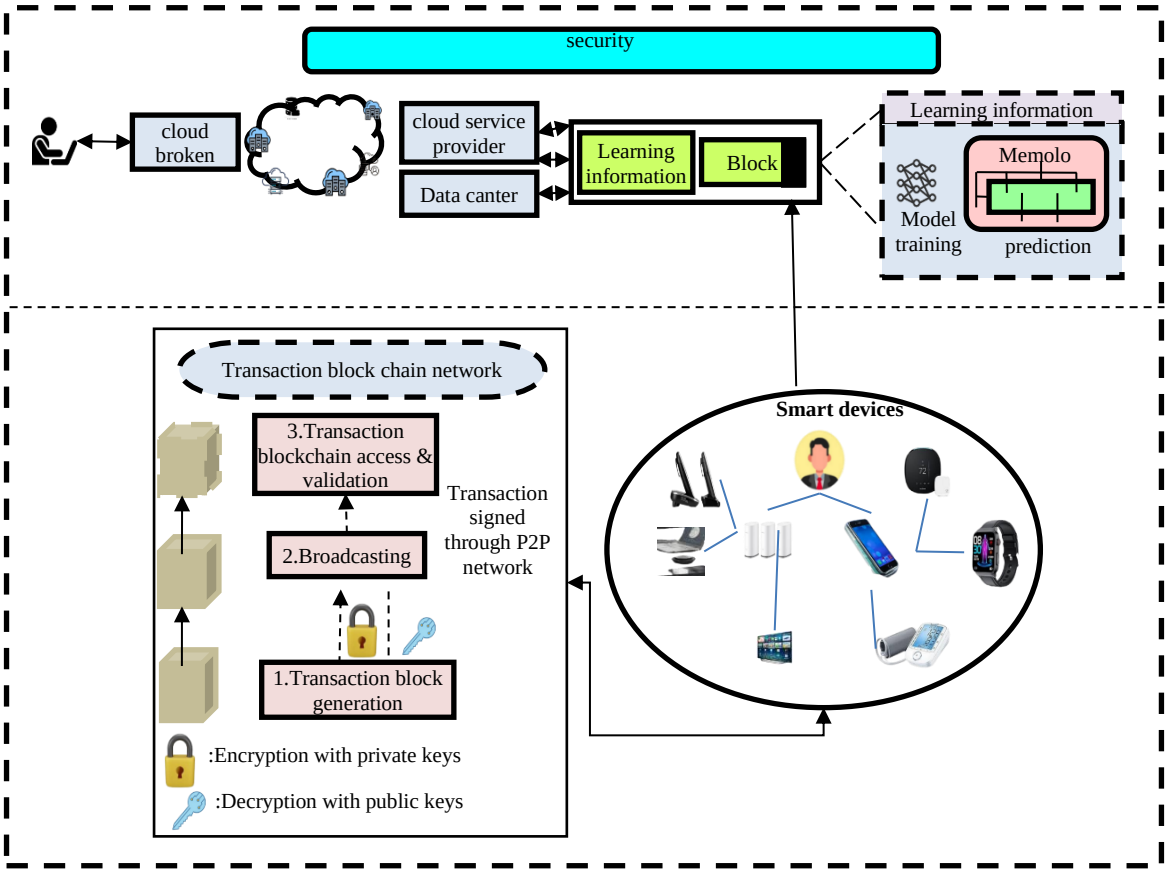

Figure 1: Flow Architecture for the Proposed Method

3.1 DS2OS Dataset

The Distributed Smart Space Orchestration System (DS2OS) is a publicly accessible open-source dataset on Kaggle (https://www.kaggle.com/francoisxa/ds2ostraffictraces). The traces collected in the DS2OS context of the IoT are included in the data collection. Compared to conventional network traces, it originates in the application layer. Four simulated IoT locations with various functions, including washing machines, batteries, thermostats, light controllers, thermometers, movement sensors, smart doors and smartphones, were used to collect the images.

3.2 Attack Detection Model Using Support Vector Machine (SVM)

The next two elements locate and examine anomalous traffic for the financial sector within the system security assaults before providing the attack detection model for financial.

Legitimate traffic analyzer: By examining traffic patterns at the packet and traffic levels, including bandwidth application, user requests, forwarding needed for smart devices and device usage frequency, the analyzer categorizes legitimate internet flow in the financial sector. To categorize internet flow, it also detects known attack patterns, such as assaults and transmission control protocol (TCP) flooding.

Legitimate traffic classifier: To prepare for attack detection, this component categorizes traffic attacks on blockchain networks for financial purposes. The SVM provides the best solutions to difficulties like local optimum and over-fitting, regression evaluation, and pattern recognition represent two methods from many applications that utilizing the SVM model. A quadratic programming (QP)

issue is converted into linear equations using a larger instance of the traditional SVM model. The method is efficient in high-dimensional instances, where the number of dimensions exceeds the number of samples. Classifying attacks using the distinct design of the SVM classifier is the main intention of this research. Figure 2 depicts its general architecture.

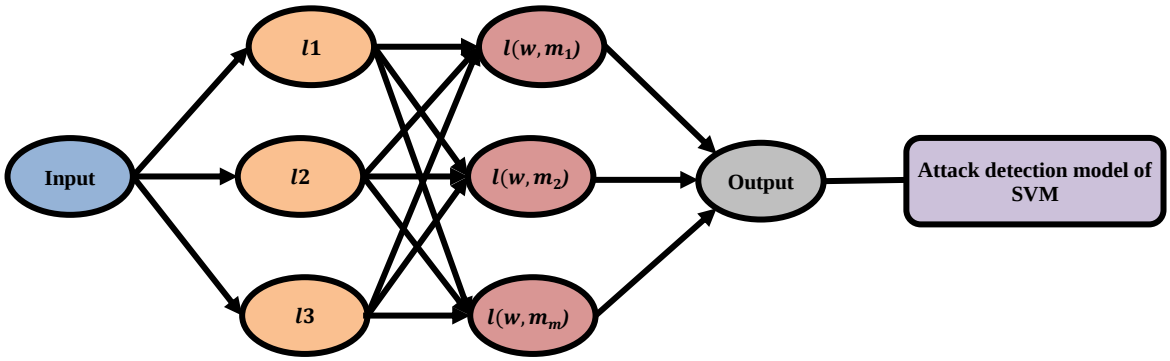

Figure 2: Framework for SVM Architecture

In the input layer, there is a vector input signal (x) and it is computed between the support vector (s) and the input signal vectors (x) in hidden layer (y). The output neuron combines the linear signals O Ofz the hidden layer neurons. Attack detection in the financial sector is comparable with the two classification issues, apply the benefits of the SVM algorithm, obtain transform data to obtain unique values, identify the optimal hyper-plane for classifying the data from regular and attacking sources, and obtain the results of classification by establishing the proposed framework by employing the test information (Equation (1)).

$$O = \sum W_i k(x_i s_i) \quad (1)$$

The hyperplane called decision performance is the primary function of SVM, that employed for concerns with uneven binary classification (Equation (2)).

$$z(y) = u^D y + p = 0 \quad (2)$$

Where bias $p \epsilon K$ and weighted vector $u \epsilon K^M$. The bounded issue of an SVM with the largest margin hyperplane, Equation (3), is presented below.

$$\min_{u,p,\beta_-,\beta_+} \frac{1}{2}\|u\|^2 + b_-\beta_- + b_+\beta_+ s.t. Y_- u + b_- p \le b_- - \beta_- Y_+ u + b_+ p \le v_+ - \beta_+\beta_- \ge 0 \quad (3)$$

Penalty parameters for regulating the weights within the elements of both negative and positive classes are b_- and b_+, where the normalization $\frac{1}{2}\|u\|^2$ provides the highest margins across two adjacent hyperplanes. The variables $\beta +$ and $\beta -$ represents the slack variables of both categories. The vectors used for the positive and negative classes are represented by b_- and b_+, with the variables Y_+ andY_-, which indicates the trained matrices for the adverse classes.

3.3 Blockchain Transaction Network Model Using Crypto-Aware Elliptic Curve (CAEC)

The encryption process employs the ECC algorithm following the creation of the shares. The elliptical curve cryptography (ECC) is a cryptographic technique based on the algebraic framework of elliptic curves moving across finite spaces of financial applications. The comparable level of financial protection uses non-EC encryption. At the ECC, the greatest possible value is selected as n_P, and an encryption key is used most frequently. Equation (4) is presented below.

$$F = o(j)^3 + v * o(j) + u \quad (4)$$

Where v and u stands for the constant value $v = u = 2$. When state $W = Z$ occurs, the ECC's best points were selected and the variables $Z$and W was indicated in Equation (5).

$$W = mod(F, m_o)$$
$$Z = mod(o(i)^2, m_o) \quad (5)$$

The expression $O(j, i)$ denotes the intersection of the elliptic curve. The prime number is denoted as n_P. This doubling approach is used to define Z and W values. The optimal point $O_f(k, l)$ and O_e, displayed below that indicates a widely used key, shown in Equation (6).

$$O_e = G * O_f \quad (6)$$

The encryption procedure allocates each share into the collection of blocks, and each block has encrypted portions. Blocks are represented by rows and columns B (i, j), whereas the overall block quantity is represented by j and i. Each of the data points is presently offered as input for data encryption. The following Equation (7) expresses the information $C_z(j\ +\ 1, i)$ and $C_w(j, i)$ is determined.

$$D_1 = G * O_f,$$
$$D_2 = (C_w, C_z) + D_1 \quad (7)$$

The decryption method implements the private key (H) for communication, decryption, and point D_{11} for pixel decryption, is stated in Equation (8).

$$D_{11} = G * D_1,$$
$$D_{ji} = D_2 - D_{11} \quad (8)$$

In the D_{ji}, the decryption process's output is provided. Pixel values for IR and the initial colored bands are kept distinct from the D_{ji}outputs.

3.4 Enhancement of Extensive Transaction Records Using Logistic Regression (LR)

Applications of the logistic regression model is widely used in a variety of fields, including the biological sciences. When categorizing data objects into groups is the goal, the LR procedure is employed.

$$z = g_\theta(w) = \theta^S w \quad (9)$$

To attack a binary value $(z^{(j)} \varepsilon \{0,1\})$, equation (9) proves highly ineffective. As a result, that introduces a function in equation (10) to forecast whether a specific patient (with specified characteristics) is more likely to be in the "1" (positive) class than the "0" (negative) class.

$$O(z = 1|w) = g_\theta(w) = \frac{1}{1 + \exp(-\theta^S w)} \equiv \sigma(\theta^S w)$$
$$(O(z = 0|w) = 1 - O(z = 1|w) = 1 - g_\theta(w) \quad (10)$$

By using the sigmoid function, or equation (11), maintain the value of $\theta^S w$ inside the [0,1] range. Next, look for a value of θ such that, for every x in the "1" class, the probability $O(z = 1|w) = g_\theta(w)$ is great and for every x in the "0" class, it is small.

$$\sigma^{(S)} = \frac{1}{(1 - f^{-S})} \quad (11)$$

The output and outcome are covered in the next part once our logistic regression technique has been successfully modelled and put into practice.

3.5 Cloud Evaluation Framework

A single interface for managing numerous clouds and resources for data interchange with customers' dispersed data services is offered by the cloud assessment model. For effective transaction record data

gathering in large companies, the private cloud model, which is backed by CAEC, integrates cloud and services. It's perfect for companies that prioritize computing power, security and information sharing services since it offers instantaneous services, lowers attack threats and enables consumers to accept dependable transactions:

Cloud Service with Several Users

The cloud service manages user requests and offers digitally signed transaction records. It is made up of a data center, a cloud broker and a CSP. In addition to strengthening multi-tenancy structures and safeguarding data from hackers, the data center also oversees virtualization and remote access. Information centers facilitate access from three components by managing redundancy, numerous locations and multiple services:

- **Clients:** The customer chooses the most suitable CSP.
- **CSP:** The service provider has direct access to the resources for data exchange amongst themselves for the combined cloud service of their operations.
- **Public clouds:** This includes the scheduling enabler and public directory access for the cloud service specified.

Cloud computing comprises an interchange service in virtualized services and permits access to transaction records in information centers. It manages services for smart devices, with an emphasis on resources for data sharing. In multi-tenancy cloud services, network resources and storage oversee related resources:

Service analyzer: The decision to approve or decline the client's requests is made by gathering and analyzing the submitted requests. The cloud platform's aggregated service is provided by the updated load services across VMs and cloud brokers.

Service scheduler: Taking into account the immense number of smart gadgets that are linked to residences, infrastructure and cities. The virtual machines (VMs) are then assigned the data-sharing resources, and the client request is assigned to the VM.

Resource analysis: Efficiently, the resource analyzer provides the client with the stored transaction data. Cloud computing is improved by data center resource pooling, which reduces the latency and energy use of smart devices. The client's requested distributed resource is also managed by the resource analyzer.

4 Results and Discussion

The following is a description of the simulation parameter settings. An 8 GB RAM computer system based on a CPU, the 2 GHz Intel Core i7 processor and 256 GB of storage is the gear utilized in this instance. Furthermore, Tensor-Flow 1.4.0 and Python 3.6.8 are used in the software development process. The efficacy of the suggested DistB-LearningCloud is evaluated in comparison to various existing methods, among these are Blockchain distributed machine learning (BC-DML) (Pon & V, 2022), blockchain-based smart homes that combine cloud computing and blockchain (SH-Block CC) (Pon & V, 2022), blockchain-assisted security for Internet of Things network (BlockSecIoTNet) (Pon & V, 2022), and blockchain-authorized blockchain in medical cloud servers (ABC-MCS) (Pon & V, 2022). The purpose of these comparisons is to assess the consequences of computing cost, computational complexity, mining blocks, throughput and transaction delay.

Throughput: It determines the transaction flow rate handled by the blockchain network using a combination of different operations for reading and writing at different transaction sending rates. Seconds (s) are used to measure. As follows, Equation (12) constant Bit Rate is shortened to CBR. The assault case is identified by the fluctuating time in seconds (s) at which the attack occurred. Throughput is drastically reduced compared to other techniques when a system assault happens. Typically, as the volume of requests rises, an attack would not occur. Consequently, Figure 3 (a, b) compares the DistB-learningCloud comparative findings, which indicate greater throughput in both the attack and normal cases.

$$\text{Throughput} = \frac{\sum_{n=i}^{n} \text{CBRrece}}{\text{Simulation time}} \quad (12)$$

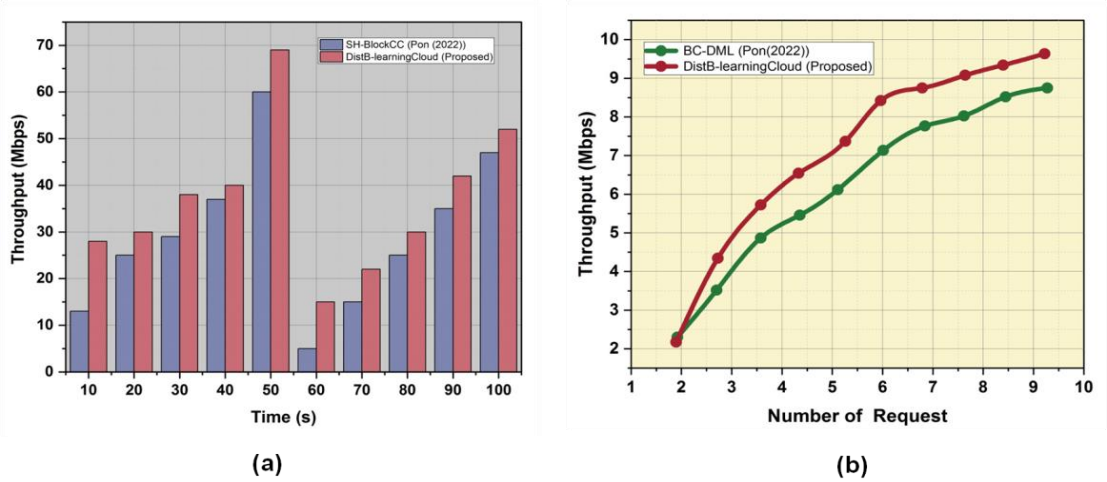

Figure 3: Comparison of the Throughput, (a) Attack, (b) Normal

Transaction latency: This processing time is referred to as the original broadcast transaction time (T), assuming different block sizes, transaction sending rates and transaction numbers. The client transmits to the P2P network ledger for processing. Figure 4 illustrates how the suggested DistB-learning Cloud provides lower transaction latency than the BC-DML system. Here, up to 500 cycles, the existing BC-DML approach's computing time coverage is more than 18 times lower than the suggested design.

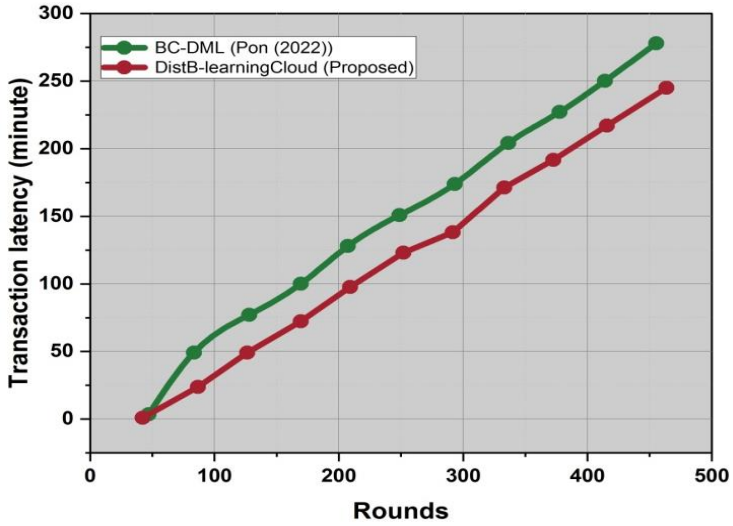

Figure 4: Comparison of the Transaction Latency

Computation cost: The execution time for every time step in a simulation is the computation cost. To find out how long the model takes to execute on real-time hardware, the execution-time budget of the experiment on an actual-time target system is determined. The computing costs of the suggested technique take advantage of lower costs than the existing ABC-MCS scheme, as shown by the study in Figure 5.

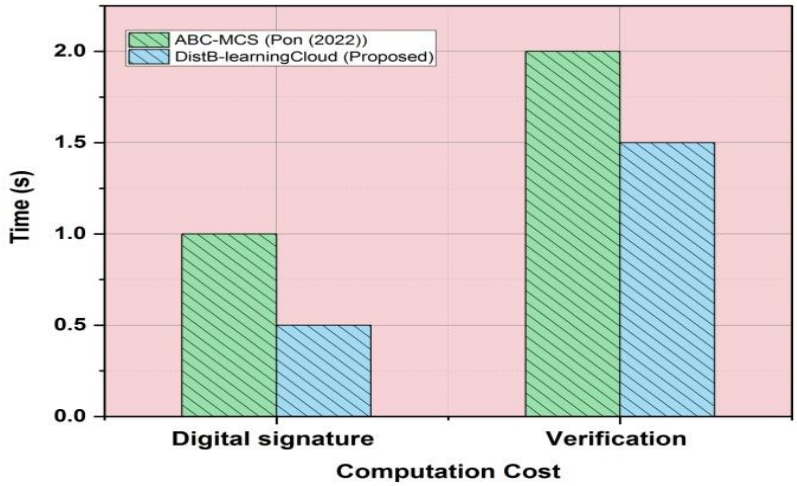

Figure 5: Comparison of the Computation Cost

Computational complexity: The study of mathematical complexity focuses on the least resources required to solve issues related to computing. Specifically, it attempts to differentiate situations that are intrinsically intractable from those that have methods of operation. Figure 6 illustrates the total computing complexity of the suggested approach versus the existing technique.

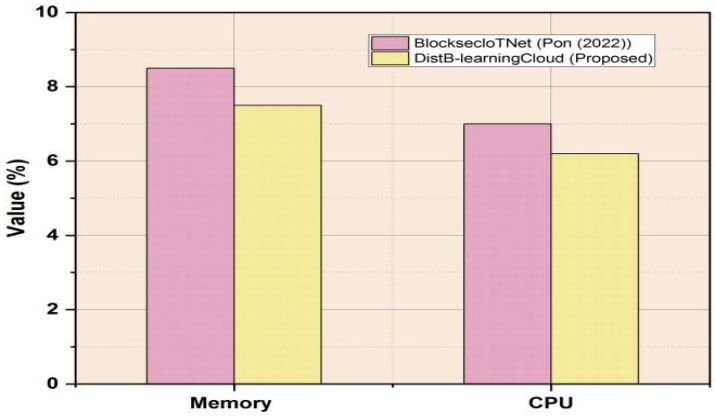

Figure 6: Comparison of the Computational Complexity

5 Conclusion

Attacks cause unsecured data transactions on a large number of smart devices as the transaction network's demand rises. To provide a safe traffic flow access transaction system for the financial sector, they presented a DistB-learning Cloud architecture in the article that is built on blockchain and ML technology in cloud computing. Based on four architectural concepts, the DistB-learning Cloud primarily focuses on financial security and storage computation issues. Initially, system security assaults

are intended to be detected by the attack detection model using SVM. Subsequently, an LR is employed to enhance the transaction production forecast. Enhancing the efficacy of cloud services is the intent of the cloud evaluation framework, which provides a user-friendly environment for managing saved record transactions across various cloud platforms. The evaluation's findings show that a high degree of service is estimated for each block by the DistB-learning Cloud security architecture of traffic information transactions for the financial sector. The low computation cost (0.5 s) is achieved during the performance. To increase the effectiveness and security of information from smart devices, the whole security architecture guards against assaults for financial transactions in financial institutions. In further research, I intend to expand the blockchain operational systems into several fields that are potentially useful in urgent and important applications.

References

[1] Alkadi, O., Moustafa, N., Turnbull, B., &Choo, K. K. R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet of Things Journal*, 8(12), 9463-9472. https://doi.org/10.1109/JIOT.2020.2996590

[2] Awotunde, J. B., Gaber, T., Prasad, L. N., Folorunso, S. O., &Lalitha, V. L. (2023). Privacy and security enhancement of smart cities using hybrid deep learning-enabled blockchain. *Scalable Computing: Practice and Experience*, 24(3), 561-584. https://doi.org/10.12694/scpe.v24i3.2272

[3] Ayaz, A. T. (2019). The Role of International Non-governmental Organizations (NGO) in preserving international peace and security. *International Academic Journal of Social Sciences, 6*(1), 62–66. https://doi.org/10.9756/IAJSS/V6I1/1910006

[4] Daah, C., Qureshi, A., Awan, I., &Konur, S. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: *A Proposed Framework. Electronics, 13*(5), 865. https://doi.org/10.3390/electronics13050865

[5] Elankavi, R., Kalaiprasath, R., & Udayakumar, R. (2017). A fast clustering algorithm for high-dimensional data. International *Journal Of Civil Engineering And Technology (Ijciet), 8*(5), 1220-1227.

[6] Hemamalini, V., Mishra, A. K., Tyagi, A. K., &Kakulapati, V. (2024). Artificial Intelligence–Blockchain-Enabled–Internet of Things-Based Cloud Applications for Next-Generation Society. *Automated Secure Computing for Next-Generation Systems*, 65-82. https://doi.org/10.1002/9781394213948.ch4

[7] Huang, J. (2024). Impact of Non-performing Corporate Assets on Shareholder's Equity and Return on the Application of AI and Block Chain Technologies. *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl, 15*(3), 412-423. https://doi.org/10.58346/JOWUA.2024.I3.027

[8] Kim, J., Nakashima, M., Fan, W., Wuthier, S., Zhou, X., Kim, I., & Chang, S. Y. (2022). A machine learning approach to anomaly detection based on traffic monitoring for secure blockchain networking. *IEEE Transactions on Network and Service Management*, 19(3), 3619-3632. https://doi.org/10.1109/TNSM.2022.3173598

[9] Krishna, A. M., &Tyagi, A. K. (2020, February). Intrusion detection in intelligent transportation systems and its applications using blockchain technology. *In 2020 international conference on emerging trends in information technology and engineering (IC-ETITE)* (pp. 1-8). IEEE. https://doi.org/10.1109/ic-ETITE47903.2020.332

[10] Kumar, S., Lim, W. M., Sivarajah, U., & Kaur, J. (2023). Artificial intelligence and blockchain integration in business: trends from a bibliometric-content analysis. *Information Systems Frontiers*, 25(2), 871-896. https://doi.org/10.1007/s10796-022-10279-0

[11] Kumari, A., Gupta, R., Tanwar, S., & Kumar, N. (2020). Blockchain and AI amalgamation for energy cloud management: Challenges, solutions, and future directions. *Journal of Parallel and Distributed Computing, 143*, 148-166. https://doi.org/10.1016/j.jpdc.2020.05.004

[12] Leema, A. A., Balakrishnan, P., & Jothiaruna, N. (2024). Harnessing the power of web scraping and machine learning to uncover customer empathy from online reviews. *Indian Journal of Information Sources and Services, 14*(3), 52-63. https://doi.org/10.51983/ijiss-2024.14.3.08

[13] Li, W., Su, Z., Li, R., Zhang, K., & Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6G networks. *IEEE Network*, 34(6), 31-37. https://doi.org/10.1109/MNET.021.1900629

[14] Liu, Y., Hao, X., Ren, W., Xiong, R., Zhu, T., Choo, K. K. R., & Min, G. (2022). A blockchain-based decentralized, fair, and authenticated information-sharing scheme in zero trust internet-of-things. *IEEE Transactions on Computers*, *72*(2), 501-512. https://doi.org/10.1109/TC.2022.3157996

[15] Nguyen, D. C., Pathirana, P. N., Ding, M., &Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications and challenges. *IEEE Communications surveys & tutorials*, 22(4), 2521-2549. https://doi.org/10.1109/COMST.2020.3020092

[16] Philip, A. O., &Saravanaguru, R. K. (2023). Multisource traffic incident reporting and evidence management in Internet of Vehicles using machine learning and blockchain. *Engineering Applications of Artificial Intelligence*, *117*, 105630. https://doi.org/10.1016/j.engappai.2022.105630

[17] Pon, P., & V, K. (2022). Blockchain-based cloud service security architecture with distributed machine learning for smart device traffic record transactions. *Concurrency and Computation: Practice and Experience*, 34(3), e683. https://doi.org/10.1002/cpe.6583

[18] Rahman, A., Islam, M. J., Band, S. S., Muhammad, G., Hasan, K., &Tiwari, P. (2023). Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. *Digital Communications and Networks*, 9(2), 411-421. https://doi.org/10.1016/j.dcan.2022.11.003

[19] Rakesh, N., Mohan, B. A., Kumaran, U., Prakash, G. L., Arul, R., & Thirugnanasambandam, K. (2024). Machine learning-driven strategies for customer retention and financial improvement. *Archives for Technical Sciences, 2*(31), 269–283. https://doi.org/10.70102/afts.2024.1631.269

[20] Saba, T., Haseeb, K., Rehman, A., & Jeon, G. (2023). Blockchain-enabled intelligent iot protocol for high-performance and secured big financial data transaction. *IEEE Transactions on Computational Social Systems*, *11*(2), 1667-1674. https://doi.org/10.1109/TCSS.2023.3268592

[21] Selvarajan, S., Srivastava, G., Khadidos, A. O., Khadidos, A. O., Baza, M., Alshehri, A., & Lin, J. C. W. (2023). An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. *Journal of Cloud Computing*, 12(1), 38. https://doi.org/10.1186/s13677-023-00412-y

[22] Shahbazi, Z., &Byun, Y. C. (2021). A framework of vehicular security and demand service prediction based on data analysis integrated with a blockchain approach. *Sensors*, *21*(10), 3314. https://doi.org/10.3390/s21103314

[23] Unal, D., Hammoudeh, M., Khan, M. A., Abuarqoub, A., Epiphaniou, G., &Hamila, R. (2021). Integration of federated machine learning and blockchain for the provision of secure big data analytics for the Internet of Things. *Computers & Security*, 109, 102393. https://doi.org/10.1016/j.cose.2021.102393

[24] Vij, P., & Prashant, P. M. (2024). Predicting aquatic ecosystem health using machine learning algorithms. *International Journal of Aquatic Research and Environmental Studies, 4*(S1), 39-44. https://doi.org/10.70102/IJARES/V4S1/7

[25] Wong, S., Yeung, J. K. W., Lau, Y. Y., & So, J. (2021). Technical sustainability of cloud-based blockchain integrated with machine learning for supply chain management. *Sustainability*, *13*(15), 8270. https://doi.org/10.3390/su13158270

[26] Yang, P. (2024). Electric vehicle-based smart cloud model cyber security analysis using fuzzy machine learning with blockchain technique. *Computers and Electrical Engineering*, *115*, 109111. https://doi.org/10.1016/j.compeleceng.2024.109111

Authors Biography

K. Balaji is an Associate Professor in the Department of Commerce and Management at Amrita Vishwa Vidyapeetham (Deemed University), Mysuru Campus, India. He is actively engaged in teaching, research, and academic development in the areas of commerce, management, and business studies. His work focuses on developing industry-relevant skills among students and contributing to the academic community through research and publication.

Vaibhav Kaushik is affiliated with the Centre of Research Impact and Outcome at Chitkara University, Rajpura, Punjab, India. His work focuses on advancing research effectiveness and promoting data-driven academic and societal outcomes. He is involved in supporting interdisciplinary initiatives and enhancing the visibility and impact of scholarly research.

M. Ulagammai is an Associate Professor at Saveetha Engineering College, Chennai, India. With a strong academic background and extensive teaching experience, her expertise lies in engineering education and research. She is committed to fostering innovation and analytical thinking among students, and actively contributes to the academic community through scholarly research and collaboration.

Lovish Dhingra is affiliated with the Chitkara Centre for Research and Development at Chitkara University, Himachal Pradesh, India. His work focuses on advancing interdisciplinary research and fostering innovation through academic collaboration and evidence-based practices. He is actively involved in initiatives aimed at enhancing research quality and impact across diverse fields.

Ashish Kumar Kaushal is an Assistant Professor at Jindal Global Business School, O. P. Jindal Global University, Sonepat, Haryana, India. He brings a strong academic foundation and practical insight to the field of business and management studies. His teaching and research interests span areas such as organizational behavior, strategic management, and contemporary business practices. He is committed to nurturing future business leaders through innovative teaching and scholarly engagement.

Mohit Sharma is an Associate Professor at Symbiosis Law School, Noida, a constituent of Symbiosis International (Deemed University), Pune, India. He has substantial experience in legal education and research, with interests spanning constitutional law, legal theory, and interdisciplinary legal studies. He is actively involved in academic development, curriculum enhancement, and scholarly publications.