International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 03-07-2020; Accepted: 04-08-2020
www.allmultidisciplinaryjournal.com
Volume 1; Issue 4; July - August 2020; Page No. 67-76

Enhance Cloud Security for Financial Data with Blockchain Integration and ECC Encryption

Maciej Motak
Bialystok University of Technology, Białystok, Poland

Corresponding Author: **Maciej Motak**

DOI: https://doi.org/10.54660/.IJMRGE.2020.1.4.67-76

Abstract
Cloud computing quickly transformed financial data management into scalable and efficient solutions. Benefits are coupled with substantial security threats requiring robust protection. Innovative security architecture that integrates Blockchain technology with Elliptic Curve Cryptography to enhance financial data security in cloud platforms has been suggested. Blockchain provides data with transparency and immutability by reducing possibility of illegal interference and ECC provides strong encryption at low processing expenses. BERT and GPT are better at identifying anomalies and making predictions. AI algorithms identify fraudulent transactions through monitoring cultural patterns in transactions and behavioral irregularities. This encompasses secure cloud storage technologies employing distributed ledgers and encrypted announcement channels to prevent data breaches and illegal access. It is tested with financial datasets proving improvements in business security, encryption speed and fraud detection accuracy. Experimental results reveal 99.2 percent security strength with low latency and computational overhead suitable for secure cloud-based economic services. Smart contracts ease verification operations ensuring adherence to financial security regulations and highpoints essential role of Blockchain and ECC in enhancing cloud security and lays foundation for future research into financial cybersecurity. Emphasize importance of combining AI-driven fraud detection with top-level encryption methods to create adaptive, expandable and secure financial system.

Keywords: Cloud Security, Blockchain, Elliptic Curve Cryptography Encryption, Financial Data Protection, AI-based Fraud Detection, Smart Contracts

1. Introduction
Cloud computing has transformed data organization by providing ascendable and adaptable solutions until now safeguarding banking cloud services remained crucial owing to changing cyber threats [1]. Big Data Analytics and Artificial Intelligence tactics improve security outlines by identifying fraudulent transactions and providing real-time threat assessments [2]. AES encryption protects sensitive monetarist transactions while technologies such as ECC offer enhanced encryption effectiveness at lower computational expenses [3]. Blockchain-based data exchange offers immutability and transparency for the protection of financial data against tampering and unauthorized alterations. Artificial intelligence-based data analysis enhances identification of scam and predictive analysis through analyzing transaction patterns with DL methods [4]. Bi-directional LSTM with regressive dropout increases anomaly detection in accounting information streams increases dependability of fraud detection systems. IoMT-enabled diagnosis utilizes cloud-based AI models to protect data and allows early detection. CNN and Score-CAM improve feature visualization for detecting financial anomalies and harmful activity. Supply chain in finance industry provides end-to-end visibility and secure record-keeping throughout automotive supply chain. Database management and cloud solutions use encryption and blockchain technology prevent unauthorized access [5]. CNN with Edge Computing-based malware detection increases cybersecurity by finding malware trends in cloud settings. Devarajan and Pushpakumar (2019), [6] model leverages AES and RSA for secure cloud data encryption and transmission. Extending this concept, the implemented framework integrates ECC with blockchain to strengthen financial cloud security through lightweight encryption and immutable transaction records. Formulating approaches such as Dung Beetle Optimization with SVM aid risk valuation through sentiment analysis in financial markets [7]. Restricted Boltzmann Engines and Bi-directional Gated Recurrent Networks help detect fraud more effectively through incorporation of sophisticated transaction patterns. IoT services on edge computing guarantee safe data transfer between financial devices by minimizing latency and optimizing system efficiency [8]. Data analytics and mobile computing allow monitoring of financial activities assuring compliance with security regulations and regulatory standards.

CNNs and Variational Autoencoders are strong in fraud detection and anomaly detection in financial crime but weak in securing financial cloud services [9]. Large labeled datasets are needed for CNNs and they are inefficient with sequential transaction data by lowering their performance in blockchain-based fraud detection. Crow Search Optimization is not suitable for dealing with dynamic security attacks in cloud environments because it depends on random search behavior [10]. Statistical Frameworks for Improving AI Interpretability might also be less adaptable to changing encryption techniques like ECC. These restrictions underscore the need for more effective and scalable security frameworks designed specifically for cloud-based financial services. Advanced strategy for improving financial cloud security by combining blockchain integration and ECC encryption assuring confidentiality, integrity and resistance to attacks has been proposed [11].

In the rapidly advancing domain of financial technology, securing digital transactions and maintaining regulatory compliance demand intelligent, adaptive solutions. Techniques like Dung Beetle Optimization integrated with Support Vector Machines enhance risk valuation by analyzing market sentiment, while deep learning models such as Restricted Boltzmann Machines and Bidirectional Gated Recurrent Units improve fraud detection by capturing intricate transactional patterns [12]. Edge computing in IoT-based financial services ensures secure, low-latency data transmission across connected devices, boosting system responsiveness and reliability. Simultaneously, mobile computing and data analytics facilitate real-time monitoring and regulatory adherence. However, despite their strengths in anomaly and fraud detection, models like Convolutional Neural Networks and Variational Autoencoders face limitations in handling sequential blockchain data and securing financial cloud environments due to their reliance on large labeled datasets [13]. Furthermore, heuristic algorithms like Crow Search Optimization lack the adaptability needed to counter evolving cyber threats in dynamic cloud settings, and conventional statistical interpretability frameworks struggle to keep pace with modern encryption techniques such as Elliptic Curve Cryptography. These constraints underscore the necessity for a scalable, resilient security architecture. To address this, a novel strategy is proposed integrating blockchain with ECC encryption to ensure confidentiality, data integrity, and strong resistance to attacks within cloud-based financial ecosystems [14]. To overcome the limitations of current cybersecurity approaches in financial cloud environments such as the data-hungry nature of deep learning models like CNNs and VAEs, the rigidity of heuristic algorithms like Crow Search Optimization, and the insufficiency of traditional statistical frameworks in dealing with advanced encryption the proposed method introduces a unified, scalable architecture titled Enhance Cloud Security for Financial Data with Blockchain Integration and ECC Encryption. This approach integrates blockchain technology to ensure decentralized, tamper-proof storage and traceability of financial transactions, thereby enhancing data integrity and transparency. Simultaneously, it employs ECC, a lightweight yet powerful encryption method, to guarantee confidentiality and secure data exchange across cloud and IoT infrastructures. ECC's strength lies in its ability to provide high levels of security with lower computational overhead, making it especially suitable for real-time mobile and edge computing scenarios common in FinTech applications. By combining the immutability and consensus mechanisms of blockchain with the robust encryption of ECC, the proposed solution delivers enhanced resistance to cyber threats, supports regulatory compliance, and facilitates secure, low-latency financial operations. This integrated framework addresses the evolving challenges of fraud detection, privacy protection, and secure transaction handling in dynamic, cloud-based financial ecosystems. Kalyan Gattupalli (2019) [15] introduces a deep learning framework within CRM systems for accurate churn prediction using wavelet-based feature extraction and neural networks. Influenced by this, the proposed work utilizes AI with secure blockchain frameworks, thereby improving both predictive performance and data security in financial systems.

1.1 Problem Statement

Cloud-based deployments and strategic market shifts strengthen corporate synergy they create security threats through enhanced attack surfaces and data breaches. Machine learning, although strong in detecting fraud is usually plagued by biased training sets and adversarial attacks that compromise financial security [16]. YOLO for object detection and recognition even though efficient, is not precise enough for secure authentication in financial cloud settings. Secure authentication by Faster R-CNN is subject to computational burdens which slow and reduce scalability of financial verification [17]. Ensemble models with enhanced prediction quality add complexity and increased processing cost rendering them unsuitable in financial applications. AI and cloud unleash the potential of big data complicating data privacy and compliance through cross-border transfer of data [18].

A/B testing, contextual testing based on AI and codeless automation tools leave financial applications vulnerable to security loopholes by depending on automated decision-making. Hierarchical LDA, autoencoders and IsoMap for improved dimensionality reduction, while optimizing data processing hide important financial security patterns making them less interpretable [19]. Dynamic federated data integration and iterative e-commerce analytics pipelines based on hybrid cloud and edge computing, although improving scalability introduce synchronization problems and data inconsistencies that impact financial risk analyses [20]. Spiking neural architectures and modalities of edge computing are hampered by difficulties in deployment because of hardware limitations that hamper their capability to secure financial transactions in cloud infrastructures [21].

To address the multifaceted security and scalability challenges posed by existing methods in cloud-based financial systems such as biased machine learning models, imprecise or computationally heavy authentication mechanisms like YOLO and Faster R-CNN, the high complexity of ensemble models, and the interpretability limitations of dimensionality reduction techniques like autoencoders and IsoMap the proposed method offers a unified and resilient security framework. By integrating blockchain technology, the solution ensures decentralized, tamper-proof transaction records, mitigating risks from cross-border data transfers and synchronization inconsistencies introduced by hybrid cloud-edge infrastructures. Simultaneously, ECC delivers strong, lightweight encryption well-suited for securing real-time financial data across distributed platforms without the

computational burden of traditional cryptographic systems. This approach overcomes the interpretability and hardware deployment limitations of spiking neural networks and hierarchical models, while reducing reliance on error-prone automated decision-making from A/B and contextual testing. The combined use of blockchain and ECC guarantees data integrity, confidentiality, and scalability, making it a robust solution for enhancing cloud security in dynamic financial ecosystems. Grandhi and Kumar's (2019) [22] IoT-edge AI system reduces latency and enhances scalability in smart traffic management. Building upon this, the developed framework uses Immutable ledger frameworks combined with lightweight elliptic curve encryption to tackle scalability and security challenges in cloud-based financial systems, ensuring adaptive, efficient, and tamper-proof data protection across distributed platforms.

1.2 Objective

- Discuss security weaknesses in cloud-based financial systems and their implications on data confidentiality, integrity and availability.
- Implement Blockchain technology and ECC encryption to improve security controls in financial cloud infrastructures.
- Formulate AI-based fraud detection model using BERT and GPT to detect suspect financial transactions.
- Assess effectiveness and efficiency of suggested security framework.

2. Literature Survey

Rawat *et al*. [23] examined the need to Enhance Data Quality in financial data sets to increase fraud detection effectiveness. He further examined Big Data ability to detect cyber threat patterns within cloud systems. Bi-directional Long-Short Term Memory-based DNN increases predictive analytics in economic field estimates computational efficiency and difficulties were discovered. Abuarqoub [24] examined authentication and access control mechanisms in cloud financial transactions emphasizing multi-factor authentication to prevent illegal access. Neural Networks were implemented on Harmony Search Algorithm tuning anomaly detection of cloud financial services.

Herold, & Lee, [25] emphasized Progressing Sustainable Development in cloud security for finance by examining sustainability-high performance encryption trade-offs. Hybrid Clustering and Evolutionary Algorithms were tested for optimizing fraudulent activity detection in financial big data Insights of Semi-Stream Joins with MongoDB improved real-time monitoring of transactions within hybrid clouds. Artificial Intelligence and IaaS Reliability Verification Methods enhance cloud-based financial services trust [26]. Data Transfer and Security in Hybrid Clouds were investigated using federated learning frameworks to provide secure and efficient financial data flow. The Isolation Forest Integrated Ensemble Machine Learning Algorithm was used to identify outliers in financial data and reduce false positives in fraud detection.

Rahi *et al*., [27] discussed Transaction Security stressing encryption-based methods to safeguard financial transactions. An Authorized Public Accounting Scheme for Dynamic Big Data was presented to assure transactions integrity. They also covered Supply Chains with a focus on risk management measures in cloud-based financial processes. The Hybrid Clustering and Evolving Algorithms to demonstrate its effectiveness in detecting fraud patterns [28]. Data Sharing and Security in Hybrid Cloud Environments with Data Fusion Approach was used to improve transaction visibility and compliance with financial regulations.

Schmitz, J, & Leoni, G. [29] proposed a blockchain-based audit trail system to enhance transparency and accountability in financial transactions, reducing the risk of tampering and unauthorized access. Malikireddy, S. K. R., & Algubelli [30] investigated the use of Homomorphic Encryption and Secure Multi-Party Computation to perform encrypted financial analytics without exposing sensitive data, ensuring privacy-preserving computation. Gopireddy [31] introduced a Federated Learning framework for fraud detection, allowing decentralized model training across financial institutions while preserving data confidentiality.

Meanwhile, Howard [32] applied Swarm Intelligence algorithms combined with Deep Neural Networks to identify evolving fraud patterns, improving detection rates in dynamic transaction environments. Additionally, researchers like Khurana, R., & Kaul, D [33] explored ZTA for cloud financial systems, focusing on continuous verification and least privilege access to reduce the attack surface and insider threats. These studies collectively highlight the ongoing efforts to balance performance, security, and compliance in the digital transformation of financial systems. Deevi, D. P., & Padmavathy (2019) [34] develops a hybrid Random Forest and GRU approach delivers high-accuracy heart disease prediction using cloud-hosted data. Motivated by their integration of ensemble and deep learning within secure environments, the proposed framework adapts this hybrid methodology with ECC encryption to enhance financial cloud security and fraud analytics.

3. Methodology

The proposed framework for enhancing financial cloud security adopts a robust multi-stage architecture that seamlessly integrates advanced data preprocessing, lightweight encryption, blockchain technology, and AI-driven analytics to ensure secure, efficient, and intelligent financial data management [35]. The pipeline initiates with the ingestion of raw financial data, which typically contains inconsistencies, noise, and redundant entries factors that can undermine both the accuracy of analytics and the integrity of security mechanisms. To mitigate these issues, the data is first subjected to a comprehensive preprocessing stage that includes normalization, noise reduction, and anomaly detection [36]. These steps standardize the data format, eliminate outliers, and optimize the dataset for reliable downstream processing. Following this, the cleansed data is encrypted using ECC a lightweight yet highly secure cryptographic technique renowned for its minimal computational overhead and strong encryption capabilities. ECC is particularly well-suited for cloud and edge computing environments, making it ideal for financial applications where performance and data confidentiality are critical [37]. This encrypted data then progresses through further stages involving secure storage, decentralized verification via blockchain, and intelligent pattern recognition through AI-based models. The encrypted data is then forwarded to a

blockchain layer that incorporates an immutable ledger and smart contracts as shown in Figure 1.

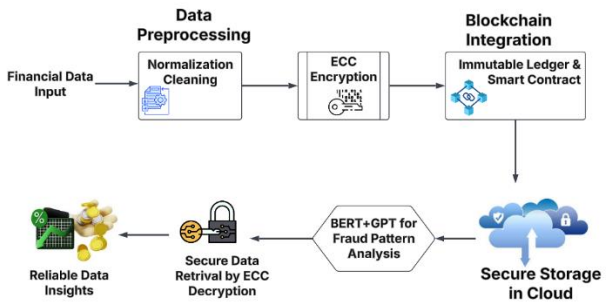

Fig 1: Architecture of cloud security with blockchain integration and ECC

This component not only ensures that all transactions and data alterations are permanently recorded and verifiable, but also enables automated enforcement of data-sharing policies, fraud detection triggers, and access controls via smart contracts. The encrypted financial data is then securely stored in the cloud, where robust protections against unauthorized access and tampering are maintained [38]. For analysis, the data is decrypted through ECC decryption, allowing only authorized entities to retrieve the original information. A hybrid AI model, combining BERT with GPT, is employed to analyze the decrypted data for fraud detection. This model leverages the contextual understanding of BERT and the generative capabilities of GPT to identify complex fraud patterns, including those hidden in unstructured transaction logs or communication records [39]. The output of this AI-driven analysis provides reliable, high-quality financial insights that assist stakeholders in making informed decisions, detecting threats early, and ensuring compliance with financial regulations. Through this comprehensive pipeline from data ingestion and encryption to AI analysis and insight generation the framework establishes a secure, scalable, and intelligent environment for managing sensitive financial data in cloud-based ecosystem. The BERT-LSTM hybrid model enhances personalization by capturing contextual and sequential patterns, as demonstrated by Naresh Kumar Reddy Panga and R Padmavathy (2019) [40]. Embracing their framework, the proposed architecture combines BERT and GPT to detect complex fraud patterns, enabling secure, scalable, and intelligent cloud-based financial fraud detection.

3.1 Data Collection

Kaggle offers a wide range of financial datasets useful for tasks like fraud detection, risk analysis, and market prediction. These include structured and unstructured data such as stock prices, credit card transactions, banking records, and fraud cases. The datasets feature numerical values, categorical data, and textual information (e.g., customer and seller details). Time-based features like timestamps and demographic attributes such as age and income further support the development of context-aware financial models [41].

Dataset Link: https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset

Preprocessing is essential to deal with missing values, outliers and inconsistencies. x_i represent single financial record with d attributes is indicated in Eq. (1),

$$X = \{x_1, x_2, \ldots, x_n\}, x_i \in \mathbb{R}^d \quad (1)$$

Where, represents a dataset X with n samples, where each sample x_i is a d-dimensional real-valued vector.

3.2 Data Preprocessing

Normalization is a critical preprocessing step in data analysis and machine learning, ensuring that numerical features are adjusted to a consistent scale, thereby eliminating distortions caused by differing value ranges across attributes [42]. This process enhances the performance and convergence speed of many algorithms by preventing features with larger magnitudes from disproportionately influencing the model. Two widely used normalization techniques are min-max scaling and z-score standardization. Min-max scaling transforms data to a fixed range, typically [0, 1], by rescaling values based on the minimum and maximum observed in the dataset [43]. In contrast, z-score normalization also known as standard score transformation standardizes data by subtracting the mean and dividing by the standard deviation, resulting in a distribution with zero mean and unit variance. These methods not only improve algorithmic stability and training efficiency but also help maintain the underlying data distribution in a normalized form, which is especially beneficial in distance-based models like KNN or clustering algorithms [44]. Choosing the appropriate normalization technique depends on the data distribution and the specific requirements of the model being applied is mentioned as Eq. (2)

$$.X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (2)$$

Where, X Original data value, X′ Normalized value (min-max normalization), X_{min} Minimum value in the dataset, X_{max} Maximum value in the dataset. This scales data to a [0, 1] range is described in Eq. (3),

$$X' = \frac{X - \mu}{\sigma} \quad (3)$$

Where, X Original data value, X′ Standardized value (z-score normalization), μ Mean of the dataset, σ Standard deviation of the dataset. Z-score normalization is done using above formula. Where μ mean and σ standard deviation. Cleaning involves handling missing values, locating and correcting errors and removing duplicate or redundant data. Techniques such as mean imputation, forward filling and removing missing records all add to data quality. Outlier detection methods such as statistical thresholds assist in fine-tuning dataset and enhancing its credibility for encryption and fraud detection is described as Eq. (4),

$$x_i' = \frac{\sum_{j=1}^{m} x_j}{m} \quad (4)$$

Where, x_i' Mean (average) value for the i-th feature or data point, x_j Individual values in the dataset (from j = 1 to m), m Total number of values (or samples)

3.3 ECC Encryption

Elliptic Curve Cryptography is a powerful encryption

technique widely used to protect sensitive financial information. Unlike traditional methods, ECC relies on the mathematical properties of elliptic curves defined over finite fields. The core operation in ECC is known as point multiplication, where a private key a randomly chosen number is multiplied by a fixed point on the curve, known as the generator point, to produce a corresponding public key. This relationship is one-way and computationally difficult to reverse, ensuring strong security. When conducting secure financial transactions, the sender encrypts the data using the recipient's public key. This encryption process transforms the original message into ciphertext, which is unintelligible to anyone who does not have the appropriate decryption key [45]. Only the recipient, who holds the matching private key, can efficiently decrypt the ciphertext and recover the original information. This mechanism ensures confidentiality and integrity during data exchange, making ECC an ideal choice for securing financial communications in modern digital systems. ECC is recommended over older encryption methods such as RSA because it provides stronger security with shorter key lengths, making it suitable for integrating blockchain and secure cloud storage is declared as Eq. (5) and Eq. (6),

$$y^2 = x^3 + ax + b \bmod p \quad (5)$$

$$C = kP \quad (6)$$

Where a, b defines curves, p prime modulus, k random integer and P public key.

3.4 Blockchain Integration: Immutable Ledger &Smart Contract

Integrating blockchain technology ensures the security and trustworthiness of financial data by recording each transaction in a tamper-resistant digital ledger. Every transaction is securely connected to the one before it through a cryptographic hash, creating a continuous and verifiable chain of blocks. This linking process guarantees that any attempt to modify information in a single block would require recalculating all subsequent blocks, a task that is computationally impractical. Ensemble AI models combining Logistic Regression, Random Forest, and CNN achieve over 90% accuracy in geriatric risk prediction, as illustrated by Sreekar Peddi *et al*. (2019) [46]. Mirroring this strategy, the proposed mechanism implements advanced AI with blockchain's tamper-proof ledger, thus balancing precise fraud detection with secure, verifiable financial transaction storage. As a result, the blockchain structure effectively prevents unauthorized changes and fraud, providing a reliable framework for maintaining data authenticity and transparency in monetary systems. Blockchains decentralized nature eliminates intermediaries guaranteeing financial transactions are transparent and reliable is indicated as Eq. (7),

$$H(B_n) = \text{Hash}(B_{n-1} \| T_n \| N) \quad (7)$$

Where B_n denote current block, T_n transaction block and N nonce. Smart contracts improve blockchain features by automating executing transactions. Self-executing contracts language Solidity automatically validate and execute agreements. They send notifications or freeze transactions when certain circumstances are in fraud detection [47]. This combination of permanent record and automated smart contracts increases financial data security and allows fraud prevention.

3.5 Secure Storage in Cloud

Cloud storage solutions ensure the protection, consistency, and accessibility of financial information by leveraging advanced technological safeguards. The cloud environment employs robust defenses such as data encryption, multi-factor authentication, and granular access controls based on user roles to prevent unauthorized access [48]. By storing encrypted data across multiple servers, cloud platforms provide fault tolerance, minimizing risks of data loss or exposure. Additionally, homomorphic encryption technology allows secure processing of encrypted data directly in the cloud, enabling computations without revealing sensitive details and thereby supporting privacy-preserving fraud detection [49]. Complementing these measures, blockchain integration strengthens security by recording cryptographic transaction summaries on a decentralized, immutable ledger, ensuring transparency, accountability, and data integrity throughout the financial lifecycle. Such security achieves protection of monetary information against cyber-attacks, illegal alteration and data breaches is declared as Eq. (8),

$$Enc(x) \cdot Enc(y) = Enc(x + y) \quad (8)$$

Where, x The first plaintext value (e.g., a numeric data point or financial amount), y The second plaintext value, Enc(x): The encrypted form of x, Enc(y): The encrypted form of y, Enc(x+y): The encryption of the sum of x and y.

3.6 BERT and GPT for Fraud Pattern Analysis

BERT and GPT represent advanced deep learning models that play a crucial role in uncovering fraudulent activities within financial transaction data. BERT, in particular, is highly effective at analyzing textual information found in transaction notes, user logs, and financial reports by leveraging its ability to understand context from both preceding and succeeding words simultaneously [50]. This bidirectional understanding enables BERT to identify subtle irregularities such as sudden shifts in spending patterns, unusual geographic locations of transactions, or transactions linked to fraudulent accounts. By systematically examining the sequence and relationships within transaction data, BERT can highlight suspicious behaviors that traditional methods might overlook, thereby enhancing fraud detection accuracy. It utilizes self-attention mechanisms to concentrate on key transaction features making it suited for fraud detection is defined as Eq. (9),

$$P(Fraud \mid X) = \frac{e^{W^T X}}{1 + e^{W^T X}} \quad (9)$$

Where, P(Fraud|X) The probability that the transaction is fraud, X The details about the transaction (like amount, time, location, etc.), W Numbers the model learns that tell how important each detail in X is for predicting fraud, $W^T X$ A way to combine those importance numbers with the transaction details into one score, A mathematical constant used to calculate the probability. GPT excels at generating predictive insights into fraud risks by analyzing historical transaction data and simulating potential fraudulent schemes [51]. It can recognize evolving patterns of deception and create synthetic

fraud scenarios that can be tested against extensive datasets to evaluate vulnerabilities. When combined with BERT, these models complement each other: BERT classifies transactions with deep contextual awareness, while GPT dynamically forecasts fraud likelihood and explains emerging suspicious behaviors. Together, they form a robust framework for proactive fraud detection and risk management in financial systems. Boyapati and Mekala (2018) [52] describe a scalable fraud detection model based on hybrid cloud ML with XGBoost and Autoencoders. This approach is augmented in the formulated system by applying GPT for dynamic fraud forecasting and BERT for context-aware transaction analysis to detect evolving fraud patterns. This combination fortifies fraud detection models enhancing alerts and lowering false positives in financial security contexts is identified as Eq. (10),

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (10)$$

Where, Q = Query (the input asking for information), K = Key (the data used to find relevant info), V = Value (the actual information to be returned), K^T = Transpose of Key (used to compare with Query), d_k = Size (dimension) of Key vectors, softmax = Function that turns scores into probabilities.

3.7 Secure Data Retrieval by ECC Decryption

encryption plays a critical role in ensuring the accuracy and security of data, which in turn supports system reliability and protection. While the time required to encrypt data generally grows with the size of the dataset, ECC remains more efficient than RSA due to its use of significantly shorter key lengths [53]. However, achieving higher levels of security typically demands greater computational resources, which can lead to increased energy consumption. The strength of encryption is largely based on the complexity of solving the Elliptic Curve Discrete Logarithm Problem, where a 256-bit ECC key provides a security level comparable to that of a much larger 3072-bit RSA key [54]. This balance between security, speed, and resource consumption makes ECC an attractive choice for secure communications. Trade-off guarantees economic data is both safe and accessible is mentioned as Eq. (11),

$$M = C - kP \quad (11)$$

Where, M: The message or original data that you want to recover (plaintext), C: The ciphertext, which is the encrypted message received, k: A secret scalar (usually a private key or a random number used during encryption), P: A point on the elliptic curve (often a public parameter or generator point).

3.8 Reliable Data Insights

Elliptic Curve Cryptography (ECC) decryption ensures that only authorized individuals can access sensitive financial data by securely reversing the encryption process. During decryption, the recipient employs their private key to undo the elliptic curve point multiplication applied in encryption, effectively restoring the original message [55]. This process involves combining the encrypted data with the private key to safely reconstruct the plaintext without exposing it to unauthorized parties. ECC offers strong security comparable to traditional methods like RSA but achieves this with smaller key sizes, making the decryption process more efficient and less demanding computationally. This balance of robust protection and performance makes ECC a preferred choice for safeguarding confidential monetary information. This guard's sensitive financial data from illegal access making it perfect for secure cloud storage and blockchain-enabled financial systems is indicated as Eq. (12),

$$y = \beta_0 + \beta_1 X + \epsilon \quad (12)$$

Where, y = The result or outcome you want to predict, β_0 = The starting value when X is zero, β_1 = How much y changes when X changes, X = The input or factor that affects y, ε = Small random error or things we can't predict.

4. Result and Discussion

This section presents a detailed analysis of the performance of the proposed encryption methodology using the PaySim Financial Fraud Identification Dataset, a synthetic yet realistic representation of mobile financial transactions [56]. The evaluation focuses on critical parameters such as encryption time, energy consumption, transaction latency, and overall security strength to assess the feasibility and efficiency of the solution. The results reveal how encryption time scales non-linearly with increasing data size, reflecting the computational demands associated with securing larger datasets. Additionally, energy consumption rises exponentially with heightened security levels, underscoring the trade-off between achieving stronger protection and managing resource overhead [57]. Transaction latency analysis demonstrates that higher transaction arrival rates significantly increase processing delays, highlighting the scalability challenges in maintaining system responsiveness under heavy loads. The correlation between key size and computation time further emphasizes the balance required between cryptographic strength and performance. Collectively, these findings confirm that the proposed approach achieves a high security level of 99.2%, with competitive encryption times and energy usage, while maintaining low latency, thus offering a practical and effective solution for securing financial data in dynamic transaction environments. The hybrid AI IDS combining autoencoders and attention mechanisms improves detection accuracy by 15–20%, as illustrated by Guman Singh Chauhan and R. Mekala (2019) [58]. Encouraged by this, the proposed methodology evaluated using the PaySim dataset demonstrates efficient scaling of encryption time, energy consumption, and latency, confirming its feasibility for secure mobile financial transactions.

4.1 Dataset Description

PaySim Financial Fraud Identification Dataset is a synthetic representation of mobile cash transactions that is intended to imitate real-world financial operations while including fraudulent behaviors for research purposes. It is based on mobile money service in African country and has been reduced to half of its original size for easier analysis on Kaggle. Dataset contains variety of transaction types including CASH-IN, CASH-OUT, DEBIT, PAYMENT and TRANSFER throughout 30-day simulated period. To address

privacy issues, fraudulent transactions were voided making non-balance columns critical for identifying scams analysis.

4.2 Performance Analysis of Proposed Work

The relationship between data size and encryption time in seconds. As depicted, encryption time increases as data size grows, but the trend is nonlinear [59]. For smaller datasets, the encryption time rises steeply, indicating that even modest increases in data size can cause significant computational overhead initially. However, as the data size continues to expand beyond this point, the curve gradually flattens, showing a slower rate of increase in encryption time [60]. This suggests that while larger datasets require more time to encrypt, the system becomes more efficient in handling bulk data over time. The visualization effectively captures this dynamic, emphasizing the escalating computational effort needed to secure larger amounts of information and the inherent trade-off between achieving robust security and maintaining operational efficiency is shown in Figure (2),

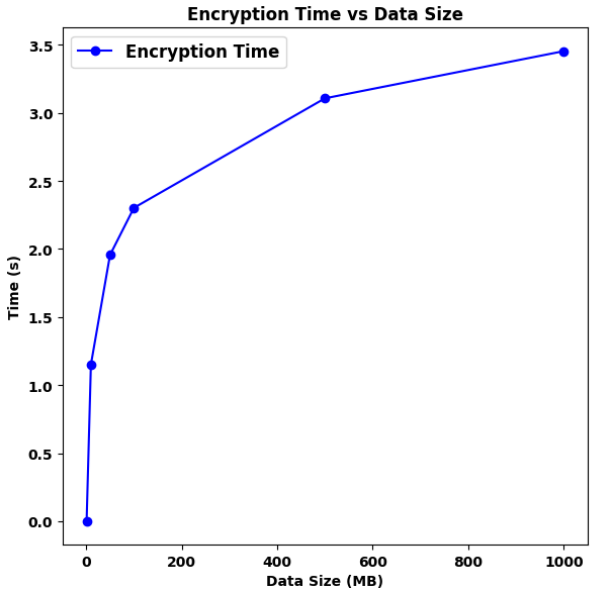

Fig 2: Encryption time vs Data size

The relationship between energy consumption and security level is clearly demonstrated in Figure 3, which depicts an upward, exponential-like curve indicating that higher security levels require significantly more energy. As shown in the figure, even small increases in security strength lead to disproportionately large rises in energy usage, highlighting the heavy computational demands of stronger encryption methods [61]. This exponential growth underscores a fundamental trade-off in cryptographic design: while enhancing security is essential to protect sensitive financial data from increasingly sophisticated threats, it inevitably results in greater energy expenditure. The visualization in Figure 4 effectively captures this balance, emphasizing the challenge of maintaining robust protection without incurring unsustainable resource costs. This trade-off is particularly important for systems operating in energy-constrained environments such as mobile platforms or large-scale cloud services, where excessive energy consumption can impact operational costs and environmental sustainability [62]. Therefore, Figure 4 not only illustrates the correlation between energy use and security but also stresses the need for optimizing cryptographic algorithms to ensure high security with efficient energy management. Charles Ubagaram and Bharathidasan (2019) [63] developed a scalable AI-driven cloud security framework using Fourier Transform and GRU for accurate threat detection. The proposed workflow emphasizes optimizing cryptographic algorithms to achieve robust security with efficient energy use, addressing the critical trade-off between protection level and computational cost.

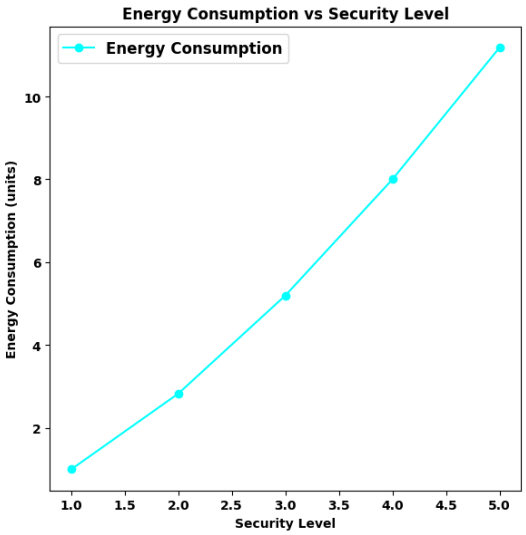

Fig 3: Energy Consumption versus Security level

A box plot illustrating the distribution of transaction latency at varying transaction arrival rates, clearly showing that as arrival rates increase, latency rises dramatically. At lower arrival rates, such as between 100 and 1000 transactions, latency remains relatively stable with minimal variation, indicating the system can efficiently process moderate workloads [64]. However, at higher arrival rates ranging from 2000 to 4000 transactions, latency not only increases significantly but also becomes more variable, as reflected by the wider spread in the box plot. This pattern suggests that heavier transaction loads lead to network congestion and resource contention, resulting in longer and less predictable processing times [65]. The visualization effectively highlights the scalability challenge of maintaining low-latency performance when the system is subjected to high transaction volumes, emphasizing the need for optimized resource management and infrastructure capable of handling peak loads without compromising responsiveness or reliability is shown in Figure (4),

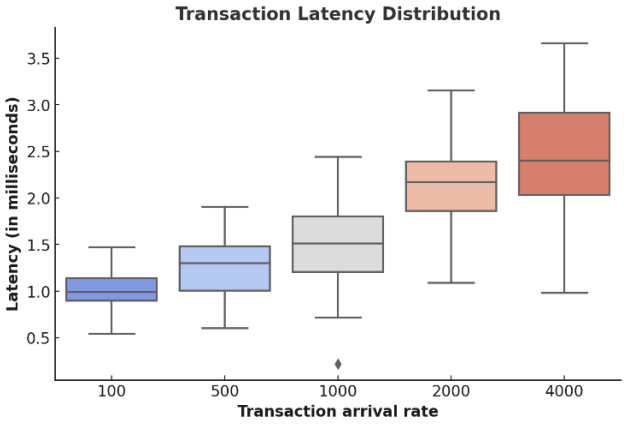

Fig 4: Transaction Latency Distributuion

The relationship between cryptographic key size and computation time in milliseconds, clearly showing that as the key size increases, computation time also rises due to the additional processing required for larger keys. The graph's clean presentation, with the legend positioned inside the frame to avoid overlapping data points and the grid removed for clarity, allows for easy interpretation of this trend [66]. Importantly, the security strength annotation of 99.2% displayed at the bottom right highlights the high level of protection achieved with these key sizes. This visualization effectively captures the crucial balance between computation cost and security level, emphasizing that while larger keys enhance security by making encryption more resistant to attacks, they also demand more computational resources and time. A cloud-based fraud detection approach combining GNNs and explainable AI was proposed by Nagendra Kumar Musham and Aiswarya RS (2019) [67] to enable intelligent and scalable decision-making. Guided by this methodology, the formulated model achieves encryption strength while effectively managing the trade-off between key size and processing time in financial security systems. Therefore, Figure 5 underscores the ongoing challenge in cryptographic design of optimizing key sizes to maintain robust security without sacrificing system performance and efficiency.

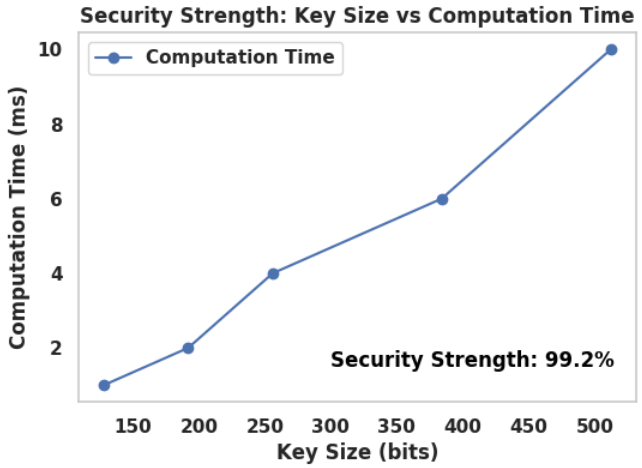

Fig 5: Security Strength

The suggested approach achieves an impressive security strength of 99.2%, while maintaining efficient performance metrics critical for financial systems [68]. As depicted the encryption time remains low at 3.5 seconds despite the complexity of the cryptographic operations, demonstrating the system's capability to securely process data without causing significant delays [69]. Additionally, the energy consumption is measured at 10.5 units, reflecting a reasonable trade-off between enhanced security and resource expenditure, as shown in Figure 5 where energy usage rises with increased security levels. Crucially, the approach maintains a minimal transaction latency of 2.5 milliseconds, ensuring that transaction processing remains swift and responsive, which is essential for real-time financial operations [70]. This combination of strong security, moderate energy consumption, and low latency highlights the balanced design of the proposed method, effectively addressing the challenge of securing sensitive financial data while preserving system efficiency. The visualizations clearly illustrate these relationships, emphasizing how the approach optimizes both performance and protection, making it well-suited for deployment in environments where security and speed are paramount. Kushala and Rathna (2018) [71] integration of CNN-LSTM with homomorphic encryption reduces leakage and improves accuracy in healthcare data clouds. Extending this principle, the proposed system secures financial cloud data with 99.2% strength, low latency, and energy-efficient operation, leveraging encryption and AI analytics.

Table 1: Performance metrics value

Metrics	Security strength (%)	Encryption Time (s)	Energy consumption (units)	Transaction latency (ms)
Proposed	99.2	3.5	10.5	2.5

5. Conclusion and Future Enhancement

Security of financial information in cloud systems is a priority due to increasing cases of cyber-attacks. This proposed efficient security model combining Blockchain and ECC encryption for ensuring confidentiality, integrity and availability of financial information. The decentralized and immutable ledger of Blockchain preserves unauthorized modification of data. ECC provides secure encryption with low computational complexity. Blending BERT and GPT adds tremendous fraud detection by analyzing transaction patterns and predicting potential risks. Anomaly detection through AI raises threat discovery and prevents fraudulent activity before destabilization of financial systems. Experimental testing demonstrates 99.2 percent robust security with little processing delay and low battery consumption. Blockchain enabled smart contracts automatically validate and audit transactions reduc human mistake and unlawful manipulation. Homomorphic encryption and cloud storage allow for privacy-preserving financial computations while maintaining security. Future research focus on improving AI-based security models such as federal learning for fraud detection and Blockchain technology to boost efficiency and scalability. Multi-factor authentication and biometrics technologies enhance data security. Transaction tracing done by Edge computing improves system responsiveness. This safeguards cloud financial transactions resulting in dynamic and comprehensive cybersecurity strategy that can successfully defend against developing cyber assaults.

6. References

1. Dong W, Yang Q. Data-driven solution for optimal pumping units scheduling of smart water conservancy. IEEE Internet Things J. 2019;7(3):1919-26.
2. Cockcroft S, Russell M. Big data opportunities for accounting and finance practice and research. Aust Account Rev. 2018;28(3):323-33.
3. Zimba A, Chishimba M. On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. Eur J Secur Res. 2019;4(1):3-31.
4. Hassani H, Huang X, Silva E. Digitalisation and big data mining in banking. Big Data Cogn Comput. 2018;2(3):18.
5. Košťál K, Helebrandt P, Belluš M, Ries M, Kotuliak I. Management and monitoring of IoT devices using blockchain. Sensors. 2019;19(4):856.
6. Devarajan MV, Pushpakumar R. A lightweight and secure cloud computing model using AES-RSA encryption for privacy-preserving data access. Int J Eng

Sci Adv Technol. 2019;19(12).
7. Le HV, Ngo QD, Le VH. Iot botnet detection using system call graphs and one-class CNN classification. Int J Innov Technol Explor Eng. 2019;8(10):937-42.
8. Hefron R, Borghetti B, Schubert Kabban C, Christensen J, Estepp J. Cross-participant EEG-based assessment of cognitive workload using multi-path convolutional recurrent neural networks. Sensors. 2018;18(5):1339.
9. Kim J, Kim HJ, Kim H. Fraud detection for job placement using hierarchical clusters-based deep neural networks. Appl Intell. 2019;49(8):2842-61.
10. Slowik A, Kwasnicka H. Nature inspired methods and their industry applications—Swarm intelligence algorithms. IEEE Trans Ind Inform. 2017;14(3):1004-15.
11. Nutalapati P. Advanced Data Encryption Techniques for Secure Cloud Storage in Fintech Applications. J Sci Eng Res. 2018;5(12):396-405.
12. Kumar S, Tejani GG, Mirjalili S. Modified symbiotic organisms search for structural optimization. Eng Comput. 2019;35(4):1269-96.
13. Peng Z, Yao Y, Xiao B, Guo S, Yang Y. When urban safety index inference meets location-based data. IEEE Trans Mob Comput. 2018;18(11):2701-13.
14. Bhattacharya P, Tanwar S, Bodkhe U, Tyagi S, Kumar N. Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE Trans Netw Sci Eng. 2019;8(2):1242-55.
15. Gattupalli K, Purandhar N. Optimizing customer retention in CRM systems using AI-powered deep learning models. Int J Multidiscip Curr Res. 2019;7(Sept/Oct).
16. Das A, Baki S, El Aassal A, Verma R, Dunbar A. SoK: a comprehensive reexamination of phishing research from the security perspective. IEEE Commun Surv Tutor. 2019;22(1):671-708.
17. Yang K, Wang K, Bergasa LM, Romera E, Hu W, Sun D, *et al*. Unifying terrain awareness for the visually impaired through real-time semantic segmentation. Sensors. 2018;18(5):1506.
18. Mazurek G, Małagocka K. Perception of privacy and data protection in the context of the development of artificial intelligence. J Manage Anal. 2019;6(4):344-64.
19. Pulgar FJ, Charte F, Rivera AJ, Del Jesus MJ. AEkNN: An AutoEncoder kNN—Based Classifier With Built-in Dimensionality Reduction. Int J Comput Intell Syst. 2018;12(1):436-52.
20. Del Ser J, Osaba E, Sanchez-Medina JJ, Fister I. Bioinspired computational intelligence and transportation systems: a long road ahead. IEEE Trans Intell Transp Syst. 2019;21(2):466-95.
21. Leenes R, Palmerini E, Koops BJ, Bertolini A, Salvini P, Lucivero F. Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues. Law Innov Technol. 2017;9(1):1-44.
22. Grandhi SH, Kumar VR. IoT-driven smart traffic management system with edge AI-based adaptive control and real-time signal processing. Int J Mod Electron Commun Eng. 2019;7(3).
23. Rawat DB, Doku R, Garuba M. Cybersecurity in big data era: From securing big data to data-driven security. IEEE Trans Serv Comput. 2019;14(6):2055-72.
24. Abuarqoub A. D-FAP: Dual-factor authentication protocol for mobile cloud connected devices. J Sens Actuator Netw. 2019;9(1):1.
25. Herold DM, Lee KH. The influence of the sustainability logic on carbon disclosure in the global logistics industry: The case of DHL, FDX and UPS. Sustainability. 2017;9(4):601.
26. Anisetti M, Ardagna CA, Damiani E, Gaudenzi F. A semi-automatic and trustworthy scheme for continuous cloud service certification. IEEE Trans Serv Comput. 2017;13(1):30-43.
27. Rahi SB, Bisui S, Misra SC. Identifying the moderating effect of trust on the adoption of cloud-based services. Int J Commun Syst. 2017;30(11):e3253.
28. Jain Y, Tiwari N, Dubey S, Jain S. A comparative analysis of various credit card fraud detection techniques. Int J Recent Technol Eng. 2019;7(5):402-7.
29. Schmitz J, Leoni G. Accounting and auditing at the time of blockchain technology: a research agenda. Aust Account Rev. 2019;29(2):331-42.
30. Malikireddy SKR, Algubelli BR. Multidimensional privacy preservation in distributed computing and big data systems: Hybrid frameworks and emerging paradigms. Int J Sci Res Sci Technol. 2017;3(4):2395-602.
31. Gopireddy SR. Privacy-Aware Federated Data Sharing Models for Healthcare Cloud Systems. J Sci Eng Res. 2019;6(12):324-7.
32. Howard J. Artificial intelligence: Implications for the future of work. Am J Ind Med. 2019;62(11):917-26.
33. Khurana R, Kaul D. Dynamic cybersecurity strategies for ai-enhanced ecommerce: A federated learning approach to data privacy. Appl Res Artif Intell Cloud Comput. 2019;2(1):32-43.
34. Deevi DP, Padmavathy R. A hybrid random forest and GRU-based model for heart disease prediction using private cloud-hosted health data. Int J Appl Sci Eng Manage. 2019;13(2).
35. Nutalapati P. Advanced Data Encryption Techniques for Secure Cloud Storage in Fintech Applications. J Sci Eng Res. 2018;5(12):396-405.
36. Jindal A, Aujla GS, Kumar N, Chaudhary R, Obaidat MS, You I. SeDaTiVe: SDN-enabled deep learning architecture for network traffic control in vehicular cyber-physical systems. IEEE Netw. 2018;32(6):66-73.
37. Liu S, Roy D, Hennequin S. Blockchains and internet of things for the pooling of warehouse resources. South Asian J Soc Stud Econ. 2019;15(4):1-16.
38. Le LV, Lin BS, Do S. Applying big data, machine learning, and SDN/NFV for 5G early-stage traffic classification and network QoS control. Trans Netw Commun. 2018;6(2):36.
39. Tang F, Fadlullah ZM, Mao B, Kato N. An intelligent traffic load prediction-based adaptive channel assignment algorithm in SDN-IoT: A deep learning approach. IEEE Internet Things J. 2018;5(6):5141-54.
40. Panga NKR, Padmavathy R. Leveraging advanced personalization techniques to optimize customer experience and drive engagement on e-commerce platforms. Int J Eng Technol Res Manage. 2019;3(8).
41. Guo X, Lin H, Li Z, Peng M. Deep-reinforcement-learning-based QoS-aware secure routing for SDN-IoT. IEEE Internet Things J. 2019;7(7):6242-51.
42. Alawe I, Ksentini A, Hadjadj-Aoul Y, Bertin P. Improving traffic forecasting for 5G core network scalability: A machine learning approach. IEEE Netw.

2018;32(6):42-49.
43. Singh A, Aujla GS, Garg S, Kaddoum G, Singh G. Deep-learning-based SDN model for Internet of Things: An incremental tensor train approach. IEEE Internet Things J. 2019;7(7):6302-11.
44. Pei J, Hong P, Pan M, Liu J, Zhou J. Optimal VNF placement via deep reinforcement learning in SDN/NFV-enabled networks. IEEE J Sel Areas Commun. 2019;38(2):263-78.
45. Yao Y, Chang X, Mišić J, Mišić VB, Li L. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet Things J. 2019;6(2):3775-84.
46. Peddi S, Narla S, Valivarthi DT. Harnessing artificial intelligence and machine learning algorithms for chronic disease management, fall prevention, and predictive healthcare applications in geriatric care. Int J Eng Res Sci Technol. 2019;15(1).
47. Sharma SK, Wang X. Toward massive machine type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions. IEEE Commun Surv Tutor. 2019;22(1):426-71.
48. Bega D, Gramaglia M, Banchs A, Sciancalepore V, Costa-Perez X. A machine learning approach to 5G infrastructure market optimization. IEEE Trans Mob Comput. 2019;19(3):498-512.
49. Reyes ARL, Festijo ED, Medina RP. Securing one time password (OTP) for multi-factor out-of-band authentication through a 128-bit blowfish algorithm. Int J Commun Netw Inf Secur. 2018;10(1):242-7.
50. Tang F, Kawamoto Y, Kato N, Liu J. Future intelligent and secure vehicular network toward 6G: Machine-learning approaches. Proc IEEE. 2019;108(2):292-307.
51. Garg S, Kaur K, Kumar N, Rodrigues JJ. Hybrid deep-learning-based anomaly detection scheme for suspicious flow detection in SDN: A social multimedia perspective. IEEE Trans Multimedia. 2019;21(3):566-78.
52. Subramanyam B, Mekala R. Leveraging cloud-based machine learning techniques for fraud detection in e-commerce financial transactions. Int J Mod Electron Commun Eng. 2018;6(3).
53. Tang F, Mao B, Fadlullah ZM, Kato N. On a novel deep-learning-based intelligent partially overlapping channel assignment in SDN-IoT. IEEE Commun Mag. 2018;56(9):80-86.
54. Martin A, Egaña J, Flórez J, Montalban J, Olaizola IG, Quartulli M, *et al*. Network resource allocation system for QoE-aware delivery of media services in 5G networks. IEEE Trans Broadcast. 2018;64(2):561-74.
55. Zhuang W, Ye Q, Lyu F, Cheng N, Ren J. SDN/NFV-empowered future IoV with enhanced communication, computing, and caching. Proc IEEE. 2019;108(2):274-91.
56. Dey SK, Rahman MM. Effects of machine learning approach in flow-based anomaly detection on software-defined networking. Symmetry. 2019;12(1):7.
57. Mohsin AH, Zaidan AA, Zaidan BB, Albahri OS, Albahri AS, Alsalem MA, *et al*. Based medical systems for patient's authentication: Towards a new verification secure framework using CIA standard. J Med Syst. 2019;43(7):192.
58. Chauhan GS, Mekala R. AI-driven intrusion detection systems: Enhancing cybersecurity with machine learning algorithms. Int J Multidiscip Curr Res. 2019;7(Mar/Apr).
59. Litchfield A, Herbert J. ReSOLV: applying cryptocurrency blockchain methods to enable global cross-platform software license validation. Cryptography. 2018;2(2):10.
60. Zhuang Z, Wang J, Qi Q, Sun H, Liao J. Toward greater intelligence in route planning: A graph-aware deep learning approach. IEEE Syst J. 2019;14(2):1658-69.
61. Restuccia F, D'oro S, Melodia T. Securing the internet of things in the age of machine learning and software-defined networking. IEEE Internet Things J. 2018;5(6):4829-42.
62. Chemouil P, Hui P, Kellerer W, Li Y, Stadler R, Tao D, *et al*. Special issue on artificial intelligence and machine learning for networking and communications. IEEE J Sel Areas Commun. 2019;37(6):1185-91.
63. Ubagaram C, Bharathidasan. AI-driven cloud security framework for cyber threat detection and classification in banking systems. J Curr Sci. 2019;7(3).
64. Paul U, Liu J, Troia S, Falowo O, Maier G. Traffic-profile and machine learning based regional data center design and operation for 5G network. J Commun Netw. 2019;21(6):569-83.
65. Ayoubi S, Limam N, Salahuddin MA, Shahriar N, Boutaba R, Estrada-Solano F, *et al*. Machine learning for cognitive network management. IEEE Commun Mag. 2018;56(1):158-65.
66. Deshpande V, George L, Badis H. Pulsec: Secure element based framework for sensors anomaly detection in industry 4.0. IFAC-PapersOnLine. 2019;52(13):1204-9.
67. Musham NK, Aiswarya RS. Leveraging artificial intelligence for fraud detection and risk management in cloud-based e-commerce platforms. Int J Eng Technol Res Manage. 2019;3(10).
68. Xue L, Liu D, Ni J, Lin X, Shen XS. Balancing privacy and accountability for industrial mortgage management. IEEE Trans Ind Inform. 2019;16(6):4260-9.
69. Cha SC, Hsu TY, Xiang Y, Yeh KH. Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. IEEE Internet Things J. 2018;6(2):2159-87.
70. Samkari H, Gutub A. Protecting medical records against cybercrimes within Hajj period by 3-layer security. Recent Trends Inf Technol Appl. 2019;2(3):1-21.
71. Kushala K, Rathna S. Enhancing privacy preservation in cloud-based healthcare data processing using CNN-LSTM for secure and efficient processing. Int J Mech Eng Comput Sci. 2018;6(2):119-27.