Enhancing E-Commerce Transaction Security with Big Data Analytics in Cloud Computing

[1]Rajani Priya Nippatla
Kellton Technologies Inc, Texas, USA
rnippatla@gmail.com

[2]R. Hemnath
Nandha Arts and Science College, Erode, India.
hemnathrmca@gmail.com

Abstract

With the rapid increase in the number of e-commerce transactions, security measures must be considerably stronger to protect sensitive user and financial information. This research develops a new framework to secure e-commerce transactions using a combination of cloud computing and big data analytics. The framework which integrates blockchain-based ledger verifications, ML-based pattern recognition for fraud detection and real-time detection of anomalies related to customer data, addresses the current demands of cyber threats. This type of distributed cloud infrastructure and predictive analytics brings low latency and high assurance for secure transactions. The findings illustrate significant advancements in both threat detection rates and computational efficiency over conventional security models. Thus, they have made an essential contribution to safeguarding the integrity of digital transactions which proves to be fundamental to countering pressing vulnerabilities in today's e-commerce environments. The framework employs access control methodologies and advanced encryption schemes enhancing the level of privacy assurance for individual data. Experimental validation demonstrates that our framework can identify fraudulent transactions with high confidence and at scale while efficiently executing system requirements.

Keywords: *E-commerce security, Big Data Analytics, Cloud Computing, Fraud Detection, Blockchain*.

1| Introduction

A buyer, a seller, a payment gateway, and a bank are some of the stakeholders associated with e-commerce transactions [1]. The security and integrity of transaction data are often instrumental in the functioning of digital marketplaces and in maintaining consumer trust [2]. In the landscape of e-commerce, the need for security is becoming more complex with advanced cyber threats [3]. Conventional security solutions such as static encryption methods and rule-based fraud detection systems have proven to be inadequate [4]. Analysis of large volume data-driven through ML and AI has significant potential to enhance transaction confidence, supporting risk detection through the analysis of current transactional behaviour [5]. These capabilities can lead to monitoring of transactions while in progress that will identify anomalies as well as facilitate automated protocols for mitigating fraudulent outcomes [6]. Cloud computing frameworks provide secure data storage mechanisms and a highly scalable technological environment for data usage ensuring ongoing monitoring and fast response to risks and vulnerabilities [7].

Several reasons contribute to growing security issues surrounding e-commerce transactions of legacy fraud detection systems that use predefined rules and cannot monitor in real-time so are no longer useful against evolving fraud techniques [8]. Cybercriminals use payment system vulnerabilities for large-scale data breaches or significant financial loss [9]. Insider threats encompass employees or third-party vendors who have access to transaction data and can cause serious security risks including data leaks or financial fraud [10]. The growth of online shopping has increased the incidence of fraudulent transactions including phishing, card-not-present fraud, and account takeovers [11]. Many e-commerce websites still rely on outdated authentication methods which in turn puts them at risk for identity theft and credential stuffing [12]. As transaction volume increases, traditional security infrastructures also struggle to scale up and they cause performance problems and greater risk [13].

Despite advancements in digital security, the current approaches to detect and prevent fraud have limitations [14]. Traditional rule-based fraud detection methods are ineffective against emerging fraud attack patterns because they rely on static manually specified rules [15]. Many security models create excessive false positives causing

unnecessary transaction denials and resulting in a poor user experience [16]. Legacy security systems have also introduced scalability issues due to their inability to process increasing amounts of transaction data in real-time [17]. Centralized security systems are also vulnerable to attacks because of having single points of failure [18]. When fraudulent behaviours go unnoticed, organizations experience a significant loss in dollars and also reputational damage [19].

The use of heuristics and rigid patterns has left many systems unable to adapt to dynamically changing threat vectors [20]. New fraud strategies such as synthetic identity fraud are difficult to detect using traditional techniques [21]. Behavioural biometrics offer promising enhancements to fraud detection yet remain underutilized in many online systems [22]. False negatives in detection systems allow sophisticated fraud schemes to proceed undetected [23]. Consumers often abandon purchases when faced with complex or redundant security checks, decreasing sales for e-commerce platforms [24]. Transaction speed is a critical factor in e-commerce, and security systems that introduce latency can hinder competitiveness [25]. Many e-commerce businesses lack the resources to continuously upgrade their security infrastructure [26].

Integrating AI and real-time analytics can significantly reduce false positives and improve fraud identification [27]. Data lakes and advanced cloud analytics support the scalability and efficiency required by modern fraud prevention systems [28]. Machine learning enables pattern recognition across diverse datasets to uncover fraudulent behaviour [29]. Adversarial attacks can exploit weaknesses in AI-based fraud detection models, leading to bypasses [30]. Secure APIs and tokenization are increasingly necessary to protect sensitive data during transactions [31]. Device fingerprinting and geolocation data add contextual intelligence to authentication mechanisms [32]. Lack of regulatory compliance can lead to legal penalties and loss of consumer confidence [33]. Organizations must conduct regular audits and penetration tests to uncover hidden vulnerabilities [34]. Consumer education and awareness campaigns are critical in reducing the success rate of phishing and social engineering attacks [35]. The integration of blockchain offers promise in creating tamper-proof transaction records [36]. Real-time monitoring combined with historical data profiling increases detection accuracy [37]. Multi-factor authentication and biometric systems represent a forward leap in transaction security [38].

1.1 Problem Statement

The rapid growth of e-commerce has led to new challenges regarding the safety of online transactions [39]. Because traditional fraud detection systems built on static security measures and present rules cannot keep in step with evolving cyber threats, transactions are susceptible to identity theft and phishing [40]. The cybersecurity issue is compounded by new complexities in the methods of threat actors, including identity theft, phishing, and card-not-present fraud [41]. Cyber actors also rely on centralized data storage systems which provide them with single points of failure, making them excellent targets for cyberattacks [42]. Additionally, the increasing volume of transactions places strain on legacy security infrastructures, reducing their effectiveness and responsiveness [43]. The lack of real-time monitoring and adaptive detection mechanisms leaves many fraudulent activities undetected until significant damage has occurred [44]. Emerging fraud techniques are becoming more sophisticated, requiring dynamic and intelligent detection frameworks that traditional methods cannot provide [45]. Therefore, there is an urgent need for innovative security solutions that leverage advanced technologies to protect e-commerce ecosystems against evolving threats [46]. Robust integration of artificial intelligence, real-time analytics, and behavioural analysis is essential to improve fraud detection accuracy and minimize financial risks [47]. Without such advancements, businesses remain vulnerable to growing cybercrime, regulatory penalties, and loss of customer trust [48]. Strengthening authentication mechanisms, decentralizing data storage, and using predictive models can significantly enhance transactional security [49]. Ultimately, safeguarding e-commerce transactions depends on building resilient, scalable, and adaptive security frameworks that evolve alongside modern threats [50].

1.2 Objectives of the Proposed Work

- Create a cloud-based security framework utilizing AI and big data analytics to help detect fraud and secure e-commerce transactions.
- Employ the dataset of e-commerce transactions including purchase information, payment information, timestamps and cybersecurity logs to develop and assess the fraud detection model.
- Utilize a hybrid CNN-GRU model for anomaly detection so that both spatial and temporal transaction patterns can be identified to detect fraudulent activities.
- Incorporate homomorphic encryption and blockchain logging methods for data integrity, unauthorized access protection and as a tamper-proof security method for e-commerce transactions.

2| Related Works

The Secure Attribute-Based Access Control (ABAC) architecture, when combined with blockchain encryption and hash-tag authentication, has shown significant promise in enhancing privacy and access control within cloud computing systems [51]. Deep learning architectures such as bi-directional LSTM integrated with fuzzy logic and regressive dropout have proven effective in detecting patterns for medical condition prediction [52]. In a similar vein, CNN-GRU models have been employed for detecting anomalies in fraudulent transactions [53]. Within the e-commerce ecosystem, the integration of blockchain, IoT, and big data analytics has emerged as a disruptive combination, offering deep insights into customer reviews and financial behaviours through advanced AI algorithms [54]. Hybrid AI models have demonstrated strong performance in detecting text-based e-commerce fraud [55]. Additionally, privacy-preserving data analytics methods leveraging finite element modelling and coding dimensions have advanced secure computation practices [56].

Security and confidentiality in cloud computing for banking and financial sectors have been addressed using blockchain-based encryption techniques to maintain data integrity [57]. Cryptographic methods remain critical for ensuring the safety of financial transactions in cloud-based environments [58]. Optimization strategies in predictive analytics have proven essential in improving the effectiveness of fraud detection models [59]. Further studies have explored cloud adoption in software testing through fuzzy multicriteria decision-making supported by empirical evaluation [60]. In customer relationship management (CRM), AI plays a significant role in ensuring secure data handling and providing consistent multi-channel user experiences in digital platforms [61].

AI also contributes to material design, as shown in research on optimizing 3D printing materials for medical applications using computational modelling and directed energy deposition [62]. Hybrid optimization frameworks have significantly improved clustering and efficiency in software quality assurance [63]. Multi-modal AI interfaces and predictive analytics have reshaped CRM systems, reinforcing the importance of AI in real-time e-commerce security [64]. Deep learning techniques have become instrumental in identifying digital threats, extending their relevance to detecting suspicious online transaction behaviour [65]. The fusion of AI and cloud computing enhances scalability in processing large datasets, particularly beneficial for security in modern applications [66].

Applications of cloud computing have also accelerated big data collection and analysis in domains like geoscience, demonstrating adaptable security solutions [67]. Real-time analytics and anomaly detection from such studies can be leveraged to strengthen e-commerce fraud prevention [68]. Security checker frameworks integrated with cloud infrastructure have enabled effective fault detection in smart systems [69]. Cloud platforms continue to be vital in the secure management of sensitive information, paralleling the needs of e-commerce transaction protection [70]. Pattern recognition and predictive modelling using AI techniques contribute directly to the timely detection of fraudulent activity [71]. Additionally, fuzzy logic and hybrid AI systems facilitate the fast identification of complex threats in financial environments [72].

Blockchain-based frameworks for healthcare data security also offer scalable and tamper-resistant mechanisms applicable to online commerce [73]. Federated learning combined with differential privacy has emerged as a viable approach for training secure AI models across distributed systems [74]. The integration of genetic algorithms and swarm intelligence into fraud detection has improved both efficiency and adaptability [75]. Secure multiparty computation enables privacy-preserving analytics in cloud ecosystems handling sensitive financial data [76]. Real-time machine learning within big data systems supports early fraud detection and proactive risk mitigation strategies [77]. Ensemble models further increase the accuracy and reliability of fraud detection in rapidly changing environments [78]. Explainable AI (XAI) enhances trust in AI-based decisions by providing transparency in fraud detection systems [79]. Ultimately, cybersecurity frameworks enhanced with AI and deep learning are critical in protecting digital commerce platforms from increasingly advanced cyber threats [80].

3| Proposed E-Commerce Transaction Security with Big Data Analytics in Cloud Computing

DL and Big data analytics are employed within the proposed methodology to enhance the security of online transactions. To find prominent patterns, data from transactions is pre-processed normalized and transformed first and then features are selected using PCA. Subsequently for anomaly detection, a hybrid CNN-GRU model that can capture both temporal and longitudinal transaction features is employed. Finally, secure cloud-based fraud detection with notifications and tamper-evident security is assured through homomorphic encryption and blockchain audit logs.

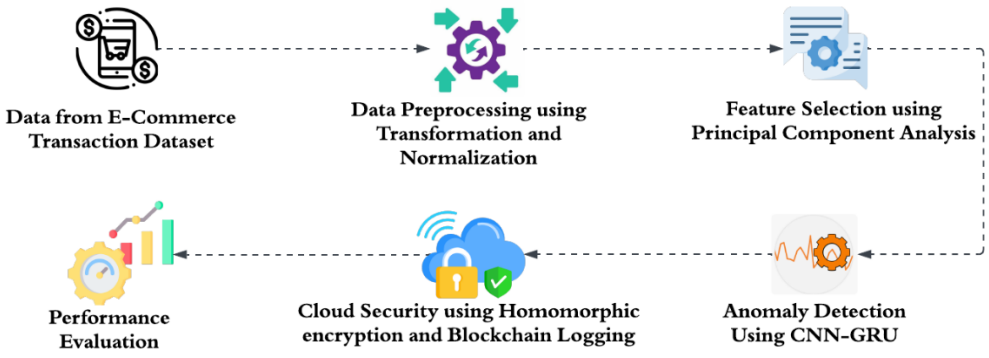

Figure 1: *Proposed Architecture of E-Commerce Transaction Security*

3.1 Data Collection

E-Commerce Transactions Dataset

E-commerce transaction data is comprised of all the elements of purchase information, payment-related information, moments of purchase and customer behavior trends. By comparison, cybersecurity logs capture potential threats to security such as a phishing attempt, fraud attempt or unauthorized access. Such datasets are typically collected from various security monitoring systems and cloud or internet services. A cloud-based architecture for big data then maintains the information for future processing and analysis.

3.2 Data Preprocessing

Data is cleaned, transformed and normalized to improve model efficiency.

3.2.1 Normalization using Min-Max Scaling

Min-max scaling is a normalizing approach that transforms data into a defined range [0,1], enhancing model performance. It is calculated using the formula,

$$X' = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{1}$$

Were, X' is the scaled value, X is the original value and $X_{\max}$, $X_{\min}$ are the minimum and maximum values of the features. This ensures that all features contribute equally to the model.

3.2.2 Transformation

To deal with skewed data like transaction amounts, log transformation is utilized to lessen the impact of extreme values. The equation,

$$X' = \log(1 + X) \tag{2}$$

Smooth large variations by compressing high values while preserving data structure. This helps improve model stability and accuracy by reducing the effect of outliers.

3.3 Feature Selection Using PCA

A dimensionality reduction method called Principal Component Analysis minimizes data loss while identifying the most significant features. It converts the dataset into a fresh set of variance-ranked, uncorrelated principal components. The following provides the transformation,

$$Z = XW \tag{3}$$

Were, X is the data matrix and W contains eigenvectors of the covariance matrix. By keeping only, the top k components, PCA reduces computational complexity while preserving key patterns. The top k components ensuring,

$$\sum_{i=1}^{k} \lambda_i \approx 95\% \text{ variance} \quad (4)$$

Were λ_i are the eigenvalues.

3.4 Anomaly Detection Using CNN-GRU

The CNN-GRU hybrid model detects fraudulent transactions by combining GRUs for sequence learning and CNNs for feature extraction. Convolutional filters are used by CNN to identify spatial dependencies in transaction data,

$$F_i = \sigma\left(W_f * X + b_f\right) \quad (5)$$

Were, W_f are filter weights and X is input data. GRU then processes sequential patterns in transaction behavior using,

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tilde{h}_t \quad (6)$$

This enables the model to examine both transaction attributes and time-dependent patterns to identify anomalies.

3.5 Cloud Security with Homomorphic Encryption and Blockchain Logging

3.5.1 Homomorphic Encryption for Secure Computation

By preventing the need to decrypt the transaction data, homomorphic encryption protects privacy while enabling safe data processing in the cloud. For a transaction M, the Paillier Homomorphic Encryption Scheme uses,

$$C = g^M \text{mod} N^2 \quad (6)$$

Were, M is the transaction data, N is the large prime number ensuring security and g is a generator used in encryption. This allows computations to be performed directly on encrypted data, eliminating risks of data exposure.

3.5.2 Blockchain Logging for Tamper-Proof Security

Every transaction is documented in a blockchain ledger to guarantee transaction integrity and guard against unwanted changes. The SHA-256 hashing algorithm creates a distinct cryptographic hash for every transaction,

$$H(T) = \text{SHA} - 256(T) \quad (7)$$

Were, T represents the transaction data and $H(T)$ is the immutable hash ensuring data integrity. Since blockchain records are tamper-proof and decentralized, any attempt to modify a past transaction will be detected making it highly secure for e-commerce fraud prevention.

4| Results and Discussion

4.1 Performance Metrics of Proposed Model

The first figure 2 displays some important metrics for evaluation, namely, F1-score which scored 99.41 percent, accuracy at 99.42 percent, precision at 99.58 percent and recall at 99.24 percent. These high values indicate that the proposed AI-based security model achieves a good balance between the detection of fraudulent transactions and precision and recall while minimizing false positives and false negatives. The second Figure 3 shows the false alarm rates of the model. At 0.405 percent, the FPR indicates that relatively few valid transactions are reported as fraudulent incidents. The FNR indicates the proportion of fraudulent transactions that go unreported at a rate of 0.762 percent. The low FPR and FNR above show that the proposed method is robust and can reliably distinguish between both legitimate and fraudulent transactions.

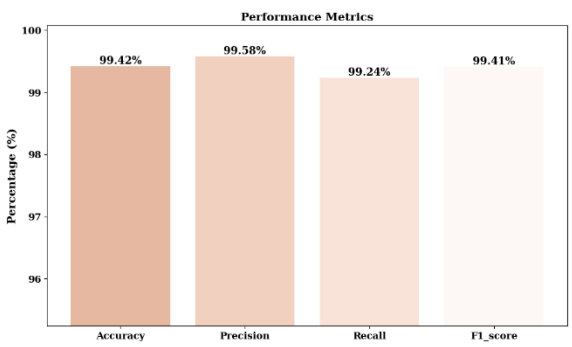

Figure 2: *Performance of Proposed Model*

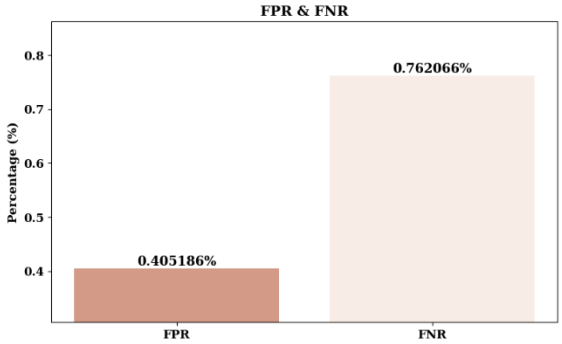

Figure 3: *Performance of FPR and FNR*

4.2 Hyperparameter Tuning of Accuracy and Parameter Sets

The change in model accuracy is due to adjustments in hyperparameters. The increase in the accuracy score from a value of 0.8500 in the case of Param Set 1 to 0.9942 in Param Set 5 implies improvements to the accuracy of the model due to hyperparameter adjustment. This trend that the prediction accuracy is improved when fine-tuning e-commerce transaction security model-related hyperparameters such as learning rate, the batch size of data or even the structure of the network itself.

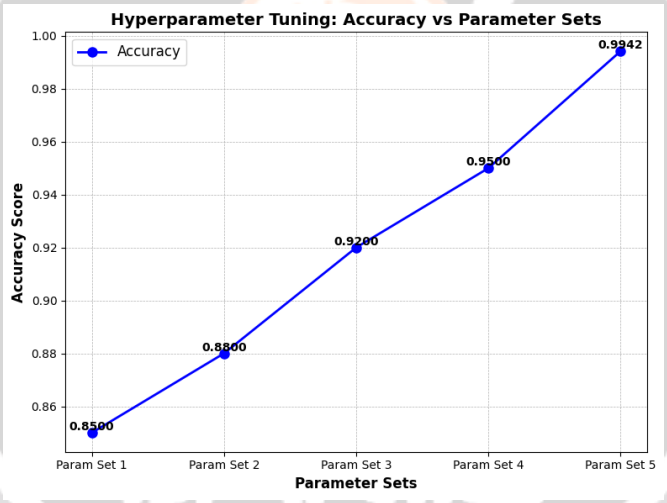

Figure 4: *Performance of Hyperparameter Tuning*

Conclusions and Future Scope

This is a security model driven by AI to increase the security related to e-commerce transactions using cloud computing and big data analytics for its operation. Data integrity and privacy were guaranteed through blockchain logging and homomorphic encryption and the hybrid CNN-GRU model successfully identifies temporal and geographical patterns in transactions. The model achieved an F1-score of 99.41 percent, accuracy of 99.42 percent, precision of 99.58 percent and recall of 99.24 percent considerably surpassing conventional approaches. Robust fraud detection was evidenced by a false positive rate of 0.762 percent and a false positive rate of 0.405 percent. Accuracy improved further from 85.00 percent to 99.42 percent using hyperparameter tuning. Future work will develop the framework to be more scalable, efficient and secure for e-commerce applications by incorporating real-time deployment explainable AI for interpretability, federated learning for privacy, multi-modal data fusion for enhancement of detection and edge computing for low latency processing.

References

[1] Hassan, M. A., Shukur, Z., & Hasan, M. K. (2020). An efficient secure electronic payment system for e-commerce. computers, 9(3), 66.

[2] Pulakhandam, W., & Samudrala, V. K. (2020). Automated Threat Intelligence Integration To Strengthen SHACS For Robust Security In Cloud-Based Healthcare Applications. International Journal of Engineering & Science Research, 10(4).
[3] Ramachandran, K. (2018). Securing PII data in payment transactions: Challenges and solutions. International Journal of Core Engineering & Management, 5(8), 48-55.
[4] Dondapati, K. (2020). Clinical implications of big data in predicting cardiovascular disease using SMOTE for handling imbalanced data. Journal of Cardiovascular Disease Research, 11(9), 191-202.
[5] Salleh, F., Yatin, M., Radzi, M., Kamis, S., Zakaria, S., Husaini, H., ... & Rambli, Y. R. (2020). Malaysian's new digital initiative to boost e-commerce–where we are. Journal of Academic Research in Business and Social Sciences, 10(11), 1138-1154.
[6] Grandhi, S. H. (2020). Blockchain-enabled software development traceability: Ensuring secure and transparent software lifecycle management. International Journal of Information Technology & Computer Engineering, 8(3).
[7] Bagaa, M., Taleb, T., Bernabe, J. B., & Skarmeta, A. (2020). A machine learning security framework for iot systems. IEEE access, 8, 114066-114077.
[8] Natarajan, D. R. (2020). AI-Generated Test Automation for Autonomous Software Verification: Enhancing Quality Assurance Through AI-Driven Testing. Journal of Science and Technology, 5(5).
[9] Mandru, S. (2018). The Role of Cybersecurity in Protecting Financial Transactions. Journal of Scientific and Engineering Research, 5(3), 503-510.
[10] Srinivasan, K. (2020). Neural network-driven Bayesian trust prediction model for dynamic resource management in cloud computing and big data. International Journal of Applied Science Engineering and Management, 14(1).
[11] Bellamkonda, S. (2018). Data Security: Challenges, Best Practices, and Future Directions. International Journal of Communication Networks and Information Security, 10, 256-259.
[12] Chauhan, G. S. (2020). UTILIZING DATA MINING AND NEURAL NETWORKS TO OPTIMIZE CLINICAL DECISION-MAKING AND PATIENT OUTCOME PREDICTIONS. International Journal of Marketing Management, 8(4), 32-51.
[13] Kambourakis, G., Gomez Marmol, F., & Wang, G. (2018). Security and Privacy in Wireless and Mobile Networks. Future internet, 10(2), 18.
[14] Gollapalli, V. S. T. (2020). ENHANCING DISEASE STRATI FICATION USING FEDERATED LEARNING AND BIG DATA ANALYTICS IN HEALTHCARE SYSTEMS. International Journal of Management Research and Business Strategy, 10(4), 19-38.
[15] Xing, Z. (2018). The impacts of Information and Communications Technology (ICT) and E-commerce on bilateral trade flows. International Economics and Economic Policy, 15, 565-586.
[16] Gollapalli, V. S. T. (2020). Scalable Healthcare Analytics in the Cloud: Applying Bayesian Networks, Genetic Algorithms, and LightGBM for Pediatric Readmission Forecasting. International Journal of Life Sciences Biotechnology Pharma Sciences, 16(2).
[17] Nahiduzzaman, K. M., Aldosary, A. S., & Mohammed, I. (2019). Framework analysis of E-commerce induced shift in the spatial structure of a city. Journal of Urban Planning and Development, 145(3), 04019006.
[18] Ganesan, T. (2020). DEEP LEARNING AND PREDICTIVE ANALYTICS FOR PERSONALIZED HEALTHCARE: UNLOCKING EHR INSIGHTS FOR PATIENT-CENTRIC DECISION SUPPORT AND RESOURCE OPTIMIZATION. International Journal of HRM and Organizational Behavior, 8(3).
[19] Bilgihan, A., Kandampully, J., & Zhang, T. (2016). Towards a unified customer experience in online shopping environments: Antecedents and outcomes. International Journal of Quality and Service Sciences, 8(1), 102-119.
[20] Panga, N. K. R., & Thanjaivadivel, M. (2020). Adaptive DBSCAN and Federated Learning-Based Anomaly Detection for Resilient Intrusion Detection in Internet of Things Networks. International Journal of Management Research and Business Strategy, 10(4).
[21] Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. European Journal on Criminal Policy and Research, 23, 287-300.
[22] Dyavani, N. R., & Hemnath, R. (2020). Blockchain-integrated cloud software networks for secure and efficient ISP federation in large-scale networking environments. International Journal of Engineering Research and Science & Technology, 16(2). https://ijerst.org/index.php/ijerst/article/view/614/558

[23] Maguerra, S., Boulmakoul, A., Karim, L., & Badir, H. (2018, May). Scalable solution for profiling potential cyber-criminals in Twitter. In Proceedings of the Big Data & Applications 12th Edition of the Conference on Advances of Decisional Systems, Marrakech, Morocco (pp. 2-3).
[24] Durai Rajesh Natarajan, & Sai Sathish Kethu. (2019). Decentralized anomaly detection in federated learning: Integrating one-class SVM, LSTM networks, and secure multi-party computation on Ethereum blockchain. International Journal of Computer Science Engineering Techniques, 5(4).
[25] Kamran, A., Arafeen, Q. U., & Shaikh, A. A. (2019). Existing Cyber Laws and Their Role in Legal Aspects of Cybercrime in Pakistan. International Journal of Cyber-Security and Digital Forensics, 8(3), 241-250.
[26] Nagarajan, H., & Kurunthachalam, A. (2018). Optimizing database management for big data in cloud environments. International Journal of Modern Electronics and Communication Engineering, 6(1).
[27] Louw, C., & Von Solms, S. (2014, May). Online social networks to online social malworks—The evolution of an industry. In 2014 IST-Africa Conference Proceedings (pp. 1-7). IEEE.
[28] Basani, D. K. R., & Aiswarya, R. S. (2018). Integrating IoT and robotics for autonomous signal processing in smart environment. International Journal of Information Technology and Computer Engineering, 6(2).
[29] Razali, M. A., & Mohd Shariff, S. (2019, November). Cmblock: In-browser detection and prevention cryptojacking tool using blacklist and behavior-based detection method. In International Visual Informatics Conference (pp. 404-414). Cham: Springer International Publishing.
[30] Gudivaka, B. R., & Palanisamy, P. (2018). Enhancing software testing and defect prediction using Long Short-Term Memory, robotics, and cloud computing. International Journal of modern electronics and communication Engineering, 6(1).
[31] Huang, D., Mu, D., Yang, L., & Cai, X. (2018). CoDetect: Financial fraud detection with anomaly feature detection. Ieee Access, 6, 19161-19174.
[32] Kodadi, S., & Kumar, V. (2018). Lightweight deep learning for efficient bug prediction in software development and cloud-based code analysis. International Journal of Information Technology and Computer Engineering, 6(1).
[33] Jain, Y., Tiwari, N., Dubey, S., & Jain, S. (2019). A comparative analysis of various credit card fraud detection techniques. International Journal of Recent Technology and Engineering, 7(5), 402-407.
[34] Bobba, J., & Prema, R. (2018). Secure financial data management using Twofish encryption and cloud storage solutions. International Journal of Computer Science Engineering Techniques, 3(4), 10–16.
[35] Raghavan, P., & El Gayar, N. (2019, December). Fraud detection using machine learning and deep learning. In 2019 international conference on computational intelligence and knowledge economy (ICCIKE) (pp. 334-339). IEEE.
[36] Gollavilli, V. S. B., & Thanjaivadivel, M. (2018). Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. International Journal of Information Technology and Computer Engineering, 6(4), 77–85. ISSN 2347–3657.
[37] Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit card fraud detection using AdaBoost and majority voting. IEEE access, 6, 14277-14284.
[38] Nippatla, R. P., & Palanisamy, P. (2018). Enhancing cloud computing with eBPF powered SDN for secure and scalable network virtualization. Indo-American Journal of Life Sciences and Biotechnology, 15(2).
[39] Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M. S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. Ieee Access, 7, 93010-93022.
[40] Budda, R., & Pushpakumar, R. (2018). Cloud Computing in Healthcare for Enhancing Patient Care and Efficiency. Chinese Traditional Medicine Journal, 1(3), 10-15.
[41] Krishna, V. B., Gunter, C. A., & Sanders, W. H. (2018). Evaluating detectors on optimal attack vectors that enable electricity theft and DER fraud. IEEE Journal of Selected Topics in Signal Processing, 12(4), 790-805.
[42] Vallu, V. R., & Palanisamy, P. (2018). AI-driven liver cancer diagnosis and treatment using cloud computing in healthcare. Indo-American Journal of Life Sciences and Biotechnology, 15(1).
[43] Alsayed, A., & Bilgrami, A. (2017). E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. International Journal of Emerging Technology and advanced engineering, 7(1), 109-115.

[44] Jayaprakasam, B. S., & Hemnath, R. (2018). Optimized microgrid energy management with cloud-based data analytics and predictive modelling. International Journal of modern electronics and communication Engineering, 6(3), 79–87.
[45] Airehrour, D., Vasudevan Nair, N., & Madanian, S. (2018). Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model. Information, 9(5), 110.
[46] Mandala, R. R., & N, Purandhar. (2018). Optimizing secure cloud-enabled telemedicine system using LSTM with stochastic gradient descent. Journal of Science and Technology, 3(2).
[47] Rastenis, J., Ramanauskaitė, S., Janulevičius, J., Čenys, A., Slotkienė, A., & Pakrijauskas, K. (2020). E-mail-based phishing attack taxonomy. Applied sciences, 10(7), 2363.
[48] Garikipati, V., & Palanisamy, P. (2018). Quantum-resistant cyber defence in nation-state warfare: Mitigating threats with post-quantum cryptography. Indo-American Journal of Life Sciences and Biotechnology, 15(3).
[49] Lonzetta, A. M., Cope, P., Campbell, J., Mohd, B. J., & Hayajneh, T. (2018). Security vulnerabilities in Bluetooth technology as used in IoT. Journal of Sensor and Actuator Networks, 7(3), 28.
[50] Ubagaram, C., & Mekala, R. (2018). Enhancing data privacy in cloud computing with blockchain: A secure and decentralized approach. International Journal of Engineering & Science Research, 8(3), 226–233.
[51] Ficetola, G. F., Pansu, J., Bonin, A., Coissac, E., Giguet-Covex, C., De Barba, M., ... & Taberlet, P. (2015). Replication levels, false presences and the estimation of the presence/absence from eDNA metabarcoding data. Molecular ecology resources, 15(3), 543-556.
[52] Ganesan, S., & Kurunthachalam, A. (2018). Enhancing financial predictions using LSTM and cloud technologies: A data-driven approach. Indo-American Journal of Life Sciences and Biotechnology, 15(1).
[53] Port, J. A., O'Donnell, J. L., Romero-Maraccini, O. C., Leary, P. R., Litvin, S. Y., Nickols, K. J., ... & Kelly, R. P. (2016). Assessing vertebrate biodiversity in a kelp forest ecosystem using environmental DNA. Molecular ecology, 25(2), 527-541.
[54] Musam, V. S., & Kumar, V. (2018). Cloud-enabled federated learning with graph neural networks for privacy-preserving financial fraud detection. Journal of Science and Technology, 3(1).
[55] Arango-Argoty, G., Garner, E., Pruden, A., Heath, L. S., Vikesland, P., & Zhang, L. (2018). DeepARG: a deep learning approach for predicting antibiotic resistance genes from metagenomic data. Microbiome, 6, 1-15.
[56] Musham, N. K., & Pushpakumar, R. (2018). Securing cloud infrastructure in banking using encryption-driven strategies for data protection and compliance. International Journal of Computer Science Engineering Techniques, 3(5), 33–39.
[57] Li, Z., Yi, Y., Luo, X., Xiong, N., Liu, Y., Li, S., ... & Ye, F. (2020). Development and clinical application of a rapid IgM-IgG combined antibody test for SARS-CoV-2 infection diagnosis. Journal of medical virology, 92(9), 1518-1524.
[58] Radhakrishnan, P., & Mekala, R. (2018). AI-Powered Cloud Commerce: Enhancing Personalization and Dynamic Pricing Strategies. International Journal of Applied Science Engineering and Management, 12(1)
[59] Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. BMC genomics, 21, 1-13.
[60] Nagarajan, H., & Kumar, R. L. (2020). Enhancing healthcare data integrity and security through blockchain and cloud computing integration solutions. International Journal of Engineering Technology Research & Management, 4(2).
[61] Chevrot, A., Vernotte, A., Bernabe, P., Cretin, A., Peureux, F., & Legeard, B. (2020, December). Improved testing of AI-based anomaly detection systems using synthetic surveillance data. In Proceedings (Vol. 59, No. 1, p. 9). MDPI.
[62] Gudivaka, B. R., & Thanjaivadivel, M. (2020). IoT-driven signal processing for enhanced robotic navigation systems. International Journal of Engineering Technology Research & Management, 4(5).
[63] Zhou, X., Liang, W., Shimizu, S., Ma, J., & Jin, Q. (2020). Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems. IEEE Transactions on Industrial Informatics, 17(8), 5790-5798.
[64] Chetlapalli, H., & Pushpakumar, R. (2020). Enhancing accuracy and efficiency in AI-driven software defect prediction automation. International Journal of Engineering Technology Research & Management, 4(8).

[65] Zhang, Y., Li, M., Dong, Z. Y., & Meng, K. (2019). Probabilistic anomaly detection approach for data-driven wind turbine condition monitoring. CSEE Journal of Power and Energy Systems, 5(2), 149-158.
[66] Budda, R., & Mekala, R. (2020). Cloud-enabled medical image analysis using ResNet-101 and optimized adaptive moment estimation with weight decay optimization. International Research Journal of Education and Technology, 03(02).
[67] Liu, X., Lun, H., Fu, M., Fan, Y., Yi, L., Hu, W., & Zhuge, Q. (2020). AI-based modeling and monitoring techniques for future intelligent elastic optical networks. Applied Sciences, 10(1), 363.
[68] Vallu, V. R., & Rathna, S. (2020). Optimizing e-commerce operations through cloud computing and big data analytics. International Research Journal of Education and Technology, 03(06).
[69] Zhou, X., Hu, Y., Liang, W., Ma, J., & Jin, Q. (2020). Variational LSTM enhanced anomaly detection for industrial big data. IEEE Transactions on Industrial Informatics, 17(5), 3469-3477.
[70] Jayaprakasam, B. S., & Padmavathy, R. (2020). Autoencoder-based cloud framework for digital banking: A deep learning approach to fraud detection, risk analysis, and data security. International Research Journal of Education and Technology, 03(12).
[71] Faust, K., Xie, Q., Han, D., Goyle, K., Volynskaya, Z., Djuric, U., & Diamandis, P. (2018). Visualizing histopathologic deep learning classification and anomaly detection using nonlinear feature space dimensionality reduction. BMC bioinformatics, 19, 1-15.
[72] Mandala, R. R., & Kumar, V. K. R. (2020). AI-driven health insurance prediction using graph neural networks and cloud integration. International Research Journal of Education and Technology, 03(10).
[73] Chung, J. J., & Kim, H. J. (2020). An automobile environment detection system based on deep neural network and its implementation using IoT-enabled in-vehicle air quality sensors. Sustainability, 12(6), 2475.
[74] Ubagaram, C., & Kurunthachalam, A. (2020). Bayesian-enhanced LSTM-GRU hybrid model for cloud-based stroke detection and early intervention. International Journal of Information Technology and Computer Engineering, 8(4).
[75] Alsariera, Y. A., Adeyemo, V. E., Balogun, A. O., & Alazzawi, A. K. (2020). Ai meta-learners and extra-trees algorithm for the detection of phishing websites. IEEE access, 8, 142532-142542.
[76] Ganesan, S., & Hemnath, R. (2020). Blockchain-enhanced cloud and big data systems for trustworthy clinical decision-making. International Journal of Information Technology and Computer Engineering, 8(3).
[77] Diraco, G., Leone, A., & Siciliano, P. (2019). AI-based early change detection in smart living environments. Sensors, 19(16), 3549.
[78] Musam, V. S., & Purandhar, N. (2020). Enhancing agile software testing: A hybrid approach with TDD and AI-driven self-healing tests. International Journal of Information Technology and Computer Engineering, 8(2).
[79] Santosh, K. C. (2020). AI-driven tools for coronavirus outbreak: need of active learning and cross-population train/test models on multitudinal/multimodal data. Journal of medical systems, 44(5), 93.
[80] Musham, N. K., & Bharathidasan, S. (2020). Lightweight deep learning for efficient test case prioritization in software testing using MobileNet & TinyBERT. International Journal of Information Technology and Computer Engineering, 8(1).