International Journal of Arts Humanities and Social Sciences Studies
Volume 10 Issue 03 ‖ March 2025
ISSN: 2582-1601
www.ijahss.com

Securing and Storing Financial Data in the Cloud Using Lattice-Based Cryptography

Rajani Priya Nippatla[1], Sunil Kumar Alavilli[2], Bhavya Kadiyala[3], Chaitanya Vasamsetty[4], Subramanyam Boyapati[5], Purandhar. N[6, *]

[1]Kellton Technologies Inc, Texas, USA, [2]Sephora, California, USA, [3]Parkland Health, Texas, USA, [4]Elevance Health, Georgia, USA [5]American Express, Arizona, USA
[6]Assistant Professor, Department of CSE (Artificial Intelligence) School of Computers Madanapalle Institute of Technology and Science, Madanapalle, Andhra Pradesh

[*]Corresponding Author Name: Purandhar. N Corresponding Email: purandhar.n@gmail.com

Abstract: *Finance is a kind of territory on which empirical models rely-for their operation, they can be used anywhere in the world as an open-access model. This study is to harvest financial information from a database provided and save that information in the secure space of a cloud storage arrangement for purposes of data protection and privacy. In the fordable structures of human existence, this research makes a formal framework that presents the steps in the process from data gathering, pre-processing, and encryption through to enhanced security with the use of the Lightweight Block Cipher (LBC)-cloud storage. Thus, secure and efficient accessibility and management of financial information for future analysis and decision making can be achieved. The encryption analysis shows that 100 MB files take three seconds, 500 MB require around 15 seconds, and 1000 MB take around 30 seconds for the process. The individual upload speeds are from 10 to around 50 Mbps, while the lateness decline from around 35-static ms in stage one to just below 10 ms when processing reaches stage seven-drop as time passes during the trials to give very efficient results.*

Keywords: *Cloud Storage, Lattice-Based Cryptography (LBC), Encryption, Cloud Computing.*

I. INTRODUCTION

Cloud computing and big data analytics, which, in conjunction, improve financial data security, cite a great need for security in this digital era, especially for confidential data protection[1], [2]. This combination aids the analysis of financial data, especially in cases pertaining to high-dimensional input with sophisticated methods that ensure accurate predictive maintenance and anomaly detection[3], [4]. The cloud ensures near-infinite processing and storage for long-term archiving and analysis[5], [6]. With the occurrence of digital transformation, these organizational procedures, especially in cost accounting and financial management, have been completely transformed[7], [8]. The Internet of Things (IoT) enabling technologies are focused on wearable sensors, cloud computing, and lightweight communication protocols[9], [10].

Every stage is designed to serve the purpose of maximizing data processing efficiency, especially in cloud-computing scenarios where massive degrees of data velocity and volume are being considered[11], [12]. In adoption of cloud computing for big data, it gives the viewpoint of a company on how to cope with and analyse massive amounts of data through the adoption of cloud-based technology[13], [14]. Encrypting technology would therefore go a long way in providing security to any data sent to and kept on a cloud server[15], [16]. These new technologies have practically created an unthinkable level of cost reduction, scalability, and flexibility for the modern-day enterprise[17], [18]. With a more unstable business environment, cloud computing has come across as a disruptive technology giving small and medium enterprises (SMEs) exceptional opportunities to achieve operational efficiency and strategic growth[19], [20].

The aim of ensuring scalability and to guarantee computational economy is served with the system via cloud infrastructure, while also providing a trustworthy and secure environment[21], [22]. Through seamless and scalable solutions for managing and storing data, cloud computing has left almost every industry changing its operation platforms[23], [24].

The structure of the paper is as follows. Section 2 deals with a literature survey on ensuring security for financial data and those on Lattice Based Cryptography and cloud storage technologies in general. Section 3 specifies the methodology Section 4. tells about the results with values Section 5 concludes the paper.

II. LITERATURE SURVEY

The focus of this study is AI-based fraud investigation in the IoT domain-an advanced anomaly detection and clustering approaches. AI systems are mainly supervised and unsupervised learning methods that use historical transaction data to differentiate between legit and fraud activity[25], [26]. The study focuses on the key methods, datasets, and evaluation metrics for adaptive learning, which enables continuous improvement of the model through retraining frequently and automating response.

The research proposes an intelligent education management platform utilizing cloud computing and AI capable of enhancing educational service delivery through intelligent automation and personalized learning. Built on a service-oriented architecture (SOA) and deployed within a Hadoop-managed server cluster such that high processing efficiency and scalable data management assured[27], [28]. Massive data access and high concurrency create enabling environments for effective resource management and remote learning. Nevertheless, the whole approach lacks a rich understanding concerning aspects.

CFMSiC, stands for Cognitive Financial Management Systems in the Cloud, refers to a brand-new subclass of intelligent financial management systems for financial data management that uses cognitive techniques and semantic analysis. With a view to solving the key trust problem pertaining to confidential data protection among groups of trusted clients, these systems extend the scope of traditional financial facilities in the light of added advanced information-sharing protocol layered on top of threshold schemes[29], [30]. CFMSiC deals with an intuitive secure and strategic financial data management mechanism backed by a mechanism for innovative sharing and encryption over cloud-based systems.

The research examines the risks and challenges financial institutions encounter when integrating cloud computing for data processing, emphasizing the need for intelligent solutions to enhance efficiency and security. It highlights the importance of regulatory policies to mitigate concentration risks while ensuring data privacy[31], [32]. Additionally, the study explores the role of intelligent forecasting and evaluation technologies in financial data management, supporting digital transformation in the sector.

It intends to develop an enterprise-level financial management information system on cloud computing and big data environment. It is introducing the business-driven value management concept aimed at enhancing financial management through an expense management framework. This study describes many significant improvements, such as an 84.7% decrease in personnel across subsidiaries, with the average number of employees per subsidiary decreasing from 23 to 3.5 and an almost threefold increase in financial assets from 23 billion yuan to 68.55 billion yuan over nine years[33], [34]. Cloud computing technology provides a key role in reducing investment costs, attaining high reliability standards, allowing modular expansion on demand, and ensuring minimal financial informatization implementation time.

Owing to a discrepancy in cloud computing service implementations in the financial domain that involved security concerns, this study employed actor-based stakeholder modeling and assessed security concerns. The study used actor-dependency-based methods of modeling requirements on the changing financial sector vis-a-vis i*-style modeling where fictitious use cases of a hypothetical bank have been used to exemplify the adoption process[35], [36]. This research presents a new insight in being the first to actually model stakeholder involvement and change management processes in the financial service cloud; bringing technology into the realm of business-wise insights.

2.1. Problem Statement

In addition to the aforementioned limitations, the study is mostly confined to larger commercial organizations, i.e., 50+physical servers, but it may not be extrapolated to Small/Medium Businesses, neither may they apply to one with lesser transaction volumes and smaller data centre[37], [38]. For small organizations, expense considerations in cloud technologies may not have been fully appreciated, or implementation complexities could be far beyond organizations that do not possess required assets, headcounts, or expertise to build end-to-end automation[39], [40]. The financial metrics and their interpretations for cloud adoption could differ across industries, thus limiting the generalization of the findings.

III. METHODOLOGY

This strategic framework is designed to execute the systematic handling and storage of financial information. Starting from data collection, the fundamental stage involves the gathering of financial information that is subject to an in-depth analysis is shown in figure 1. The pre-processing is done to take care of missing values and to convert categorical data into some format before more processing can be done. After all this, the data will be encrypted using the Lightweight Block Cipher (LBC) method to improve security. The results encrypted are uploaded to cloud storage allowing for the better scale and access from different remote sites. Finally, an evaluation will be done regarding the performances by analysing the time taken for encryption, upload speed, and overall system efficiency-for a safe and optimized financial data management process.

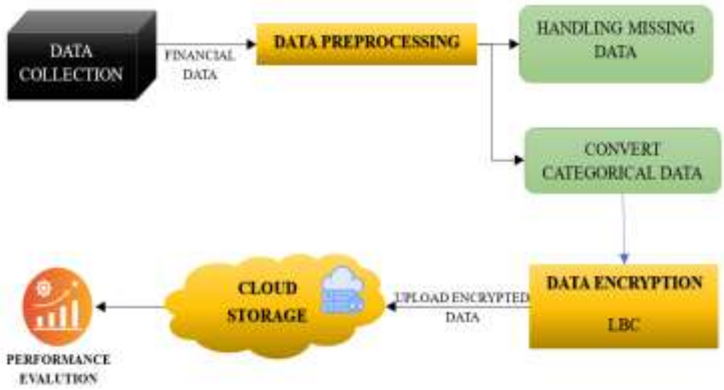

Figure 1: Secure Financial Data Processing Workflow

3.1. Data Collection

The data may include transactions with financial statements, market trends, and so on, which are necessary for a good analysis. Raw data usually contains a lot of inconsistencies, missing values, and sometimes requires pre-processing for categorical attributes. So, the data should be collected for proper accuracy, completeness, and reliability, ensuring further data processing will be a foundation already secure for encryption and data storage in the cloud with good management of financial data.

3.2. Data Pre-Processing

The most vital step that manipulates the raw financial figures to prepare for analysis after handling missing values and converting categorical data into some appropriate formats. This would ensure data consistency and accuracy and the data should be complete before encryption. Proper pre-processing continues to enhance the quality of 'data readiness' while being prepared to be secured for storage and then further processing.

3.2.1. Handling Missing Data

Handling missing data is an important step in pre-processing the data for ensuring quality and reliability of the data. Missing values for financial data may occur due to partial records or system errors in entries created by humans. Several methods such as mean imputation, regression techniques, or deletion strategies are used to deal with missing data. Well-handled missing data improves the accuracy of any later analyses and ensures consistency between the encrypted and stored data.

3.2.2. Convert Categorical Data

This workflow actually converts the non-numerical data types into a numerical format, which will make it easier to process and analyse. Here, this conversion is required, as much of the machine learning and data analysis techniques require numerical values as inputs. Common ways of conversion can be one-hot encoding, label encoding, ensuring that categorical variables have meaningful representation. Proper conversion enhances consistency of data and increased accuracy in processing financial data.

3.3. Data Encryption using LBC

Lightweight Block Cipher (LBC) data encryption acts as the immediate line of defence securing financial data before it is stored. It provides strong encryption along with very low computational overhead making it applicable to cloud-based applications. Thus, plaintext financial data is converted into ciphertext using LBC, which allows only authorized users with the correct key for decryption to access the original information. All unauthorized access, breaches and cyber threats are guarded against, ensuring that data protects its integrity as well as confidentiality. Besides, LBC creates seamless encryption without the noticeable sligh on system performance. Financial data is completely encrypted and uploaded safely onto the cloud to further secure data and access. The encryption process typically follows a transformation function is given in equation (1).

$$C = E_K(P) \tag{1}$$

Were C is the ciphertext, P is the plaintext, and E_K represents encryption using key K. Decryption follows the inverse function is given

$$P = D_K(C) \tag{2}$$

Were D_K is the decryption function using the same or a related key. This approach ensures that only authorized users can access the encrypted financial data securely stored in the cloud.

3.4. Cloud Storage

The essence of cloud storage is safely and scalable storing financial data securely so that confidentiality and integrity can be ensured. It allows authorized persons to gain remote access for proper retrieval and management of data from wherever required. When financial data is stored in the cloud, it is protected from a myriad of risks such as hardware failures, cyber-attacks, and data corruption. The finest point is that cloud storage ensures the availability of data, thereby enabling companies to carry out their financial affairs and make informed decisions. Another advantage is that it provides scalability, enabling them to handle increasing volumes of financial data without losses in performance. In this way, after data encryption, the data can be transmitted safely into the cloud for long-term storage, access, and management of financial data.

IV. RESULT

This result analyses the performance of secure financial data processing in terms of encryption time, upload speed, and latency for the completed work. The findings justify the promise of security in the management of such financial data, as purported by the approach advanced.

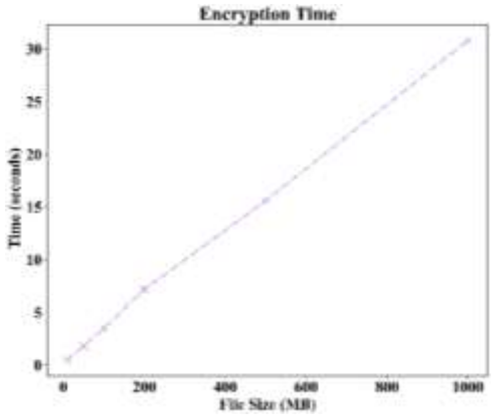

Figure 2: Encryption Time

Figure 2 correlates file size in megabytes with encryption time in seconds, depicting the gradual increase in encryption time while file size increases. Smaller files such as that of 100 MB take about 3 seconds to encrypt, while roughly 15 seconds are required for a 500 MB file. For 1000 MB, the encryption time stretches to 30 seconds. It can thus be inferred that, as the file size increases, encryption time increases in a proportionate manner, maintaining a steady encryption performance.

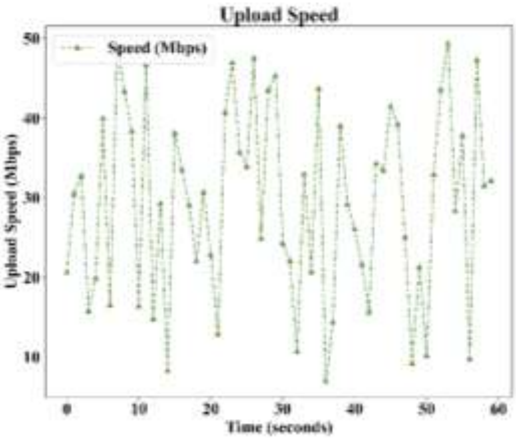

Figure 3: Upload Speed

Figure 3 represents the measurement collection of the accessing time (in seconds) spend on uploads from an actual data transfer in megabits per second (Mbps). The trend shows fluctuation over a period of time which makes the variation of the upload time over the 60 odd seconds definite. As observed, the upload speed has a range of fluctuation from 10 Mbps to 50 Mbps with no defined transmission rate. At one point, the speeds reportedly peaked at around 50 Mbps and suddenly dropped at other times to approximately 10 Mbps. It portrays the dynamic aspect of data continuity, which may be affected differently by network congestion or bandwidth restrictions in addition to server response.

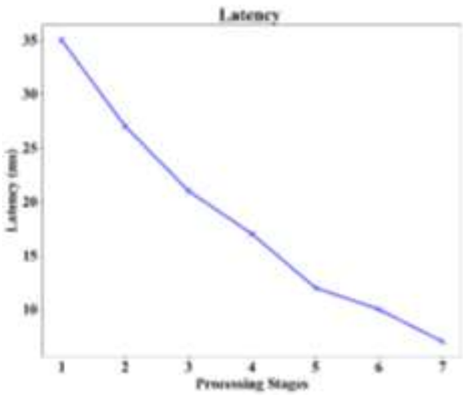

Figure 4: Latency

Figure 4 depicts latency (ms) at different stages of processing, following a downward pattern in its trend. The initial value of latency at stage 1 is around 35 ms, but it gradually decreases to about 20 ms in stage 3. Post optimization, this latency sinks below 10 ms at 7th stage which is actually an indication that they are improving efficiencies. Continual dropping indicated that as the system further progresses into higher stages of processing, the latency keeps reducing which contributes it towards efficiency and responsiveness.

V. CONCLUSION

The proposed approach establishes a secured environment for the financial data transaction life cycle, including the data entry, processing, lightweight block cipher (LBC) encryption, and cloud upload. In terms of time analysis for the encryption, it takes 3 seconds for 100 MB, 15 seconds for 500 MB and 30 seconds for 1000 MB-a straight line on the time curve. The upload speed varies between 10-50 Mbps due to the network, while the time lag reduces from 35 ms in stage 1 to lesser than 10 ms in stage 7, thus increasing efficiency. This indeed highlights the feasible scenario for making this system secure and-optimized for handling financial data. Future works include blockchain technology to have strong data integrity and edge computing to minimize latency in the process.

REFERENCES

[1] R. K. M. K. Yalla, "Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data," *Int. J. Eng. Res. Sci. Technol.*, vol. 17, no. 4, pp. 23–32, Oct. 2021.

[2] R. Ayyadurai, "Smart surveillance methodology: Utilizing machine learning and AI with blockchain for bitcoin transactions," *World J. Adv. Eng. Technol. Sci.*, vol. 1, no. 1, pp. 110–120, 2020, doi: 10.30574/wjaets.2020.1.1.0023.

[3] Akhil, R. G., Yallamelli, V., Mamidala, V., & Yalla, R. K. M. (2020). A cloud-based financial data modeling system using GBDT, ALBERT, and Firefly Algorithm optimization for high-dimensional generative topographic mapping. International Journal of Modern Electronics and Communication Engineering, 8(4).

[4] Rajeswaran, A. (2021). Big data analytics and demand-information sharing in eCommerce supply chains: Mitigating manufacturer encroachment and channel conflict. International Journal of Applied Science Engineering and Management, 15(3).

[5] R. K. M. K. Yalla, A. R. G. Yallamelli, and V. Mamidala, "A Distributed Computing Approach to IoT Data Processing: Edge, Fog, and Cloud Analytics Framework," *Int. J. Inf. Technol. Comput. Eng.*, vol. 10, no. 1, pp. 79–94, Jan. 2022.

[6] Ayyadurai, R. (2022). Transaction security in e-commerce: Big data analysis in cloud environments. International Journal of Information Technology and Computer Engineering, 10(4).

[7] Mamidala, V., Yallamelli, A. R. G., & Yalla, R. K. M. K. (2022). Leveraging robotic process automation (RPA) for cost accounting and financial systems optimization — A case study of ABC Company. International Journal of Research in Engineering Technology, 7(6).

[8] Bobba, J. (2021). ENTERPRISE FINANCIAL DATA SHARING AND SECURITY IN HYBRID CLOUD ENVIRONMENTS: AN INFORMATION FUSION APPROACH FOR BANKING SECTORS. INTERNATIONAL JOURNAL OF MANAGEMENT RESEARCH AND REVIEWS 11(3).

[9] Yallamelli, A. R. G., & Devarajan, M. V. (2023). HYBRID EDGE-AI AND CLOUDLET-DRIVEN IOT FRAMEWORK FOR REAL-TIME HEALTHCARE. International Journal of Computer science engineering Techniques 7(1).

[10] J. Bobba, "Cloud-Based Financial Models: Advancing Sustainable Development in Smart Cities," *Int. J. HRM Organ. Behav.*, vol. 11, no. 3, pp. 27–43, Aug. 2023.

[11] V. Mamidala, "Optimizing Performance with Parallel K-Means in Tunnel Monitoring Data Clustering Algorithm for Cloud Computing," *Int. J. Eng. Res. Sci. Technol.*, vol. 17, no. 4, pp. 34–49, Dec. 2021.

[12] J. Bobba, R. Ayyadurai, K. Parthasarathy, N. K. R. Panga, R. L. Bolla, and R. O. Ogundokun, "AI-Infused Spiking Neural Architectures and Edge Computing Modalities: Recalibrating Pandemic Surveillance, Dynamic Health Interpretations, and Contextual Automations in Complex Urban Terrains," *Int. J. Inf. Technol. Comput. Eng.*, vol. 11, no. 2, pp. 60–74, May 2023.

[13] Mani Kanta Yalla, R. K., Yallamelli, A. R. G., & Mamidala, V. (2022). A distributed computing approach to IoT data processing: Edge, fog, and cloud analytics framework. International Journal of Information Technology & Computer Engineering, 10(1).

[14] J. Bobba and R. L. Bolla, "Next-Gen HRM: AI, Blockchain, Self-Sovereign Identity, and Neuro-Symbolic AI for Transparent, Decentralized, and Ethical Talent Management in the Digital Era," *Int. J. HRM Organ. Behav.*, vol. 7, no. 4, pp. 31–51, Nov. 2019.

[15] Yallamelli, A. R. G. (2021). Improving cloud computing data security with the RSA algorithm. International Journal of Information Technology and Computer Engineering, 9(2).

[16] J. Bobba and R. L. Bolla, "Dynamic Federated Data Integration and Iterative Pipelines for Scalable E-Commerce Analytics Using Hybrid Cloud and Edge Computing," *Int. J. Inf. Technol. Comput. Eng.*, vol. 9, no. 4, pp. 133–150, Oct. 2021.

[17] Yallamelli, A. R. G. (2021). Critical challenges and practices for securing big data on cloud computing: A systematic AHP-based analysis. Journal of Current Science & Humanities, 9(3).

[18] J. Bobba, R. L. Bolla, E. F. Abiodun, and S. Amin, "The ATTRIBUTE-BASED K-ANONYMITY AND SE-PSO-ENHANCED SIGMOID-LECUN-TCN FOR MITIGATING RANSOMWARE ATTACK WITH API PROTECTION FOR CLOUD APPLICATIONS: RANSOMWARE ATTACK WITH API PROTECTION FOR CLOUD APPLICATION," *Int. J. Adv. Res. Inf. Technol. Manag. Sci.*, vol. 1, no. 01, Art. no. 01, Dec. 2024.

[19] A. R. G. Yallamelli, "CLOUD COMPUTING AND MANAGEMENT ACCOUNTING IN SMES: INSIGHTS FROM CONTENT ANALYSIS, PLS- SEM, AND CLASSIFICATION AND REGRESSION TREES," *Int. J. Eng.*, vol. 11, no. 3.

[20] Bolla, R. L., & Bobba, J. (2021). Optimizing AI-driven resource management: Hierarchical LDA, autoencoders, and Isomap for enhanced dimensionality reduction. International Journal of Mathematical Modeling Simulation and Applications, 9(1).

[21] Akhil, R. G., Yallamelli, V., Mamidala, V., & Yalla, R. K. M. (2020). A cloud-based financial data modeling system using GBDT, ALBERT, and Firefly Algorithm optimization for high-dimensional generative topographic mapping. International Journal of Modern Electronics and Communication Engineering, 8(4).

[22] R. L. Bolla and J. Bobba, "Enhancing Usability Testing Through A/B Testing, AI-Driven Contextual Testing, and Codeless Automation Tools," *J. Sci. Technol. JST*, vol. 5, no. 5, Art. no. 5, Oct. 2020, doi: 10.46243/jst.2020.v5.i5.pp237-252.

[23] M. V. Devarajan, "Improving Security Control in Cloud Computing for Healthcare Environments," *J. Sci. Technol. JST*, vol. 5, no. 6, Art. no. 6, Dec. 2020.

[24] R. L. Bolla, R. P. Jenie, and J. Bobba, "The SECURING FINANCIAL CLOUD SERVICES: A NOVEL APPROACH USING IDENTITY-CHAIN TECHNOLOGY AND CLUSTER EVALUATION: FINANCIAL CLOUD SERVICES USING IDENTITY-CHAIN TECHNOLOGY," *Int. J. Digit. Innov. Discov.*, vol. 1, no. 01, Art. no. 01, Mar. 2025.

[25] G. Thirusubramanian, "Machine Learning-Driven AI for Financial Fraud Detection in IoT Environments," *Int. J. HRM Organ. Behav.*, vol. 8, no. 4, pp. 1–16, Oct. 2020.

[26] M. V. Devarajan, "A Comprehensive AI-Based Detection and Differentiation Model for Neurological Disorders Using PSP Net and Fuzzy Logic-Enhanced Hilbert-Huang Transform," *Int. J. Inf. Technol. Comput. Eng.*, vol. 7, no. 3, pp. 94–104, Jul. 2019.

[27] T. Ganesan, "INTEGRATING ARTIFICIAL INTELLIGENCE AND CLOUD COMPUTING FOR THE DEVELOPMENT OF A SMART EDUCATION MANAGEMENT PLATFORM: DESIGN, IMPLEMENTATION, AND PERFORMANCE ANALYSIS," *Int. J. Eng.*, vol. 11, no. 2.

[28] Devarajan, M. V. (2020). Assessing long-term serum sample viability for cardiovascular risk prediction in rheumatoid arthritis. International Journal of Information Technology and Computer Engineering, 8(2), 18–30.

[29] T. Ganesan, M. Almusawi, K. Sudhakar, B. R. Sathishkumar, and K. S. Kumar, "Resource Allocation and Task Scheduling in Cloud Computing Using Improved Bat and Modified Social Group Optimization," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–5. doi: 10.1109/NMITCON62075.2024.10699250.

[30] M. V. Devarajan, "Improving Security Control in Cloud Computing for Healthcare Environments," *J. Sci. Technol. JST*, vol. 5, no. 6, Art. no. 6, Dec. 2020.

[31] T. Ganesan, R. R. Al-Fatlawy, S. Srinath, S. Aluvala, and R. L. Kumar, "Dynamic Resource Allocation-Enabled Distributed Learning as a Service for Vehicular Networks," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594602.

[32] Devarajan, M. V. (2022). An improved BP neural network algorithm for forecasting workload in intelligent cloud computing. Journal of Current Science, 10(3).

[33] Ganesan, T. (2022). Securing IoT business models: Quantitative identification of key nodes in elderly healthcare applications. International Journal of Management Research and Reviews, 12(3).

[34] Veerappermal Devarajan, M., & Sambas, A. (2022). Data-driven techniques for real-time safety management in tunnel engineering using TBM data. International Journal of Research in Engineering Technology, 7(3).

[35] M. V. Devarajan, M. Al-Farouni, R. Srikanteswara, R. Rana Veer Samara Sihman Bharattej, and P. M. Kumar, "Decision Support Method and Risk Analysis Based on Merged-Cyber Security Risk Management," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594070.

[36] M. V. Devarajan, M. Al-Farouni, R. Srikanteswara, R. Rana Veer Samara Sihman Bharattej, and P. M. Kumar, "Decision Support Method and Risk Analysis Based on Merged-Cyber Security Risk Management," in *2024 Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, pp. 1–4. doi: 10.1109/ICDSIS61070.2024.10594070.

[37] M. V. Devarajan, S. Aluvala, V. Armoogum, S. Sureshkumar, and H. T. Manohara, "Intrusion Detection in Industrial Internet of Things Based on Recurrent Rule-Based Feature Selection," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–4. doi: 10.1109/NMITCON62075.2024.10698962.

[38] M. V. Devarajan, S. Aluvala, V. Armoogum, S. Sureshkumar, and H. T. Manohara, "Intrusion Detection in Industrial Internet of Things Based on Recurrent Rule-Based Feature Selection," in *2024 Second International Conference on Networks, Multimedia and Information Technology (NMITCON)*, Aug. 2024, pp. 1–4. doi: 10.1109/NMITCON62075.2024.10698962.

[39] M. V. Devarajan, A. R. G. Yallamelli, V. Mamidala, R. K. M. K. Yalla, T. Ganesan, and A. Sambas, "IoT-based enterprise information management system for cost control and enterprise job-shop scheduling problem," *Serv. Oriented Comput. Appl.*, Nov. 2024, doi: 10.1007/s11761-024-00438-3.

[40] M. V. Devarajan, A. R. G. Yallamelli, R. K. M. Kanta Yalla, V. Mamidala, T. Ganesan, and A. Sambas, "Attacks classification and data privacy protection in cloud-edge collaborative computing systems," *Int. J. Parallel Emergent Distrib. Syst.*, vol. 0, no. 0, pp. 1–20, 2024, doi: 10.1080/17445760.2024.2417875.