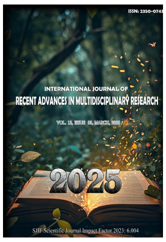
ISSN : 2350-0743

International Journal of Recent Advances in Multidisciplinary Research

Vol. 12, Issue 03 pp.10871-10876, March, 2025



RESEARCH ARTICLE

OPTIMIZED SECURE MULTI-PARTY COMPUTATION FOR CLOUD-BASED IOT DOCUMENT SHARING USING PRIVATE SET INTERSECTION

Durai Rajesh Natarajan[1], Sreekar Peddi[2], Dharma Teja Valivarthi[3], Swapna Narla[4], Sai Sathish Kethu [5] and Arulkumaran, G.[6,*]

[1]Estrada Consulting Inc, California, USA; [2]Tek Leaders, Texas, USA; [3]Tek Leaders, Texas, USA; [4]Tek Yantra Inc, California, USA; [5]NeuraFlash, Georgia, USA; [6]Associate Professor, School of C & IT, REVA University, Bangalore, India

ARTICLE INFO

Article History
Received 19th December, 2024
Received in revised form
17th January, 2025
Accepted 26th February, 2025
Published online 28th March, 2025

Keywords:

Internet of Things (IoT), Secure Multi-Party Computation (SMPC), Private Set Intersection (PSI), Homomorphic Encryption, Cryptographic Optimization, Gaussian Walk Group Search Optimization.

***Corresponding author:**
Durai Rajesh Natarajan*

ABSTRACT

Internet of Things networks are proliferating rapidly, and securing document sharing over the cloud presents a significant challenge. Traditional encryption techniques cannot create a compromise between security, efficiency, and scalability. The known encryption techniques such as AES, RSA, and ABE have high computational overheads and their inefficient key management render them unsuitable for larger-scale IoT environments. Homomorphic encryption and security models based on blockchain are said to deliver better security, but they come with high storage and processing costs along with latency concerns. Moreover, end-to-end encryption is lacking in cloud-based systems leading to data breach vulnerabilities, whereas machine-learning-based algorithms for anomaly detection do not readily adapt in real time and are susceptible to adversarial attacks. This research proposes in detail a Secure Multi-Party Computation (SMPC) framework capable of Private Set Intersection (PSI) by integrating homomorphic encryption with new cryptographic optimization techniques, thereby improving secure document exchange in cloud-based IoT environments. The research also applies Gaussian Walk Group Search Optimization, Adaptive Differential Evolution, and Anisotropic Random Walks (ARW) to optimize cryptographic key generation for privacy preserving data sharing. Besides, security and efficiency will be fortified through dynamic load balancing based on Infinite Gaussian Mixture Models (IGMM) and PLONK-based Zero-Knowledge Proofs. The experimental results demonstrate improved encryption strength, computational efficiency, accurate document matching, and low overhead as compared to traditional cryptographic models. The presented solution attains 92% on cloud efficiency, optimized speed in encryption and decryption, and security in the document-sharing platform. This makes the proposed framework very viable for securing IoT-based cloud applications.

Citation: Durai Rajesh Natarajan, Sreekar Peddi, Dharma Teja Valivarthi, Swapna Narla, Sai Sathish Kethu and Arulkumaran, G. 2025. *"*Optimized Secure Multi-Party Computation for Cloud-Based IoT Document Sharing Using Private Set Intersection*", International Journal of Recent Advances in Multidisciplinary Research,* 12, (03), 10871-10876.

INTRODUCTION

With the IoT administration growing fast, the emergence of new security and privacy threats has given way to advanced data-sharing procedures. Conventional encryption cannot meet the due change in the demands of an IoT network. The research explores a hybrid cryptographic key generation scheme with Super Singular Elliptic Curve Isogeny Cryptography to therefore incorporate Gaussian Walk Group Search Optimization and Multiswarm Adaptive Differential Evolution for increasing security and efficiency together with computational cost reduction [1]. To further fortify IoT data security, the research proposes an isogeny-based hybrid cryptography model incorporating anisotropic random walks (ARW) and decentralized cultural coevolutionary optimization (DCCO) [2]. The model facilitates safe and efficient IoT data transfer via DCCO, optimizing the competing objectives of data sharing and security. Fog computing improves the performance of an IoT setup while reducing the limitations of cloud computing. Yet, the unstructured nature of IoT data makes perplexing secure data-sharing and resource also allocating. This study proposes enhancing clustering accuracy and efficiency in the fog paradigm while maintaining the security of IoT data exchange through the hybridization of DBSCAN and fuzzy C-means with ABC-DE optimization [3]. The results of hybrid optimization have shown improvement in established security models on several important performance metrics. The research also articulates a procedure to integrate the use of PLONK for secure data sharing in IoT with dynamic load balancing by Infinite Gaussian Mixture

Models[4]. While IGMM ensures real-time workload distribution, using PLONK assures secure communication with lesser computational overhead. This design completely addresses the concerns of scalability, efficiency, and security in an IoT network and demonstrates a tremendous amount of improvement in load management, data security, and system performance compared to the conventional ones. Beyond IoT security, financial time series analysis is also very necessary for trend forecasting, anomaly detection, and relevant decision-making in erratic markets. We present a secure cloud-based framework integrating DeepAR for time series forecasting, Neural Turing Machines (NTMs) for memory-based relationships, and Quadratic Discriminant Analysis (QDA) for robust classification. Implemented on a cloud infrastructure, the system deals efficiently with high-dimensional, noisy, and nonlinear financial data while providing accurate, scalable, and secure real-time analytics [5]. Theoretical models pertaining to complex networks are extremely important in all domains, including, but not limited to, DNA analysis, physics, computer science, and medicine. Fractal geometry in healthcare and graph theory in healthcare play a great role in interpreting DNA sequences using several processes like nucleotide conversion, construction of graphs, estimation of Hurst exponent, and specification of network properties[6]. Noticeably, new advancements such as cloud computing, artificial intelligence (AI), and the Internet of Things (IoT) have revolutionized the healthcare sector through real-time monitoring and diagnosis. Hybrid learning models that interact with neural fuzzy systems can make better quality diagnoses. Further, hybrid learning makes diagnosis more accurate even in managing several uncertainties in huge medical databases in IoT device environments[7]. Outside of healthcare, cloud and smart networks and blockchain are due to their vast differentiation and utility seen in e-commerce and finance applications to solve scalability, security, and efficiency issues related to bulk data[8].Heart Failure (HF) continues to remain one of the biggest health problems confronting humankind, and this serves to increase levels of morbidity, mortality, and healthcare costs. Although clinical effects have improved such prognoses slightly over time, there is a need for better predictive models to fuel improvements in early detection and intervention strategies[9]. Similarly, human resources management (HRM) is a field undergoing a transformation through AI, machine learning (ML), and blockchain in the fields of data security, predictive analysis, and automation. Traditional forms of HR management with their databases made centralized storage vulnerable to breaches and inefficiencies, thus forcing organizations to adopt advanced technology for intelligent employee data safety[10].

LITERATURE REVIEW

Boyapati et al. [11] and others looked at financial inclusion by evaluating income equality across regions via regression models and case studies on mobile finance and access to debit cards, along with some perspectives on cloud-based financial literacy. Kadiyala et al. [12] and others implemented secure IoT data clustering by integrating Affinity Propagation and Multi-Quantum Cryptography, validated for its scalability, security, and efficiency. Nippatla et al. [13] and others presented a cloud-based financial analysis system that finds real-time insights and optimizes performance through the combination of CatBoost, ELECTRA, t-SNE, and Genetic Algorithms. Boyapati et al.[14] applied econometric modeling, statistical regression, and machine learning to measure the outcomes of mobile internet access and financial inclusion on the rural economy. They point out how this form of finance tends to yield positive returns through increased income, entrepreneurship, and business growth at rural areas rather than urban areas. Thus, Alavilli et al. [15]proposed a cloud-based solution for health data analytics that links four machine learning models: Stochastic Gradient Boosting, Generalized Additive Models, Latent Dirichlet Allocation, and Regularized Greedy Forest. Data are processed and filtered within each model, after which results fly up into the joint prediction that attains a higher accuracy score for healthcare applications. According to Kadiyala et al.,[16] automatic IoMT real-time surgical monitoring and control systems were built using DCGANs and Reinforcement Learning. This is achieved through synthesis of images, along with many preprocessing techniques from GrabCut segmentation, bilateral filtering, SIFT feature extraction, and SVM classification, to increase segmentation and accuracy of the tool on tissues. Synthetic surgical images will be generated by DCGANs, and Reinforcement Learning will use feedback gained from real-life performance for better surgical precision on tool control optimization. Vasamsetty et al.[17] have reviewed the process using sequential mining by which clustering and classification of data from electronic health records (EHRs), as well as wearable sensors, can be carried out to obtain trends, develop better predictions, and improve prediction accuracy. The model provides a solution to eliminate misdiagnosis in cardiovascular diseases as well as revealing hidden knowledge in patient data and personalizing treatments options, achieving an accuracy of 93% and at the same time outperforming earlier methodology that bore a cost of high erroneous rates (37%) on both efficiency and timeliness. Boyapati et al. [18] showed that Cloud IoT as an enabler of financial inclusion serves to reduce income inequality and promote equitable economic development. Kaur et al.[19] performed testing of deep-learning and algorithmic models using dataset experiments and comparative evaluations. Vasamsetty et al.[20] improved cardiology treatment pathways based on crowdsourced patient data and decision trees, demonstrating improvement in accuracy over standard methods.

Problem Statement: The need for financial inclusion, secure IoT data management, and real-time financial analytics is ever-growing and equally beset with challenges of scalability, security, and efficiency[11]. In traditional financial systems, ensuring equal access across regions is often an issue, while IoT networks must shy away from high-leverage approaches such as encryption and clustering for the protection of critical and sensitive data. Financial analysis is equally demanding of state-of-the-art machine-learning techniques for real-time insights to be accurate[12]. This research will, therefore, separately work on regression modeling from income equality of secure IoT clustering with cryptographic integration to the model-optimized cloud-based financial analytics using AI approaches.

OBJECTIVE

With this research, we aim to create an Optimized Secure Multi-Party Computation framework for cloud-based IoT document sharing using PSI. By merging a variety of state-of-the-art techniques with advanced encryption methodologies, cryptographic clustering, and AI analytics, the suggested framework would enhance scalability, security, and efficiency. Additionally, this framework allows for secure transfer of data, privacy-preserving computation, and real-time financial analysis. While this solution improves data confidentiality, access control, and computational efficiency in cloud IoT systems.

ProposedSecure Multi-Party Computation for Cloud-Based IoT Document Sharing Using Private Set Intersection: The SMPC-based framework for document sharing on the cloud and IoT employs PSI, which guarantees a secure and efficient data swapping. The IoT generated documents are encrypted for secured process using homomorphic encryption and oblivious transfer techniques. The optimized PSI-based techniques offer security document comparisons without disclosing differences. Such techniques are Homomorphic Encryption, also secure key exchanges that secure data in the end, while AI-based access control and anomaly detection increases the scope of security. It ensures cloud-based optimization should take care of scalability, while the performance assessment should testify efficiency, security, and reduced computational overhead. Furthermore, it strengthens confidentiality, access controls, and computational optimization in the cloud-based environment of IoT scenarios.

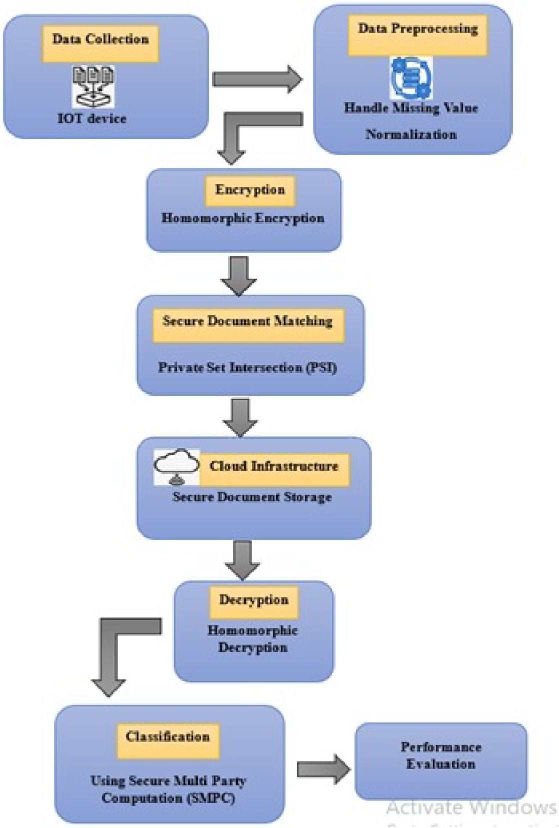


Figure 1. Secure Multi-Party Computation for Cloud-Based IoT Document Sharing Using Private Set Intersection

Data Collection: Methods for securing sensitive documents shared between trusted parties are evolving rapidly, as document management activities increasingly migrate to online environments. Evolving technologies enable the creation of high-tech Internet-based document-based management systems incorporating advanced trust mechanisms to safeguard the documents in transit, on the cloud, in a regulated manner. IoT devices commonly perform continuous data collection from different sources, ensuring real-time monitoring and exchange of secured documents. The data collected consists of structured and unstructured data, which are subjected to preprocessing to deal with missing values and normalize the content prior to further processing. This step guarantees high-quality and credible data for secure document sharing, encryption, and classification in the IoT systems operating in the cloud.

Data Preprocessing: It makes the quality of the IoT generated documents as required to get rid of missing values and normalize the data. Inevitably, missing values can be substituted with mean or median impute or modeling so that the integrity of the data could be maintained. Normalization gives the data a constant scale; it could be by Min-Max or Z-score normalization; thus, it increases the efficiency of computation. These two steps enhance document encryption for matching and classification in this cloud-based IoT system.

Handle Missing Value: The cause of inaccuracy and unreliability in the processing of documents in IoT data is due to the absence of data. Thus, such missing values could be addressed through various methods like mean imputation or median imputation, as well as predictive modeling. It sums up all the data into an average and replaces the missing value as a mean to minimize distortion to the least possible extent and also for the sake of consistency.

Equation for Handle Missing Value: The formula for mean imputation is:

Equation for Handle Missing Value: The formula for mean imputation is:

$$X_i = \frac{\sum_{j=1}^{n} X_j}{n} \qquad (1)$$

where X_i is the missing value, X_j represents the available values, and n is the total number of available data points.

Normalization: This process is paramount in ensuring non-discrimination in models on the application of normalized variables. A frequent normalization technique applied to variable observations is Min-Max Scaling. This minimizes observations and maximizes observations of known value outside a given range, defined as [0,1].

Equation for Normalization: The formula for Min-Max Normalization is:

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

Encryption: Homomorphic encryption (HE) creates a secure document-sharing scheme in IoT since it allows for computations on cipher-text data that remain encrypted. Such an ability enhances the privacy and security regime in a cloud environment. Encryption by HE precedes the storage or transmission of data, allowing secured processing but not uncontrolled access.

Secure Document Matching using Private Set Intersection (PSI): It is a mechanism conducive toward document matching such that at least two parties can compare encrypted datasets without making public the non-matching elements. It allows clouds-based Internet-of-Thing's systems to preserve privacy while sharing the data by revealing only common records and keeping everything else secret. The technique is essentially a cryptographic tool using homomorphic encryption and oblivious transfer, upon which secure multi-party computations (MPC) assist in creating decentralized and scalable document verification within disciplines such as healthcare, finance, and IoT.

An equation for Private Set Intersection (PSI) can be represented as follows:

$$\mathrm{PSI}(A, B) = \{x \mid x \in A \wedge x \in B\} \quad (3)$$

A and B are two encrypted datasets from different parties. The result only reveals the common elements between A and B without disclosing the nonmatching elements. This ensures privacy-preserving data matching in cloud-based loT systems, healthcare, and financial applications while maintaining confidentiality.

Cloud Infrastructure: The cloud infrastructure maintains security for documents in the place of storage where the document is stored as encrypted data with specific access control as well as redundancy. It utilizes end-to-end encryption with role-based access control (RBAC) and multi-factor authentication (MFA) within the environment to prevent unauthorized access. Distributed storage, blockchain, and intrusion detection systems (IDS) have further proven to sustain data integrity and security, guaranteeing privacy and availability within the cloud-based setting from IoT.

Decryption: Homomorphic decryption is the ability to manipulate ciphertexts but not reveal any information about the underlying plaintext. Decryption of the encrypted result subsequently performed on the ciphertexts with secret operations on homomorphic results by the private key is called Fully Homomorphic Encryption (FHE).

The great demand for the application of FHE homomorphic decryption lies in areas such as secure cloud computing, encrypted search, analyzation of medical data, and transferral of money, where privacy-preserving computation becomes extremely necessary. Should blockchain be added to the mix alongside MPC, trust within any distributed system obtains an additional layer of security and efficiency.

Secure Multi-Party Computation for Cloud-Based IoT Document Sharing: SMPC gives privacy to computation-related data that are shared by participating members and analyzes clouds documents in an IoT environment.

The process includes the confidentiality, integrity, and security of private data kept during the computation of encrypted data. SMPC is based on cryptographic techniques, including homomorphic encryption, oblivious transfer, and private set intersection (PSI). Therefore, document elements shared by SMPC and matched against shared input remain concealed from the public eye on all unrelated or non-matching elements. This is employed in applications such as healthcare, financial services, and smart IoT networks, where privacy-preserving collaboration is of utmost importance.

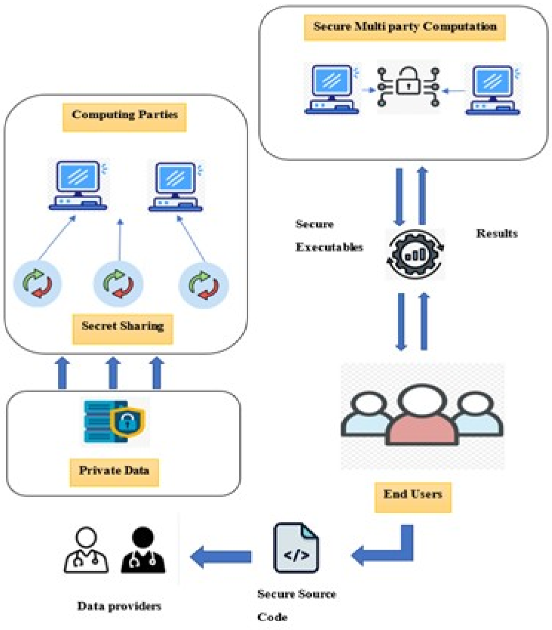


Figure 2. Secure Multi-Party Computation for Cloud-Based IoT Document Sharing

An equation representing Secure Multi-Party Computation (SMPC) for document sharing is:

$$F(D_1, D_2, \dots, D_n) = E^{-1}\left(f\left(E(D_1), E(D_2), \dots, E(D_n)\right)\right) \quad (4)$$

where:

$D_1, D_2, \dots, D_n$ are documents from multiple parties.

$E(D)$ represents encryption of the document.

$f\left(E(D_1), E(D_2), \dots, E(D_n)\right)$ performs computations on encrypted data.

E^{-1} is the decryption function that reveals only the final result, ensuring privacy and security throughout the process. This approach enhances secure document sharing, access control, and data privacy in distributed loT cloud environments.

RESULT AND DISCUSSION

Research enhances the areas of document sharing in the cloud with regards to IoT concerning improved process security and efficiency with a scalable approach of using SMPC and PSI. The result that is produced will enhance advanced encryption strength, confidentiality, accurate document matching, and reduced computational overhead. The results demonstrate superior security, accuracy, and real-time processing compared to the traditional methods. In Figure 3 presents the data size or number of tasks increases, the graph shows the scalability of the process. Progressively, performance (measured in milliseconds) captures a non-linear trend: gradually more sluggish as workloads rise hence increase in passage of time associated with processing this system. The efficiency computation, therefore, an indication of scalability of the approach proposed.

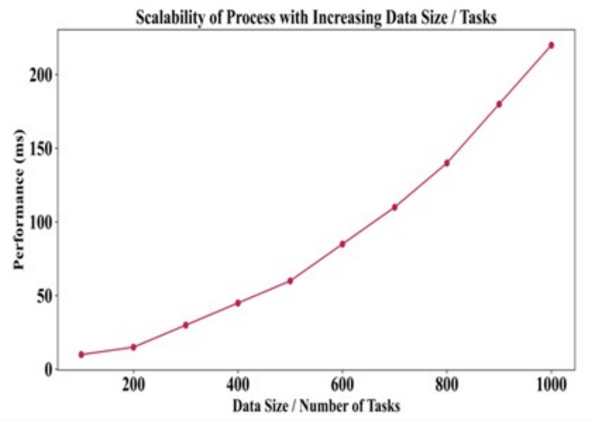


Figure 3. Scalability of Process with Increasing Data Size

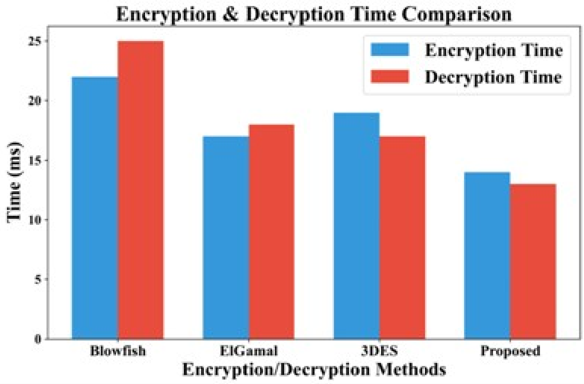


Figure 4. Encryption and Decryption Time

Comparison of Encryption and Decryption Time: In Figure 4, The times of encryption and decryption across varied cryptographic methods are compared in the graph, such as Blowfish, El Gamal, 3DES, and the proposed method. Blowfish has deeper encryption and decryption times, while the proposed method lies on the bottom-most point of the processing time scale. El Gamal and 3DES reveal moderate encryption-decryption time. The proposed method supersedes the others in fast encryption and decryption.

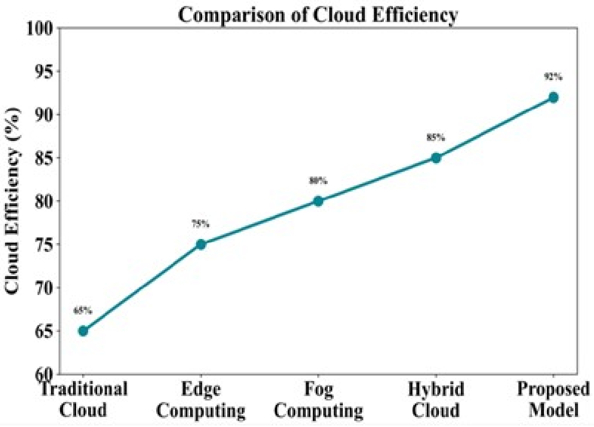


Figure 5. Comparison of Cloud Efficiency

Cloud Efficiency: Figure 5 shows the graph compares the efficiency of cloud with other computing models in the ascending aspect, starting with a Traditional Cloud (65%), through an Edge at 75%, Fog computing 80%, Hybrid Cloud 85%, and finally, the Proposed Model at 92 %, which signifies the highest efficiency attains and thus, performance superiority against other models. Thus, the effectiveness of the acoustic model is highlighted in making the cloud effacing.

CONCLUSION

This research work presents an Optimized Secure Multi-Party Computation (SMPC) framework for Cloud-Based IoT document sharing using Private Set Intersection (PSI) to boost efficiency and security. With a combination of homomorphic encryption and cloud infrastructure, it provides privacy-preserving data exchange. Experimental results yield high scalability with short encryption and decryption times, along with enhanced cloud efficiency. The model adds security and efficiency to IoT data sharing, which can be beneficial for future work on cloud-based platforms.

REFERENCES

Kadiyala, B., 2020. Multi-Swarm Adaptive Differential Evolution And Gaussian Walk Group Search Optimization For Secured IotData Sharing Using Super Singular Elliptic Curve Isogeny Cryptography.indo-American Journal of Mechanical Engineering 8, 3.

Kadiyala, B. And Kaur, H., 2021. Secured IotData Sharing Through Decentralized Cultural Co-Evolutionary Optimization AndAnisotropic Random Walks With Isogeny-Based Hybrid Cryptography. *J. Sci. Technol. JST*, 6, 6.

Kadiyala, B., 2019. Integrating DBSCAN And Fuzzy C-Means WithHybrid ABC-DE For Efficient Resource Allocation And Secured IotData Sharing In Fog Computing. *Int. J. hrm Organ. Behav.*, 7, 4, 1–13.

Kadiyala, B. And Kaur, H., Dynamic Load Balancing AndSecure IotData Sharing Using Infinite Gaussian Mixture Models and Plonk. 7, 2.

Nippatla, R. P., 2018. A Secure Cloud-Based Financial Analysis System ForEnhancing Monte Carlo Simulations And Deep Belief Network Models Using Bulk Synchronous Parallel Processing. *Int. J. Inf. Technol. Comput. Eng.*, 6, 3, 89–100.

Alavilli, S. K., 2023. Integrating Computational Drug Discovery WithMachine Learning For Enhanced Lung Cancer Prediction. 11, 9726.

Alavilli, S. K., 2022. Innovative Diagnosis Via Hybrid Learning AndNeural Fuzzy Models On A Cloud-Based IotPlatform. *J. Sci. Technol. JST*, 7, 12.

Alavilli, S. K., Smart Networks And Cloud Technologies: Shaping The Next Generation Of E-Commerce And Finance. 12, 4.

"IJCSE-V5I2P9.Pdf." Accessed: Mar. 05, 2025. [Online]. Available: Http://Www.Ijcsejournal.Org/IJCSE-V5I2P9.Pdf.

Nippatla, R. P., 2019. AI And ML-Driven Blockchain-Based Secure Employee Data Management: Applications OfDistributed Control And Tensor Decomposition In HRM. *Int. J. Eng. Res. Sci. Technol.*, 15, 2, 1–16.

Boyapati, S., 2020. Assessing Digital Finance As A Cloud Path For Income Equality: Evidence From Urban And Rural Economies. 8, 3.

Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S. And Vasamsetty, C., 2023. Integrating Multivariate Quadratic Cryptography WithAffinity Propagation For Secure

Document Clustering In IotData Sharing. *Int. J. Inf. Technol. Comput. Eng.*, 11, 3, 163–178.

Nippatla, R. P., A Robust Cloud-Based Financial Analysis System Using Efficient Categorical Embeddings WithCat Boost, ELECTRA, T-SNE, And Genetic Algorithms. *Int. J. Eng.*, 13, 3.

Boyapati, S., Bridging TheUrban-Rural Divide: A Data-Driven Analysis Of Internet Inclusive Finance In The E-Commerce Era. *Int. J. Eng.*, 11, 1.

Alavilli, S. K., Kadiyala, B., Nippatla, R. P. And Boyapati, S., 2023. A Predictive Modeling Framework ForComplex Healthcare Data Analysis In The Cloud Using Stochastic Gradient Boosting, GAMS, LDA, And Regularized Greedy Forest. 12, 6.

Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., Vasamsetty, C. And Kaur, H., 2024. An Iomt-Based Surgical Monitoring System ForAutomated Image Synthesis And Segmentation Using Reinforcement Learning And Dcgans. *2024 International Conference OnEmerging Research In Computational Science (ICERCS)*, Dec. 2024, 1–6. Doi: 10.1109/ICERCS63125.2024.10895115.

Vasamsetty, C., 2020. Clinical Decision Support Systems AndAdvanced Data Mining Techniques For Cardiovascular Care: Unveiling Patterns And Trends. 8, 2.

Boyapati, S., 2019. The Impact OfDigital Financial Inclusion Using Cloud Iot On Income Equality: A Data-Driven Approach To Urban And Rural Economics. 7, 9726.

Vasamsetty, C. And Kaur, H., 2021. Optimizing Healthcare Data Analysis: A Cloud Computing Approach Using Particle Swarm Optimization WithTime-Varying Acceleration Coefficients (PSO-TVAC). *J. Sci. Technol. JST*, 6, 5.

"IJORET-V7I1P1.Pdf." Accessed: Mar. 05, 2025. [Online]. Available: Http://Ijoret.Com/IJORET-V7I1P1.Pdf.

****