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

An Advanced Financial Cloud Security System with AI-based Data Fragmentation and Replication

Dr. Atmaram F. Shelke[1*], Sujit Dhanuka[2], K. Soumya[3], Dr. Arvind Kumar Pandey[4], Shikhar Gupta[5] and Nipun Setia[6]

[1*]Associate Professor, Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR); Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University), India. ashelke@symlaw.ac.in, https://orcid.org/0000-0001-9558-8991

[2]Assistant Professor, Department of uGDX, ATLAS SkillTech University, Mumbai, Maharashtra, India. sujit.dhanuka@atlasuniversity.edu.in, https://orcid.org/0009-0005-5001-7470

[3]Assistant Professor, Department of Computer Science and Information Technology, Jain (Deemed to be University), Bangalore, Karnataka, India. soumya.k@jainuniversity.ac.in, https://orcid.org/0000-0002-6657-386X

[4]Associate Professor, Department of Computer Science & IT, ARKA Jain University, Jamshedpur, Jharkhand, India. dr.arvind@arkajainuniversity.ac.in, https://orcid.org/0000-0001-5294-0190

[5]Chitkara Centre for Research and Development, Chitkara University, Himachal Pradesh, India. shikhar.gupta.orp@chitkara.edu.in, https://orcid.org/0009-0004-0138-3987

[6]Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. nipun.setia.orp@chitkara.edu.in, https://orcid.org/0009-0005-8635-6802

Received: May 03, 2025; Revised: June 19, 2025; Accepted: July 30, 2025; Published: August 30, 2025

Abstract

Data fragmentation operates to build pieces based on the available virtual machines (Vm) of financial cloud security. The replication process tends to enhance the security of data from one network to another network with fewer replications. An advanced financial cloud security system that utilizes AI to divide and copy data improves incursion security by distributing information over several locations and employing complex algorithms to handle and preserve data distribution. The disadvantage of this strategy is an overreliance on AI, which can result in flaws, raising the danger of data breaches and undermining system security and integrity. To overcome this issue, this study proposes an improved butterfly optimized finite elliptic curve cryptography (IBO-FECC) for autonomous technique and advanced encryption method that safeguard valuable financial information across cloud settings which strengthens data security and privacy. The system architecture employs networks to conduct cloud-based tests with successful results. The system efficiency is determined using task frequency and Vm capability. The findings are evaluated according to the unit count and virtual machine configurations, response time and throughput fluctuate with data size, but Vm=15 consistently outperformed Vm=5. Memory utilization is developed as the data becomes more complicated. Data fragmentation increases the speed of

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 3 (August), pp. 318-328. DOI: *10.58346/JISIS.2025.I3.022*

*Corresponding author: Associate Professor, Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR); Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University), India.

processing at a higher velocity. The study concluded that the suggested IBO-FECC identifies the optimal network pathway in financial cloud safety systems regarding system resiliency and security.

Keywords: Data Fragmentation and Replication, Financial Cloud Security System, Virtual Machines (Vm) and Improved Butterfly Optimized Finite Elliptic Curve Cryptography (IBO-FECC).

1 Introduction

In financial system, a safe cloud policies, rules and tools secure the financial systems (Ziwei & Han, 2023), apps and data that are kept in cloud environments. To protect from security threats, the banking sector should ensure the safety, integrity and availability of financial information, which consists of mechanisms for compliance, assessment, access controls and encryption (Gill et al., 2022). Particularly financial organizations confront specific difficulties because of the significant risk and continuous danger of cybercrime (Sagar & Sahgal, 2024). The creative approach essentially protects financial data from theft, hacking and unauthorized access by integrating the power of cloud computing (CC) with advanced safety precautions (Thabit et al., 2023). The fundamental principles of the system are data replication and fragmentation, to provide resilience and safety (Karimov & Bobur, 2024). Attackers are unable to realistically reconstruct the full fragments despite gaining entry to all of the components when sensitive data is divided into smaller bits or pieces (Ilapakurthy, 2023). Fragmentation is a procedure that uses advanced encryption techniques and algorithms to ensure that every fragment remains secure, even if a tiny percentage of them are displayed. Moreover, the data replication function copies and keeps these damaged pieces on many secure servers or locations (Amponsah et al., 2022). In addition to improve data accessibility and availability, redundancy offers an extra line of protection against data loss due to hardware failures or cyber-attacks (Papadopoulos & Christodoulou, 2024). The system can modify the quantity of fragmentation and replication in real-time threat evaluations and data consumption patterns (Soundappan & Shenoy, 2023). By providing maximum security without sacrificing scalability or speed, the dynamic strategy enables financial institutions to effectively respond to change cyber security threats. As a cost-effective and compliant solution that integrates seamlessly with existing cloud-based structures and security frameworks, financial organizations of all sizes stand to gain from the financial cloud safety system based on data fragmentation and replication (Peng et al., 2023). A financial cloud security system with data fragmentation and replication has certain drawbacks, including greater complexity that can provide management issues. Furthermore, replication leads to increased storage costs and synchronization challenges, while fragmentation can present problems with data consistency (Ricard et al., 2023). The objective of the study is to identify the best path in financial cloud safety systems (Subramanian & Malhotra, 2023) using IBO-FECC method that create a secure and dependable cloud-based system to improve the safety and resilience of processing and storing financial data in the cloud environment.

2 Related Works

Mohammed et al., 2023 proposed the cloud-based data security systems (Nair & Rao, 2023) (C-DSS) for cloud-edge data-sharing designs. Prior to providing Cyber Threat Information (CTI) for analytical techniques, the information administrators have elected a suitable assurance level and sanitization technique. Balashunmugaraja & Ganeshbabu, (2020) focused that dynamic data reserved on cloud stages by businesses worldwide, cloud security was seen to be of utmost importance in the funding sector. The crossover improved-lion algorithm (CI-LA), a novel meta-heuristic system inspired by the diverse social behavior of lions, should be used to deliver a key for the sanitization process. The original information

should be effectively restored using the same key during the restoration process. (Hazeem & AlBurshaid, 2024) discussed the problems and effects of fragmented data on transactions in the industry of real estate. The term data fragmentation explained that data was distributed and uneven throughout a financial, making it greater to reach assessments and conduct activities. To create general data frameworks and sources, the industry was seeing tendencies towards data centralization and standardization. (Castro-Medina et al., 2019) provided a strategy called fragmentation-redundancy-scattering (FRS) to tolerate errors that were either deliberate or unintentional. To dispense robust and reliable cloud storage, the FRS approach was implemented as a breach-resistant solution. Furthermore, to study how the notion got implemented in different circumstances, a cloud computing security (CCS) relying on the FRS approach was presented. (Periyanatchi & Chitra, 2020) provided the highest possible speediness and safety while considering both performance and safety concerns, as they provide the lion optimization algorithm (LOA), which optimized significance measurement fragmentation and cloud data imitation. The origination of the optimization technique was mainly driven by the unique existence of lions and their supportive behaviors. (Bella & Vasundra, 2022) recommended a detailed examination of the risks regarding security connected to specific CC features. Furthermore, the study puts out an advanced classification system for safety measures. The paper addressed the novel safety concerns that cloud service providers, data owners and cloud consumers must be concerned resultant. Due to these ever-increasing requirements, CC has attracted a lot of focus during the past few years. There were several cost benefits in employing cloud storage alternatives. (De Donno et al., 2019) the safety of cloud computing and the Internet of Things (IoT) were normally addressed individually in the literature, however, this page provided a current, structured list of security risks relating to both. They deliver a presentation of the potential influence and locations of security flaws. While cloud-based cyber disasters were the origin of cyber-attacks, they claim that safeguarding IoT devices was inadequate. Noraziah et al., (2021) proposed the binary vote assignments on grid quorum through association rules (BVAGQ-AR) method for managing the synchronous replication of fragmented databases. The database was split into disjoint segments was possible with the BVAGQ-AR technique (Veerappan, 2023). Fragmentation improved effectiveness, reliability and use in large databases. Based on the trial findings, the proposed BVAGQ-AR approach handles fragmented databases while maintaining data integrity in context.

3 Methodology

The present research built a model to select an advanced financial cloud security system based on AI-driven data Fragmentation and replication under very nonlinear constraints by making use of the features of IBO-FECC technique.

3.1. Improved Butterfly Optimized Finite Elliptic Curve Cryptography (IBO-FECC)

The IBO-FECC is a technology that enhances data privacy and protection through the application of decentralized algorithms and advanced encryption techniques to safeguard sensitive financial information in the cloud environments. The IBO-FECC secures the confidentiality and integrity of information while becoming protected to cyber attacks and unauthorized access, which develops the confidence and reliability in financial transactions and operations. IBO-FECC is divided into two, IBO is utilized to detect the optimal node in financial cloud security and FECC improved the data privacy.

3.1.1. Finite Elliptic Curve Cryptography (FECC)

Enhancing financial cloud safety requires the use of Finite Elliptic Curve Cryptography (FECC), which uses advanced methods on finite fields to provide secure key exchange, encryption and authentication

mechanisms. This ensures data integrity and discretion in financial communication conducted over cloud-based platforms. FECC uses public and private keys that are acquired by both parties which are used for encoding and decoding, much as public key encryption. The modulus of the integers employed in the huge prime number p is denoted by Fp. The elliptic E curve forms on Fp when one appears at the data using the equation (1).

$$z^2 = w^3 + bw + a \quad (1)$$

The definition of a and b in this formula are the integers employed by the factor Fp under the following condition: in an approach that $4b^3 + 27a^2 \neq 0\ (mod\ q)$ a location on the curve is represented by the pair (w, z). For all points on E, the set is represented by the E. Let E an elliptic curve, have the following identifying condition applied to equation (2).

$$z^2 = w^3 - 5w + 2 \quad (2)$$

3.1.2. Improved Butterfly Optimization (IBO)

The IBO is integrated with finite elliptic curve cryptography to improve cybersecurity measures by using decentralized algorithms for strong protection, guaranteeing data availability, confidentiality and integrity in financial conditions. Advanced techniques such as fragmentation of data and replication are also incorporated. Butterflies can detect and smell the scent of food and flowers because they have chemo-sensors strewn throughout their bodies. According to IBO, butterflies' production potential is deemed to be average. Next, this fragrance has a connection to the quality of the IBO-seeking agents. As the fragrance for one species of butterfly travels a great distance to be noticed by other species in the area, it forms a group of social information systems. An appealing insect inside its search region is detected by an IBO in financial cloud. When a butterfly's aroma is noticed by other nodes as it can travel a considerable distance to draw their attention and create a network of mutually beneficial relationships. J Formulation and e Variation are the two basic questions that explain the cloud-based butterfly occurrence in nature. For the purpose of simplicity, J in IBO is associated with the function of objectiveness. However, since e is dependent, it has to be sensed by other butterflies. The physical intensity of stimulation in IBO influences the scent in the following ways in equation (3):

$$e_j = d \times J^b \quad (3)$$

Here J is the strength of the stimulus, d is the modality of the sense which is the modality-dependent power exponential and e_j is the detectable intensity of the scent. The two primary phases of IBO are the local utilization stage and the worldwide exploration stage. Equation (4) and (5) describe the global and local stages, respectively.

$$W_j^{s+1} = W_j^s + (q^2 \times h^* - W_j^s) \times e_j \quad (4)$$

$$W_j^{s+1} = W_j^s + (q^2 \times W_i^s - W_l^s) \times e_j \quad (5)$$

The best response in the present iteration is indicated by h^*. e_jIs the scent of jth butterfly and q is a random number in the interval $[0, 1]$. The i^{th} and l^{th} butterflies are represented in the resultant space by $W_j^s$and W_l^s, respectively. Global and local stages are involved in butterfly pursues in IBO. Thus, the exploration and exploitation of the algorithm in IBO is controlled by a probability p, also called the switching probability. The IBO can also be employed to optimize security arrangements and policies according to risk evaluations and legal requirements. It can assess trade-offs and goals set by financial organizations to determine the optimum compromise among safety precautions, accessibility and efficiency in operation.

3.2. Data Fragmentation

Data fragmentation, which separates private data into smaller components, is a technique used by financial cloud security to make it harder for unauthorized access or intrusions. This approach lowers the possibility of a single point of failure, improves overall defense against cyber-attacks in financial systems and strengthens data security by distributing pieces among several locations or servers. The owner of the data expressed security issues while turning over ownership of the financial data to a third party. To assure security, fragmentation is used in the financial suggested approach to address this problem. The number of virtual machines is first counted during execution, data chunks are created by fragmenting the machine. Figure. 1 shows the flow chart of the suggested method.

The following scenario assesses the probability of a successful assault on this framework inevitably are examining a cloud node that has M integers and q fragments of data files. Let m be the total number of successful incursions on different nodes of networks in the cloud, where $t > y$. The following represents the probability $(Q(t, y))$ which $t$denotes the number of victim nodes including all of the y sites containing the file fragments using the equation (6):

$$E(b, o) = \frac{\binom{b}{o}\binom{M-b}{t-o}}{\binom{M}{t}} \quad (6)$$

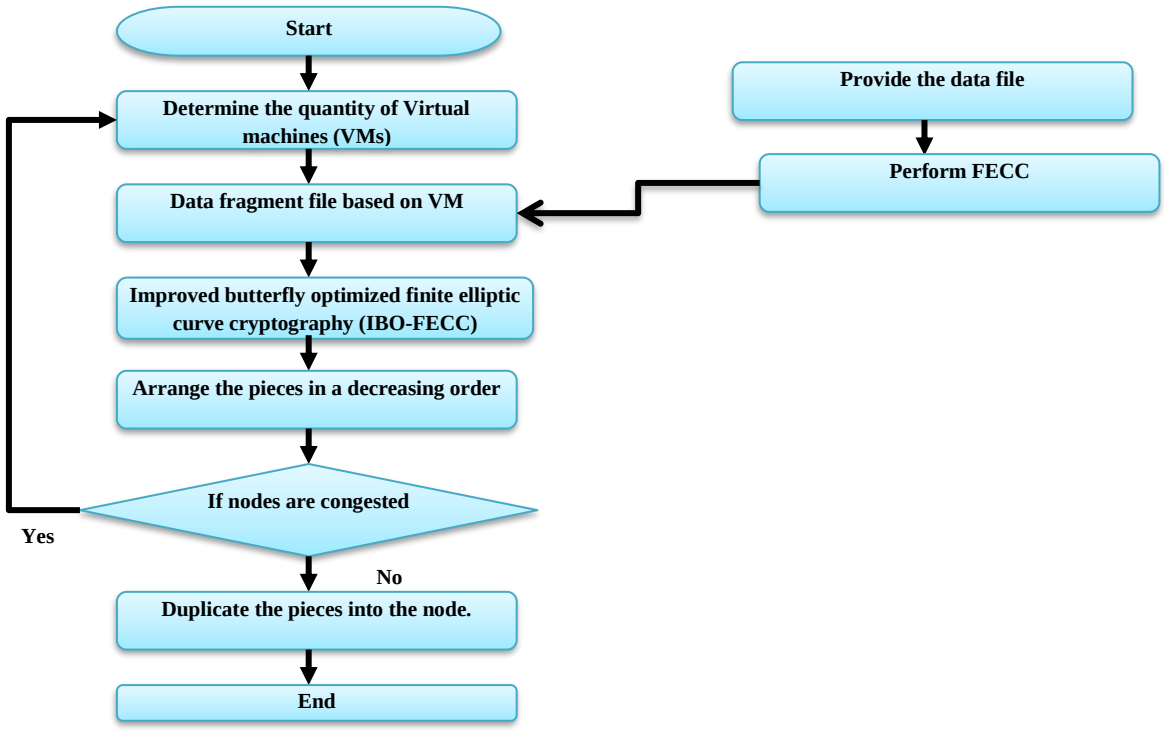

Figure 1: Flow Chart of Suggested Method

4 Results

Fig.2 shows the outcome of response time which makes it evident that the suggested procedures produce an effective result. Response times for several scenarios involving various virtual machine (Vm) setups are displayed in milliseconds (ms). The reaction times for 25 units extend from 102 ms to 306 ms forVm=5. For 25 units, the reaction times range from 130 ms to 360 ms for Vm=15. There appears to

be a relationship between the Vm setup, the number of units handled and the reaction time that result, which might point to areas for improvement or constraints in performance. Table 1 shows the numerical result of response time.

Table 1: Numerical Result of Response Time

Response Time	Time (ms)	
	Vm=5	Vm=15
25	102	130
50	154	155
100	208	220
150	250	264
250	306	360

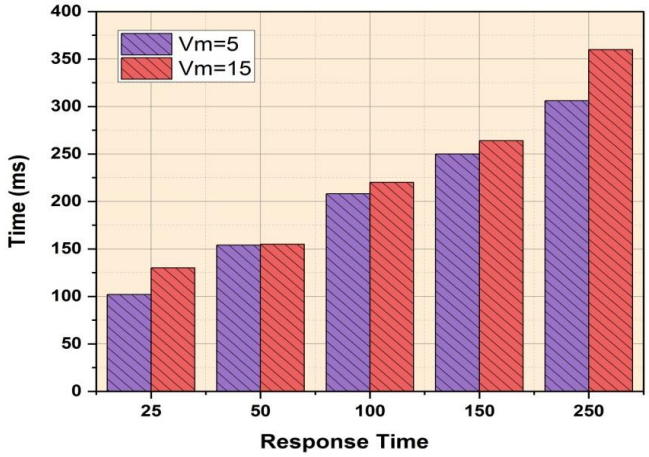

Figure 2: Outcome of Response Time

Figure 3 shows the outcome of throughput, the information previously mentioned demonstrates that suggested methods have a beneficial outcome. For both Vm settings, throughput often drops as the data size rises from 25 to 250. For all data sizes, Vm=15 continuously outperforms than Vm=5 in terms of throughput, suggesting that the Vm=15 configuration handles data more effectively in the allotted time frames. Table 2 shows the numerical outcome of throughput.

Table 2: Numerical Outcome of Throughput

Throughput	Time (ms)	
	Vm=5	Vm=15
25	1.5	3
50	2.8	3.2
100	3	3.5
150	4	4.5
250	5	5.6

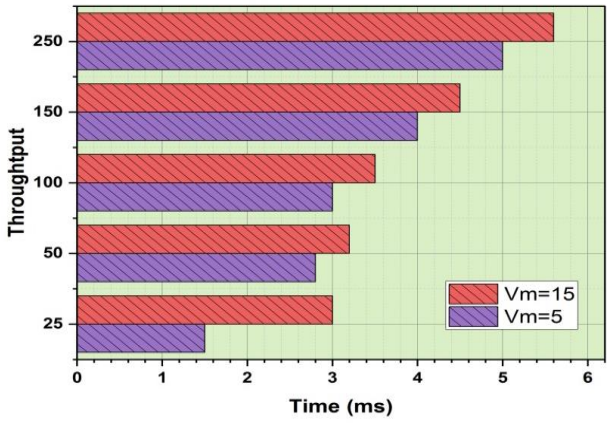

Figure 3: Outcome of Throughput

Figure 4 shows the outcome of memory utilized; the information mentioned above clearly demonstrates that the suggested methods provide a beneficial result. These measurements of time and memory utilization (Vm=5, Vm=15) for various data sizes. For example, memory utilization hits 39 (Vm=5) and 40 (Vm=15) with a data size of 250. This illustrates that the intricacy of the information increases the computation time and memory use. Table 3 shows the numerical result of memory utilization.

Table 3: Numerical Result of Memory Utilization

Memory Utilization	**Time (ms)**	
	Vm=5	**Vm=15**
25	25.8	27
50	30	32
100	32	35
150	38	39
250	39	40

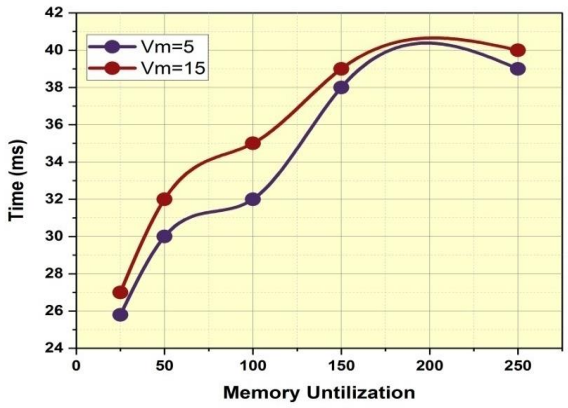

Figure 4: Outcome of Memory Utilized

Figure 5 shown the outcome of the data fragmentation. The data exposed above adequately confirms that the indicated techniques produce positive outcomes. The fragmentation affects time for two separate velocities of movement values, Vm=5 and Vm=15. Both Vm values show an increase in time as the fragmentation degree increases. But, Vm=15 as opposed to Vm=5 as it increases to over time and

becomes more significant. This suggests that larger fragmentation levels, especially when traveling at higher speeds, have a significant influence on longer timeframes. Table 4 shows the numerical outcome of data fragmentation.

Table 4: Numerical Outcome of Data Fragmentation

Fragmentation	Time (ms)	
	Vm=5	Vm=15
25	70	74
50	95	86
100	130	120
150	182	174
250	230	210

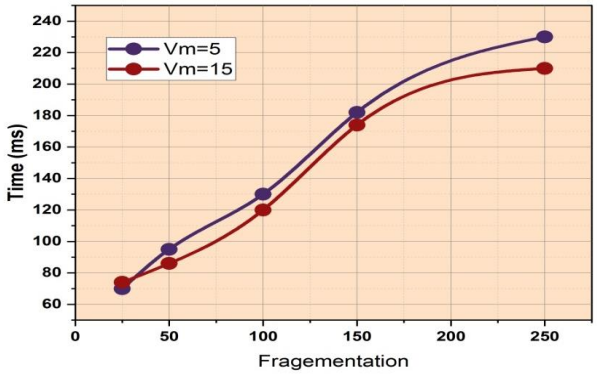

Figure 5: Outcome of Data Fragmentation

5 Conclusion

This study evaluated the tests to develop a powerful financial cloud safety system that employed data fragmentation and replication approaches to increase data security and resilience. This research revealed that the proposed IBO-FECC finds the ideal network path and financial cloud safety solution, with significant outcomes regarding both resiliency and security. The result indicates a significant finding across some metrics like response time, throughput, etc. For response time, with 25 units, times range from 102 ms to 306 ms (Vm=5) and 130 ms to 360 ms (Vm=15). Throughput decreases as data size increases, favoring Vm=15 over Vm=5 consistently. Memory usage rises with data size, reaching 39 (Vm=5) and 40 (Vm=15) at a data size of 250. Fragmentation increases the processing time, notably more pronounced for Vm=15 compared to Vm=5. This study emphasized the usefulness of combining sophisticated cryptography technologies and data management strategies to strengthen cloud-based financial systems, resulting in a more secure and reliable financial network. Future research may focus on fine-tuning the system design to address performance restrictions and improve its appropriateness for protecting financial information in the cloud.

References

[1] Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). Improving the financial security of national health insurance using cloud-based blockchain technology application. *International Journal of Information Management Data Insights*, *2*(1), 100081. https://doi.org/10.1016/j.jjimei.2022.100081

[2] Balashunmugaraja, B., & Ganeshbabu, T. R. (2020). Optimal key generation for data sanitization and restoration of cloud data: Future of financial cyber security. *International Journal of Information Technology & Decision Making*, *19*(04), 987-1013. https://doi.org/10.1142/S0219622020500200

[3] Bella, H. K., & Vasundra, S. (2022, January). A study of security threats and attacks in cloud computing. In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 658-666). IEEE. https://doi.org/10.1109/ICSSIT53264.2022.9716317

[4] Castro-Medina, F., Rodríguez-Mazahua, L., López-Chau, A., Machorro-Cano, I., & Abud-Figueroa, M. A. (2019, August). Design of a horizontal data fragmentation, allocation and replication method in the cloud. In *2019 IEEE 15th International Conference on Automation Science and Engineering (CASE)* (pp. 614-621). IEEE. https://doi.org/10.1109/COASE.2019.8842934

[5] De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., & Mazzara, M. (2019). Cyber-storms come from clouds: Security of cloud computing in the IoT era. *Future Internet*, *11*(6), 127. https://doi.org/10.3390/fi11060127

[6] Gill, S. H., Razzaq, M. A., Ahmad, M., Almansour, F. M., Haq, I. U., Jhanjhi, N. Z., ... & Masud, M. (2022). Security and privacy aspects of cloud computing: a smart campus case study. *Intelligent Automation & Soft Computing*, *31*(1), 117-128. https://doi.org/10.32604/iasc.2022.016597

[7] Hazeem, H., & AlBurshaid, E. (2024). Fragmented Data Landscape and Data Asymmetries in the Real Estate Industry. In *Blockchain in Real Estate: Theoretical Advances and New Empirical Applications* (pp. 179-205). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-8533-3_10

[8] Ilapakurthy, S. V. (2023, October). Bolstering the Mobile Cloud: Addressing Emerging Threats and Strengthening Multi-Layered Defenses for Robust Mobile Security. In *2023 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (pp. 1-7). IEEE. https://doi.org/10.1109/IOTSMS59855.2023.10325824

[9] Karimov, Z., & Bobur, R. (2024). Development of a food safety monitoring system using IoT sensors and data analytics. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(1), 19-29.

[10] Mohammed, S., Nanthini, S., Krishna, N. B., Srinivas, I. V., Rajagopal, M., & Kumar, M. A. (2023). A new lightweight data security system for data security in the cloud computing. *Measurement: Sensors*, *29*, 100856. https://doi.org/10.1016/j.measen.2023.100856

[11] Nair, M., & Rao, A. (2023). Blockchain for Terminology Traceability in Decentralized Health Systems. *Global Journal of Medical Terminology Research and Informatics*, *1*(1), 9-11.

[12] Noraziah, A., Fauzi, A. A. C., Ubaidillah, S. H. S. A., Alkazemi, B., & Odili, J. B. (2021). BVAGQ-AR for fragmented database replication management. *IEEE Access*, *9*, 56168-56177. https://doi.org/10.1109/ACCESS.2021.3065944

[13] Papadopoulos, G., & Christodoulou, M. (2024). Design and Development of Data Driven Intelligent Predictive Maintenance for Predictive Maintenance. *Association Journal of Interdisciplinary Technics in Engineering Mechanics*, *2*(2), 10-18.

[14] Peng, T., Liao, C., Ye, X., Chen, Z., Li, X., Lan, Y., ... & An, G. (2023). Machine learning-based clustering to identify the combined effect of the DNA fragmentation index and conventional semen parameters on in vitro fertilization outcomes. *Reproductive Biology and Endocrinology*, *21*(1), 26. https://doi.org/10.1186/s12958-023-01080-y

[15] Periyanatchi, S., & Chitra, K. (2020). A lion optimization algorithm for an efficient cloud computing with high security. *Journal of Scientific Research*, *64*(1). http://dx.doi.org/10.37398/JSR.2020.640152

[16] Ricard, T. C., Zhu, X., & Iyengar, S. S. (2023). Capturing weak interactions in surface adsorbate systems at coupled cluster accuracy: a graph-theoretic molecular fragmentation approach improved through machine learning. *Journal of Chemical Theory and Computation*, *19*(23), 8541-8556. https://doi.org/10.1021/acs.jctc.3c00955

[17] Sagar, M. S., & Sahgal, D. (2024). Artificial Intelligence with Cloud Resource Allocation: Cloud Computing Services With AI. In *Futuristic e-Governance Security with Deep Learning Applications* (pp. 199-222). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-6684-9596-4.ch011

[18] Soundappan, K., & Shenoy, G. S. (2023, February). Cloud Data Security Using Hybrid Encryption with Blockchain. In *International Conference on Emerging Research in Computing, Information, Communication and Applications* (pp. 383-393). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-7633-1_29

[19] Subramanian, M. V., & Malhotra, R. (2023). Bioinspired Filtration Systems for Heavy Metal Removal from Industrial Effluents. *Engineering Perspectives in Filtration and Separation*, 1-4.

[20] Thabit, F., Can, O., Wani, R. U. Z., Qasem, M. A., Thorat, S. B., & Alkhzaimi, H. A. (2023). Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms. *Concurrency and Computation: Practice and Experience*, *35*(21), e7691. https://doi.org/10.1002/cpe.7691

[21] Veerappan, S. (2023). The Role of Digital Ecosystems in Digital Transformation: A Study of How Firms Collaborate and Compete. *Global Perspectives in Management*, *1*(1), 78-89.

[22] Ziwei, M., & Han, L. L. (2023). Scientometric Review of Sustainable Land Use and Management Research. *Aquatic Ecosystems and Environmental Frontiers*, *1*(1), 21-24.

Authors Biography

Dr. Atmaram F. Shelke is an Associate Professor at Symbiosis Law School, Pune, a constituent of Symbiosis International (Deemed University). He holds an LL.M. with two gold medals from Symbiosis International University and a Ph.D. focused on Intellectual Property Rights (IPR) Volition in Cyberspace. His areas of academic specialization include IPR Violation in Cyberspace, Constitutional Law, Administrative Law, Criminal Law, and Research Methodology. Dr. Shelke brings over 14 years of teaching experience across undergraduate, postgraduate, and Ph.D. levels, including specialized courses on EU Data Protection and E-Justice. He has represented India under the DAAD New Passage to India Program in Germany and the EURASIA project in Bulgaria. A seasoned researcher and reviewer, he regularly evaluates submissions for reputed journals such as the Journal of Intellectual Property Rights (JIPR), Christ University Law Journal (CULJ), and IIJMMS. His contributions include collaborative research with institutions like City University of New York and several government-backed legal reform initiatives, including the Ministry of Home Affairs' report on the Criminal Justice System and recommendations for Digital Courts Vision (Phase III e-Courts Project). Dr. Shelke has over 20 academic publications to his credit and has guided multiple research projects in collaboration with CID Pune. He has also served as Deputy Director (Administration) at SLS Pune and has been an invited speaker at over 40 national and international academic events. He has completed advanced certifications from WIPO, GNLU, and Amaravati University in IPR, Cyber Law, and related fields.

Sujit Dhanuka is an Assistant Professor in the Department of uGDX at ATLAS SkillTech University, Mumbai, Maharashtra, India. With a keen interest in interdisciplinary design and innovation, he is actively involved in teaching and mentoring undergraduate students in design experiences and related domains. His academic and professional efforts focus on bridging creative design thinking with technological applications, contributing to a dynamic and future-oriented curriculum.

K. Soumya, is an Assistant Professor in the Department of Computer Science and Information Technology at Jain (Deemed-to-be University), Bangalore, Karnataka, India. She is engaged in teaching and research in the field of computer science, with a strong focus on modern technological trends and academic excellence. Her work contributes to both undergraduate and postgraduate learning experiences, emphasizing applied learning and innovation in computing.

Dr. Arvind Kumar Pandey is an Associate Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. With extensive experience in academia and research, Dr. Pandey focuses on advanced computing technologies, software engineering, and data analytics. He has contributed significantly to curriculum development and has guided numerous students in research projects and academic excellence.

Shikhar Gupta is affiliated with the Chitkara Centre for Research and Development, Chitkara University, located in Himachal Pradesh, India. His research contributions are aligned with emerging technologies, innovation, and applied sciences, contributing to the university's research ecosystem. He actively collaborates on institutional and interdisciplinary projects aimed at advancing impactful research outcomes.

Nipun Setia is affiliated with the Centre of Research Impact and Outcome, Chitkara University, Rajpura, Punjab, India. He is actively engaged in interdisciplinary research and academic development initiatives that contribute to the institution's mission of impactful scholarship and innovation.