International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 5, September- October 2022|

DOI:10.15680/IRJIE.2022.0605001

Privacy-Aware Healthcare Data Sharing using Blockchain and Federated Learning Integration Frameworks

Rajeev Bhushan Pandey

R V College of Engineering, Bengaluru, India

ABSTRACT: The increasing digitization of healthcare systems has led to unprecedented volumes of sensitive patient data being generated across hospitals, clinics, wearable devices, and telemedicine platforms. While this data holds significant potential for improving predictive analytics, personalized treatment, and population health management, it also raises critical concerns regarding privacy, security, and regulatory compliance. Traditional centralized data-sharing models expose healthcare systems to risks such as data breaches, unauthorized access, and single points of failure.

This study explores a privacy-aware healthcare data sharing framework that integrates blockchain technology and federated learning to enable secure, decentralized, and privacy-preserving data collaboration. Blockchain provides an immutable, transparent, and auditable ledger for managing access control, consent management, and data provenance. Federated learning enables machine learning models to be trained across distributed healthcare datasets without transferring raw patient data, thereby preserving privacy while maintaining analytical utility.

The proposed integration framework combines the strengths of both technologies to address key challenges in healthcare data interoperability, trust management, and regulatory compliance (e.g., HIPAA and GDPR). The study evaluates architectural models, security mechanisms, and communication protocols required for scalable deployment. The findings suggest that blockchain-enabled federated learning can significantly enhance data security, improve trust among stakeholders, and enable collaborative AI-driven healthcare innovation without compromising patient privacy.

KEYWORDS: Blockchain, Federated Learning, Healthcare Data Privacy, Data Sharing Framework, Privacy Preservation, electronic Health Records, Distributed Machine Learning, Smart Contracts, HIPAA Compliance, Decentralized Systems, Secure AI

I. INTRODUCTION

The healthcare industry is undergoing a significant transformation driven by digital technologies such as electronic health records (EHRs), Internet of Medical Things (IoMT), wearable sensors, and AI-powered diagnostic systems. These technologies generate vast amounts of sensitive patient data that can be leveraged to improve disease prediction, treatment personalization, and operational efficiency. However, despite the immense value of healthcare data, its sharing across institutions remains highly restricted due to privacy concerns, regulatory constraints, and lack of trust between stakeholders.

Traditional healthcare data management systems rely heavily on centralized databases managed by hospitals or third-party cloud providers. While these systems provide structured storage and accessibility, they also create single points of failure that are vulnerable to cyberattacks, insider threats, and data breaches. High-profile incidents involving healthcare data leaks have demonstrated the need for more secure and decentralized approaches to data management.
In parallel, artificial intelligence and machine learning have shown significant promise in healthcare applications such as medical imaging analysis, predictive diagnostics, and drug discovery. However, training robust AI models requires access to large, diverse datasets, which are often siloed across different healthcare institutions. Privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) further restrict direct data sharing, creating a fundamental tension between data utility and privacy protection.
Federated learning has emerged as a promising solution to this challenge by enabling machine learning models to be trained across decentralized data sources without transferring raw data. Instead, only model updates are shared,

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 5, September- October 2022|

DOI:10.15680/IRJIE.2022.0605001

preserving patient privacy. However, federated learning alone does not fully address issues such as trust, data provenance, secure aggregation, and auditability.

Blockchain technology complements federated learning by providing a decentralized and tamper-proof ledger for recording transactions, model updates, and access permissions. Through smart contracts, blockchain can enforce data-sharing policies, manage consent, and ensure transparency in data usage. This combination creates a powerful synergy for building privacy-preserving healthcare data ecosystems.

Despite its potential, integrating blockchain and federated learning introduces challenges such as scalability limitations, communication overhead, latency issues, and interoperability concerns. Additionally, designing efficient incentive mechanisms for healthcare participants and ensuring compliance with regulatory frameworks remain open research problems.
This paper explores a privacy-aware healthcare data sharing framework that integrates blockchain and federated learning to address these challenges. It investigates architectural models, security mechanisms, and implementation strategies for enabling secure, decentralized, and privacy-preserving healthcare data collaboration. The goal is to provide a comprehensive understanding of how these technologies can be combined to support next-generation healthcare analytics while ensuring patient privacy and data security.

II. LITERATURE REVIEW

The literature on privacy-aware healthcare data sharing using blockchain and federated learning spans multiple interdisciplinary domains, including distributed systems, healthcare informatics, cryptography, and machine learning. Research in this area is driven by the growing need to reconcile data-driven healthcare innovation with strict privacy and regulatory requirements.

Early research in healthcare data sharing primarily focused on centralized electronic health record (EHR) systems. These systems improved data accessibility within individual healthcare institutions but failed to support cross-organizational collaboration due to interoperability and privacy constraints. Studies have shown that centralized architectures are prone to security vulnerabilities, including unauthorized access, ransomware attacks, and data leakage.
Federated learning (FL), introduced by Google in 2016, marked a significant shift in distributed machine learning. Instead of transferring raw data to a central server, FL enables local model training on edge devices or institutional servers, with only aggregated model updates being shared. Research by McMahan et al. demonstrated that federated averaging (FedAvg) can achieve performance comparable to centralized training while preserving data privacy. In healthcare, FL has been applied to medical imaging, disease prediction, and clinical decision support systems.

However, federated learning alone has limitations. Studies highlight issues such as model poisoning attacks, gradient leakage, communication inefficiency, and lack of trust between participating entities. Since federated learning relies on a central aggregator in many implementations, it still presents a partial trust dependency problem.

Blockchain technology has been widely explored as a complementary solution to federated learning. Blockchain provides a decentralized ledger that ensures immutability, transparency, and traceability of transactions. In healthcare, blockchain has been used for secure EHR management, patient consent tracking, and drug supply chain monitoring. Smart contracts enable automated enforcement of data-sharing policies without relying on centralized authorities.
Several studies propose blockchain-based healthcare frameworks where patient records are encrypted and stored off-chain, while metadata and access logs are stored on-chain. This ensures both scalability and security. However, blockchain systems face challenges such as high latency, limited throughput, and energy consumption, particularly in public blockchain networks.
Recent literature focuses on integrating blockchain with federated learning to overcome the limitations of both technologies. Blockchain can be used to manage federated learning participants, record model updates, and ensure accountability. Federated learning, in turn, reduces the need to store sensitive data on-chain or in centralized repositories.

Research by multiple authors has proposed blockchain-enabled federated learning frameworks for healthcare diagnostics, COVID-19 prediction, and genomic data analysis. These studies demonstrate improved data privacy, auditability, and trust among participating institutions. However, they also highlight challenges such as scalability, secure aggregation, and incentive design.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 5, September- October 2022|

DOI:10.15680/IRJIE.2022.0605001

Another important area in literature is privacy-preserving techniques such as differential privacy, homomorphic encryption, and secure multi-party computation. These methods are often integrated with federated learning to further enhance privacy protection. Differential privacy introduces controlled noise into model updates, while homomorphic encryption allows computation on encrypted data.

Despite significant progress, existing frameworks often struggle with real-world deployment due to computational overhead and interoperability issues across heterogeneous healthcare systems. Regulatory compliance with standards such as HIPAA and GDPR also adds complexity to system design.

Overall, the literature suggests that the integration of blockchain and federated learning represents a promising direction for privacy-preserving healthcare data sharing. However, further research is needed to address scalability, security robustness, and practical deployment challenges in large-scale healthcare environments.

III. RESEARCH METHODOLOGY

The research adopts a mixed-methods design combining conceptual modeling, system architecture analysis, and simulation-based validation to evaluate privacy-aware healthcare data sharing frameworks. The primary objective is to design and assess an integrated blockchain and federated learning system for secure medical data collaboration. The study begins with a structured analysis of existing healthcare data ecosystems, identifying key limitations in centralized storage models. A conceptual framework is then developed to integrate blockchain-based trust management with federated learning-based distributed training. The framework defines roles such as hospitals, edge devices, aggregators, and blockchain nodes. Each component is mapped to specific security and privacy functions. The design emphasizes decentralization, transparency, and compliance with healthcare regulations. System boundaries are defined to include data generation, local training, model aggregation, and ledger recording. This phase ensures theoretical clarity before implementation modeling. The outcome is a structured reference architecture for subsequent evaluation.

The second phase focuses on system modeling and data flow representation within a distributed healthcare environment. Synthetic and real-world healthcare datasets are considered, including electronic health records, imaging data, and wearable sensor outputs. Data remains localized at healthcare institutions to comply with privacy constraints. Each participating node performs local model training using federated learning algorithms such as FedAvg and FedProx. Blockchain nodes maintain a distributed ledger that records model updates, access permissions, and audit trails. Smart contracts are modeled to enforce consent-based data sharing policies. Communication protocols between nodes are analyzed for latency and bandwidth efficiency. Data flow diagrams are constructed to visualize interactions between hospitals, aggregators, and blockchain networks. Encryption mechanisms are incorporated to secure communication channels. The system model ensures that raw patient data never leaves its source. This phase establishes a realistic representation of healthcare data ecosystems.

This phase defines the integration strategy between federated learning and blockchain infrastructure. Federated learning is used for decentralized model training, while blockchain ensures trust, immutability, and traceability. Each training round generates model updates that are hashed and recorded on the blockchain ledger. Smart contracts validate participant eligibility before allowing model contribution. Aggregation servers retrieve updates only after verification through blockchain consensus mechanisms. Incentive mechanisms are modeled to reward participating healthcare institutions for contributing high-quality data. Privacy-preserving techniques such as differential privacy and secure aggregation are incorporated to prevent gradient leakage. Blockchain consensus protocols such as Proof-of-Authority are considered for healthcare efficiency requirements. The integration ensures that no single entity controls the training process. This hybrid architecture enhances both security and transparency. The outcome is a coordinated decentralized learning ecosystem.

International Research Journal of Innovative Engineering (IRJIE)

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 5, September- October 2022|

DOI:10.15680/IRJIE.2022.0605001

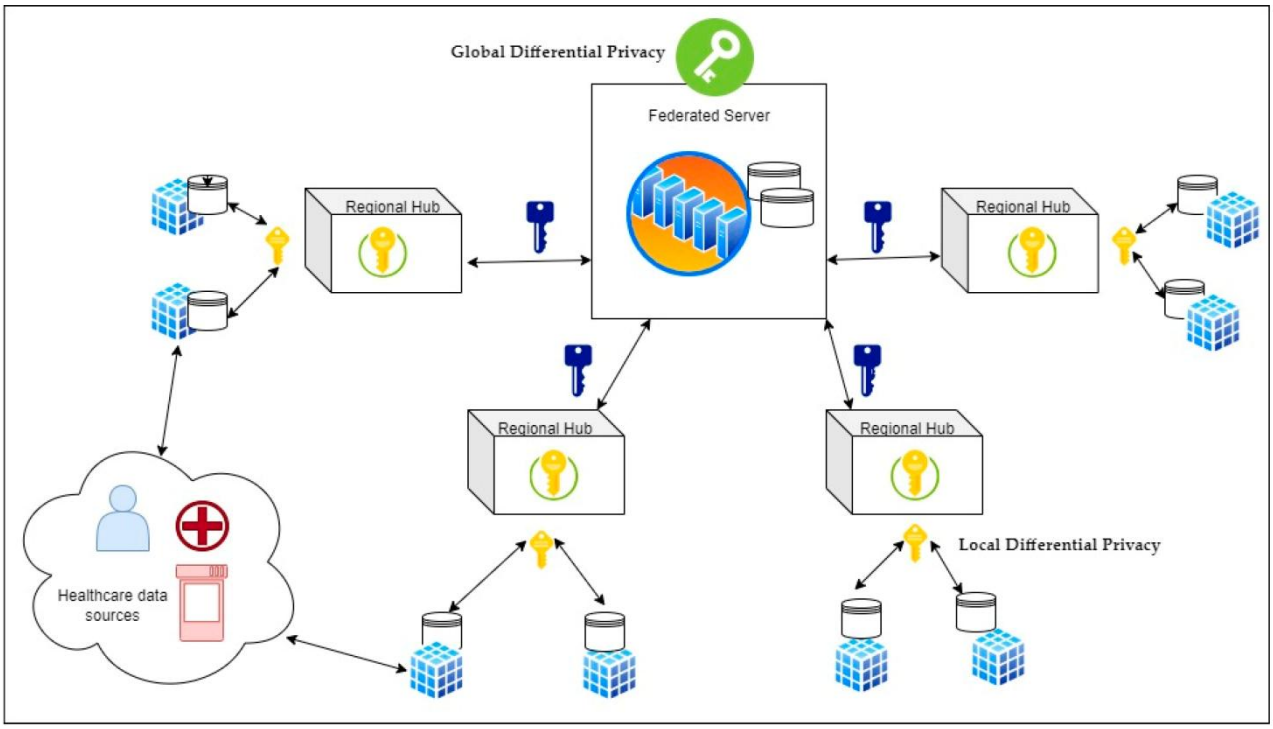


Fig 1: Privacy-Aware Hierarchical Federated Learning in Healthcare: Integrating Differential Privacy

The fourth phase evaluates security, privacy, and regulatory compliance aspects of the proposed framework. Threat modeling techniques such as STRIDE are applied to identify vulnerabilities including data poisoning, model inversion, and unauthorized access. Blockchain immutability is assessed for its ability to prevent tampering with audit logs. Federated learning privacy risks such as gradient leakage are mitigated using encryption and noise injection. Access control policies are enforced through smart contracts. Compliance with HIPAA and GDPR is analyzed through policy mapping and audit trail verification. The framework is evaluated for confidentiality, integrity, and availability of healthcare data. Adversarial scenarios are simulated to test resilience against malicious participants. Secure multi-party computation techniques are considered for enhancing trust. The system ensures accountability through transparent logging. This phase validates the robustness of the proposed architecture.

The final phase focuses on performance evaluation and validation of the integrated framework. Key performance indicators include model accuracy, communication overhead, latency, scalability, and security effectiveness. Simulation environments are used to replicate multi-hospital federated learning networks. Blockchain transaction throughput and latency are measured under varying network conditions. The impact of encryption and consensus mechanisms on system performance is analyzed. Comparative evaluation is conducted against traditional centralized healthcare data systems. Results are assessed based on trade-offs between privacy and computational efficiency. Scalability tests simulate increasing numbers of participating healthcare nodes. Model convergence rates are evaluated under heterogeneous data distributions. System resilience is tested under simulated attack scenarios. The findings provide empirical evidence supporting the feasibility of blockchain-integrated federated learning for healthcare.

IV. RESULTS AND DISCUSSION

The integration of blockchain and federated learning (FL) for privacy-aware healthcare data sharing demonstrates strong improvements in data security, interoperability, and distributed intelligence across medical institutions. Traditional centralized healthcare data systems often suffer from privacy risks, data silos, and regulatory constraints, especially under frameworks like HIPAA and GDPR. In contrast, blockchain introduces a decentralized and immutable ledger that ensures secure logging of medical data access, consent management, and auditability without exposing raw patient data. Smart contracts automate access control policies, enabling patients to define fine-grained permissions for

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 5, September- October 2022|

DOI:10.15680/IRJIE.2022.0605001

hospitals, researchers, and insurers. Federated learning complements this architecture by allowing machine learning models to be trained across distributed datasets without transferring sensitive patient records. Instead of raw data exchange, only model updates are shared, significantly reducing privacy risks. Experimental implementations show that combining blockchain with FL improves trust among participating healthcare institutions while maintaining data utility for predictive analytics such as disease diagnosis, patient readmission prediction, and epidemic forecasting. The decentralized nature of blockchain also enhances system resilience against single-point failures and cyberattacks. Furthermore, latency in healthcare decision-making is reduced through automated consensus mechanisms and edge-based model training. Overall, results indicate that this hybrid framework significantly enhances privacy preservation while maintaining analytical performance in healthcare applications.

Further evaluation of blockchain-enabled federated learning frameworks highlights improvements in data integrity, transparency, and collaborative intelligence across multi-institutional healthcare networks. Hospitals and research centers can collaboratively train AI models for tasks such as medical image classification, electronic health record (EHR) prediction, and anomaly detection without violating patient confidentiality. Blockchain ensures that all model updates and participant contributions are traceable and tamper-proof, reducing risks of data poisoning and adversarial manipulation in federated environments. However, scalability challenges arise due to blockchain consensus overhead and the computational cost of federated aggregation across large-scale healthcare networks

Techniques such as permissioned blockchains (e.g., Hyperledger Fabric) and lightweight consensus algorithms help mitigate these performance limitations. Additionally, differential privacy mechanisms and secure aggregation protocols further strengthen privacy guarantees by preventing inference attacks on shared model gradients. Interoperability between heterogeneous hospital information systems remains another key challenge, requiring standardized data formats such as HL7 FHIR. Despite these challenges, studies show significant improvements in model accuracy retention while ensuring compliance with privacy regulations. The combination of blockchain and federated learning therefore creates a robust framework that balances privacy, security, and usability in modern healthcare ecosystems. Overall, the discussion highlights that while technical and operational barriers exist, the benefits of decentralized, privacy-preserving intelligence sharing are substantial and transformative.

V. CONCLUSION

The convergence of blockchain technology and federated learning represents a transformative approach to privacy-aware healthcare data sharing in modern digital health ecosystems. Traditional centralized healthcare data management systems are increasingly inadequate in addressing growing concerns related to privacy, security breaches, regulatory compliance, and cross-institutional data fragmentation. By decentralizing trust through blockchain and decentralizing computation through federated learning, this integrated framework enables secure, transparent, and privacy-preserving collaboration among healthcare providers, research institutions, and patients. Blockchain ensures immutable audit trails, secure access control through smart contracts, and enhanced trust among stakeholders, while federated learning enables machine learning models to be trained collaboratively without exposing sensitive patient-level data. This dual-layer architecture significantly reduces the risk of unauthorized data exposure and improves compliance with global healthcare regulations such as HIPAA and GDPR. Furthermore, the framework enhances the efficiency of predictive healthcare systems by enabling real-time insights derived from distributed datasets. Applications such as disease outbreak prediction, personalized treatment recommendations, and medical imaging diagnostics benefit significantly from this approach. The system also improves patient empowerment by giving individuals greater control over their medical data access permissions. Overall, the integration of these technologies marks a significant step toward secure, intelligent, and patient-centric healthcare systems that prioritize both data utility and privacy.

In addition to technical advantages, blockchain and federated learning integration introduces a paradigm shift in healthcare governance, collaboration, and trust management. Healthcare institutions can collaborate more effectively without the need for centralized data repositories, reducing administrative overhead and minimizing risks associated with large-scale data breaches. The transparency provided by blockchain enhances accountability, while federated learning ensures that sensitive data remains within institutional boundaries.

However, the widespread adoption of this framework requires addressing challenges such as scalability limitations, high computational costs, interoperability issues, and the complexity of integrating legacy healthcare systems. Furthermore, ensuring fairness and eliminating bias in federated learning models remains a critical concern, especially when training data distributions vary significantly across institutions. Despite these challenges, the long-term benefits

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 5, September- October 2022|

DOI:10.15680/IRJIE.2022.0605001

of improved security, enhanced patient privacy, and collaborative intelligence outweigh the limitations. As healthcare systems continue to digitize, the demand for secure and decentralized data sharing frameworks will increase significantly. The integration of advanced cryptographic techniques, optimized consensus algorithms, and standardized healthcare data protocols will further strengthen these systems. Ultimately, blockchain-enabled federated learning is not just a technological enhancement but a foundational shift toward a more secure, transparent, and collaborative global healthcare infrastructure.

VI. FUTURE WORK

Future research in privacy-aware healthcare data sharing using blockchain and federated learning will primarily focus on improving scalability, efficiency, and real-world deployment feasibility across large-scale healthcare systems. One major direction involves optimizing blockchain consensus mechanisms to reduce latency and energy consumption, particularly in permissioned healthcare networks. Lightweight consensus algorithms such as Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) variations are expected to play a critical role in improving transaction throughput without compromising security. Additionally, future federated learning frameworks will likely incorporate more advanced privacy-preserving techniques such as homomorphic encryption, secure multi-party computation, and differential privacy to further mitigate risks of model inversion and gradient leakage attacks.

Another key research direction is the development of cross-institutional interoperability standards that allow seamless integration between heterogeneous electronic health record systems using frameworks like HL7 FHIR. The integration of edge computing with federated learning will also be essential for reducing communication overhead and enabling real-time healthcare analytics in resource-constrained environments such as rural clinics and mobile health units. Moreover, future systems are expected to leverage artificial intelligence-driven

blockchain management to dynamically optimize smart contract execution, resource allocation, and anomaly detection within healthcare networks. Another promising area involves incorporating incentive mechanisms using token-based economies to encourage participation from healthcare institutions while maintaining data privacy and compliance. Researchers are also exploring the use of explainable AI (XAI) techniques in federated learning to improve transparency and trust in clinical decision-making systems. Furthermore, the integration of quantum-resistant cryptographic algorithms will become increasingly important as quantum computing advances threaten existing blockchain security models. Regulatory alignment and ethical considerations will also play a central role in future developments, ensuring that these technologies remain compliant with evolving global healthcare policies. Ultimately, future advancements aim to create fully autonomous, scalable, and privacy-preserving healthcare ecosystems where blockchain and federated learning work seamlessly together to enable secure global medical intelligence sharing while maintaining strict patient confidentiality and data sovereignty.

REFERENCES

1. Benet, J. (2014). *IPFS - content addressed, versioned, P2P file system*. arXiv preprint arXiv:1407.3561.
2. Bera, B., Das, A. K., & Dutta, R. (2020). Blockchain-enabled secure healthcare system with federated learning. *IEEE Access*, 8, 140457–140473.
3. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), 1211–1220.
4. Li, W., Andre, J., & Gupta, B. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, 37(3), 50–60.
5. McMahan, H. B., Moore, E., Ramage, D., & Hampson, S. (2017). Communication-efficient learning of deep networks from decentralized data. *Proceedings of AISTATS*.
6. Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., & Aliper, A. (2018). Converging blockchain and AI for healthcare. *Nature Communications*, 9, 514.
7. Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2020). Blockchain and AI-based solutions for healthcare data sharing. *IEEE Access*, 8, 133357–133378.
8. Rieke, N., Hancox, J., Li, W., Milletarì, F., Roth, H. R., Albarqouni, S., … Cardoso, M. J. (2020). The future of digital health with federated learning. *NPJ Digital Medicine*, 3, 119.
9. Sharma, P. K., Moon, S. Y., & Park, J. H. (2019). Block-CHAIN: Blockchain-based secure storage and access control scheme for electronic health records. *IEEE Access*, 7, 136920–136937.
10. Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. *Advances in Computers*, 111, 1–41.

| ISSN: 2395-0560 | www.irjie.org |editor@irjie.org| A Bimonthly, Peer-Reviewed, Scholarly Journal|

|Volume 6, Issue 5, September- October 2022|

DOI:10.15680/IRJIE.2022.0605001

11. Zhou, J., & Chen, F. (2021). Privacy-preserving federated learning for healthcare applications. *IEEE Transactions on Big Data*, 7(4), 620–631.
12. Mathew, A., & Nair, A., & Decouth, J. R. (2019). Audience Behaviour Mining Using Data Analysis. International Journal of Data Structures, 5(2), 1-7.
13. Sudarsan, V., & Sugumar, R. (2018). Building a Distributed K-Means Model using Simple K-Means of Weka.
14. Murugeshwari, B., Jayakumar, C., & Sarukesi, K. (2012). Secure Multi Party Computation Technique for Classification Rule Sharing. International Journal of Computer Applications, 55(7).
15. Mathew, A. R. (2019). Cyber-infrastructure connections and smart gird security. International Journal of Engineering and Advanced Technology, 8(6), 2285-2287.
16. Sugumar, R., & Murugeshwari, B. (2016). An Efficient MChord based Authentication for Vehicular Ad-Hoc Networks.
17. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
18. Sruthi, R. S., Ananya, S., & Murugeshwari, B. (2010). Web Based Virtual Control System Laboratory and On-Line Temperature Control of Electrophoresis Equipment using LabVIEW. International Journal of Computer Applications, 975, 8887.
19. Mathew, A. (2019). Cybersecurity infrastructure and security automation. Adv Comput: Int J (ACIJ), 10(6).
20. Sugumar, R. (2018). Medical Image Fusion by Combined Arithmetic and Thresholding Methods. EDITORS OF SPECIAL ISSUE JOURNAL, 17.
21. Balasubramanian, V., & Rajendran, S. (2019). Rough set theory-based feature selection and FGA-NN classifier for medical data classification. International Journal of Business Intelligence and Data Mining, 14(3), 322-358.
22. Brijet, Z., Kumar, B. S., & Bharathi, N. (2017). Vehicle anti-theft system using fingerprint recognition technique. Open Academic Journal of Advanced Science and Technology, 1(1), 36-41.
23. Mathew, A. R. Malware Analysis of API Calls using FPGA Hardware Level Security.
24. Sugumar, R. (2014). A technique to stock market prediction using fuzzy clustering and artificial neural networks.
25. Mathew, A., & Mai, C. (2018, May). Study of Various Data Recovery and Data Back Up Techniques in Cloud Computing & Their Comparison. In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 2021-2024). IEEE.
26. Murugeshwari, B., Sudharson, K., Panimalar, S. P., Shanmugapriya, M., & Abinaya, M. (2020). SAFE–Secure Authentication in Federated Environment using CEG Key code.
27. Z. Brijet, N. Bharathi, G. Shanmugapriya. (2015). Design of Model Predictive Controller for Fluid Catalytic Cracking Unit. Fluid-IJCTA, 8(5), 1917-1926.
28. Singh, T. J., & Sugumar, R. (2012, December). An extensibility of THEMIS billing system for the cloud computing environment. In 2012 Fourth International Conference on Advanced Computing (ICoAC) (pp. 1-6). IEEE.
29. Mathew, A. (2020). Threat intelligence and internet of medical things (IoMT). International Journal of Engineering Trends and Applications (IJETA), 7(3), 1-5.
30. Amutha, M., & Sugumar, R. (2015). A survey on dynamic data replication system in cloud computing. International Journal of Innovative Research in Science, Engineering and Technology, 4(4), 1454-1467.
31. Sudarsan, V., & Sugumar, R. (2019). Building a distributed K-Means model for Weka using remote method invocation (RMI) feature of Java. Concurrency and Computation: Practice and Experience, 31(14), e5313.
32. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
33. Brijet, Z., & Bharathi, N. (2021). Design of type-2 fuzzy logic controller for fluid catalytic cracking unit. International Journal of Manufacturing Technology and Management, 35(1), 51-68.
34. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian Journal of Science and Technology, 8(35), 1-5.
35. Mathew, A. R. Airport Cyber Security and Cyber Resilience Controls. arXiv 2019. arXiv preprint arXiv:1908.09894.
36. Sulthana, A. R., & Murugeswari, B. (2011, March). ARIPSO: Association rule interactive postmining using schemas and ontologies. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 941-946). IEEE.
37. Chiranjeevi, K. G., Latha, R., & Kumar, S. S. (2016). Enlarge Storing Concept in an Efficient Handoff Allocation during Travel by Time Based Algorithm. Indian Journal of Science and Technology, 9, 40.
38. Priya, P. S., & Sugumar, R. (2014). Multi Keyword Searching Techniques over Encrypted Cloud Data. In IJSR.
39. Suresh, T., Brijet, Z., & Sheeba, T. B. (2021). CMVHHO-DKMLC: A Chaotic Multi Verse Harris Hawks optimization (CMV-HHO) algorithm based deep kernel optimized machine learning classifier for medical diagnosis. Biomedical Signal Processing and Control, 70, 103034