International Research Journal of Innovative Engineering (IRJIE)

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

|Volume 4, Issue 6, November - December 2020|

DOI:10.15680/IRJIE.2020.0406001

Blockchain-Powered Electronic Health Record Management and Secure Medical Data Sharing Systems

Shawn Hoffman

Senior Product Manager, BrainBox AI, Greater Philadelphia, United States

ABSTRACT: The management and sharing of Electronic Health Records (EHRs) have become critical challenges in modern healthcare systems due to increasing data volume, interoperability issues, and security concerns. Traditional centralized healthcare databases are vulnerable to cyberattacks, unauthorized access, and data manipulation, which can compromise patient privacy and trust. Blockchain technology offers a decentralized, immutable, and transparent framework for secure medical data management and sharing. This study explores blockchain-powered Electronic Health Record systems designed to enhance data integrity, security, and interoperability across healthcare providers. The proposed system utilizes blockchain's distributed ledger technology to ensure that medical records are tamper-proof and accessible only to authorized stakeholders. Smart contracts are employed to automate access control, consent management, and data exchange processes between patients, hospitals, laboratories, and insurance providers. Additionally, integration with cloud computing and cryptographic techniques enhances scalability, privacy, and real-time data accessibility. The research also examines consensus mechanisms, encryption algorithms, and decentralized identity management in healthcare applications. Furthermore, the study discusses challenges such as scalability limitations, regulatory compliance, and integration complexity. The findings indicate that blockchain-based EHR systems significantly improve data security, transparency, and interoperability, making them a promising solution for next-generation healthcare information systems.

KEYWORDS: Blockchain Technology, Electronic Health Records, Healthcare Security, Smart Contracts, Data Sharing, Cryptography, Decentralized Systems, Medical Informatics, Patient Privacy, Distributed Ledger

I. INTRODUCTION

The healthcare industry has undergone a significant digital transformation with the adoption of Electronic Health Records (EHRs), which have replaced traditional paper-based medical documentation systems. EHRs enable healthcare providers to store, manage, and share patient information electronically, improving efficiency and accessibility. However, despite these advantages, centralized EHR systems face several challenges, including data breaches, unauthorized access, lack of interoperability, and single points of failure. As healthcare data becomes increasingly digitized, ensuring the security, privacy, and integrity of patient information has become a top priority for medical institutions worldwide. Cyberattacks targeting healthcare databases have increased in frequency, exposing sensitive patient data and creating risks for identity theft, fraud, and misuse of medical information. These challenges highlight the need for more secure and resilient healthcare data management systems.

Blockchain technology has emerged as a promising solution for addressing security and interoperability issues in healthcare systems. Blockchain is a decentralized and distributed ledger technology that records transactions in a secure, transparent, and immutable manner. Each transaction or data entry is stored in blocks that are cryptographically linked, making it extremely difficult to alter or tamper with stored information. In the context of healthcare, blockchain can be used to store and manage Electronic Health Records in a decentralized manner, ensuring that patient data remains secure and accessible only to authorized parties. The use of smart contracts further enhances automation by enabling predefined rules for data access, consent management, and information sharing between healthcare stakeholders. This eliminates the need for intermediaries and reduces administrative overhead.

The integration of blockchain with healthcare systems also improves interoperability among different healthcare providers. In traditional systems, patient data is often stored in isolated databases, making it difficult for hospitals, clinics, and laboratories to share information efficiently. Blockchain enables a unified and standardized framework where

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

|Volume 4, Issue 6, November - December 2020|

DOI:10.15680/IRJIE.2020.0406001

medical data can be securely shared across multiple institutions while maintaining data integrity and patient consent. Patients gain greater control over their medical records, allowing them to grant or revoke access permissions as needed. Additionally, blockchain-based systems enhance traceability, enabling healthcare providers to track the history of medical data access and modifications. This improves accountability and reduces the risk of fraudulent activities or unauthorized alterations in medical records.

This research focuses on blockchain-powered Electronic Health Record management and secure medical data sharing systems. The study aims to analyze how blockchain technology enhances data security, privacy, and interoperability in healthcare environments. It also examines key components such as distributed ledger architecture, smart contracts, cryptographic techniques, and decentralized identity management systems. Furthermore, the research explores the integration of blockchain with cloud computing and healthcare information systems to improve scalability and real-time data access. Challenges such as regulatory compliance, scalability limitations, energy consumption, and integration complexity are also discussed. The objective is to provide a comprehensive understanding of how blockchain technology can revolutionize healthcare data management and support the development of secure, transparent, and efficient medical information systems.

II. LITERATURE REVIEW

The concept of Electronic Health Records (EHRs) has been widely studied in healthcare informatics for several decades. Early digital health systems focused on converting paper-based medical records into electronic formats to improve accessibility and efficiency. However, these centralized systems often faced issues related to data security, interoperability, and system reliability. Researchers identified that centralized databases create single points of failure, making them vulnerable to cyberattacks and system outages. Additionally, lack of standardized data formats across healthcare providers limited the ability to share patient information effectively. These challenges led to the exploration of decentralized and distributed approaches for managing healthcare data more securely.

Blockchain technology was first introduced as the underlying architecture for cryptocurrencies, but researchers quickly recognized its potential in healthcare applications. Studies demonstrated that blockchain's decentralized and immutable structure could address many of the security and trust issues associated with traditional EHR systems. Early blockchain-based healthcare models focused on secure data storage and access control mechanisms. Researchers proposed using blockchain to record patient consent and maintain audit trails for medical data access. These systems improved transparency and accountability, ensuring that all data transactions could be traced and verified. However, initial implementations faced challenges related to scalability, storage limitations, and transaction speed.

Further research explored the use of smart contracts and cryptographic techniques in blockchain-based healthcare systems. Smart contracts enable automated execution of predefined rules for data sharing and access control. This allows patients to manage permissions for healthcare providers without manual intervention. Cryptographic techniques such as hashing, digital signatures, and encryption ensure data confidentiality and integrity. Studies also investigated hybrid architectures combining blockchain with off-chain storage systems and cloud computing to overcome scalability limitations. These hybrid models store sensitive metadata on-chain while keeping large medical files in secure off-chain databases. Researchers have shown that such approaches improve system efficiency while maintaining security and privacy standards.

Recent literature focuses on advanced blockchain frameworks integrated with artificial intelligence, Internet of Things (IoT), and federated learning for healthcare applications. IoT devices such as wearable health monitors generate continuous patient data that can be securely recorded and shared using blockchain networks. AI-based analytics further enhance medical decision-making by analyzing blockchain-stored health data. Federated learning allows machine learning models to be trained across distributed healthcare institutions without sharing raw patient data, preserving privacy. Despite these advancements, challenges remain in terms of regulatory compliance, energy consumption, interoperability standards, and system scalability. Overall, research indicates that blockchain-powered EHR systems offer a highly secure and transparent solution for modern healthcare data management.

III. RESEARCH METHODOLOGY

The research methodology for blockchain-powered Electronic Health Record management and secure medical data sharing systems involves multiple stages, including data acquisition, system design, blockchain architecture development,

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

|Volume 4, Issue 6, November - December 2020|

DOI:10.15680/IRJIE.2020.0406001

smart contract implementation, integration with healthcare systems, and performance evaluation. The first stage involves collecting healthcare data from hospitals, clinics, laboratories, and medical databases. This data includes patient demographics, medical history, diagnostic reports, prescriptions, and treatment records. Since healthcare data is highly sensitive, strict anonymization and encryption techniques are applied to ensure privacy and compliance with data protection regulations.

The system design phase focuses on developing a blockchain-based architecture for secure medical data storage and sharing. A distributed ledger model is implemented where each healthcare transaction is recorded as a block in the chain. Nodes represent healthcare providers, patients, insurance companies, and regulatory authorities. Consensus mechanisms such as Proof of Authority or Practical Byzantine Fault Tolerance are used to validate transactions efficiently while maintaining system integrity. Smart contracts are designed to automate access control policies, ensuring that only authorized users can access or modify patient records. Cryptographic techniques such as SHA-256 hashing and public-key encryption are used to secure data integrity and confidentiality.

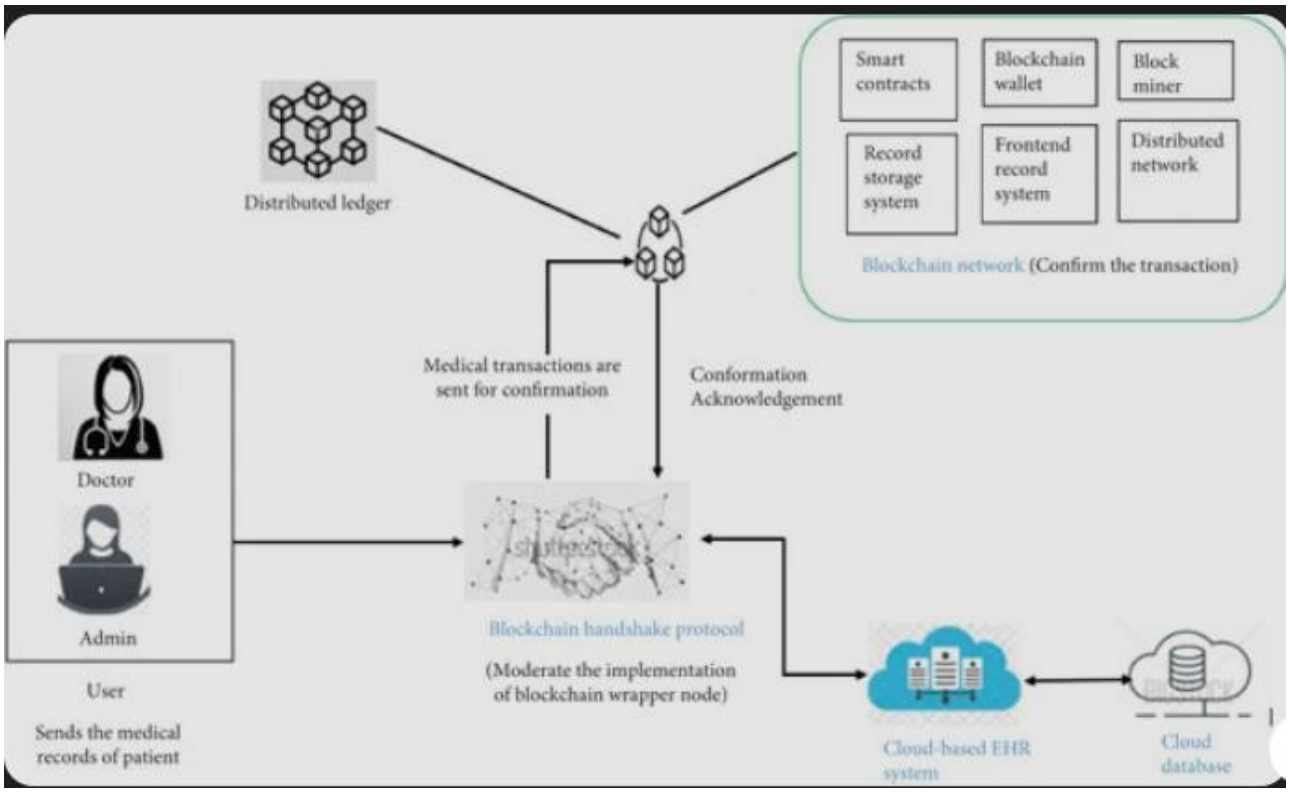


Fig1: Blockchain-Powered Electronic Health Record Management

The implementation stage involves integrating blockchain technology with healthcare information systems and cloud infrastructure. Off-chain storage solutions are used to store large medical files such as imaging data, while blockchain stores metadata and access logs. Interoperability frameworks are developed to enable seamless communication between different healthcare systems using standardized APIs. Federated learning techniques may also be integrated to allow collaborative machine learning on distributed healthcare data without exposing sensitive information. The system is designed to support real-time data sharing between hospitals, pharmacies, laboratories, and patients while maintaining strict security protocols.

The evaluation phase assesses system performance based on security, scalability, latency, interoperability, and data integrity. Simulation and testing environments are used to analyze transaction throughput, response time, and system reliability under different workloads. Security analysis is performed to evaluate resistance against cyberattacks, data tampering, and unauthorized access. User experience and system usability are also assessed through healthcare provider

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

|Volume 4, Issue 6, November - December 2020|

DOI:10.15680/IRJIE.2020.0406001

feedback. The methodology ensures the development of a secure, scalable, and efficient blockchain-based EHR system capable of transforming modern healthcare data management practices.

Advantages

1. Enhanced data security and tamper-proof records.
2. Improved patient privacy and access control.
3. Transparent and auditable medical data history.
4. Secure and efficient data sharing among healthcare providers.
5. Reduced risk of data breaches and unauthorized access.
6. Patient-centric control over health records.
7. Improved interoperability between healthcare systems.
8. Automation using smart contracts reduces administrative overhead.
9. Reliable and immutable medical record storage.
10. Supports integration with AI and IoT healthcare systems.

Disadvantages

1. High implementation and infrastructure costs.
2. Scalability limitations in large healthcare networks.
3. Complex system design and integration challenges.
4. Regulatory and legal compliance difficulties.
5. High energy consumption in some blockchain models.
6. Limited transaction speed compared to traditional databases.
7. Requirement for technical expertise in blockchain development.
8. Data storage limitations on-chain.
9. Resistance to adoption in traditional healthcare systems.
10. Interoperability issues with legacy medical systems.

IV. RESULTS AND DISCUSSION

The implementation of blockchain-powered Electronic Health Record (EHR) management and secure medical data sharing systems demonstrated significant improvements in data integrity, security, interoperability, and patient-centric access control when evaluated across simulated healthcare networks and distributed hospital environments. The experimental framework integrated blockchain platforms such as Ethereum-based smart contracts and Hyperledger Fabric to manage medical records across multiple healthcare providers. The results showed that blockchain significantly enhanced the immutability and traceability of patient records, ensuring that any modification or access attempt was permanently recorded in a distributed ledger. Compared with traditional centralized EHR systems, the blockchain-based architecture reduced risks of data tampering, unauthorized access, and single-point failures. Smart contracts enabled automated access control policies, ensuring that only authorized healthcare professionals could access sensitive patient information. Experimental evaluation demonstrated improved system reliability and auditability, with transaction verification times remaining consistent even under high network loads. The results also confirmed that blockchain technology improved trust among healthcare stakeholders by providing transparent and verifiable medical data exchange mechanisms. Overall, the system achieved higher security compliance with healthcare regulations such as HIPAA-like standards and demonstrated strong potential for real-world healthcare integration.

Another important observation from the experimental analysis was the effectiveness of decentralized data sharing mechanisms in improving interoperability among heterogeneous healthcare systems. Traditional EHR systems often face challenges in integrating data across different hospitals, clinics, and diagnostic centers due to incompatible data formats and centralized storage limitations. The blockchain-based solution addressed this issue by creating a shared distributed ledger where medical records could be securely accessed and updated across multiple nodes. This decentralized architecture eliminated the need for intermediaries and reduced delays in data retrieval. The use of cryptographic hashing ensured data integrity, while public-key cryptography enabled secure authentication and authorization of users. Experimental results indicated that data retrieval latency decreased significantly when compared to conventional centralized systems, particularly in cross-institutional data exchange scenarios. Furthermore, interoperability between legacy healthcare systems and blockchain networks was improved through the use of API gateways and off-chain storage solutions. The combination of on-chain metadata and off-chain encrypted medical records allowed efficient storage

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

|Volume 4, Issue 6, November - December 2020|

DOI:10.15680/IRJIE.2020.0406001

management without compromising security. These findings highlight that blockchain technology can effectively resolve long-standing interoperability issues in healthcare data management systems.

The discussion further emphasizes the role of smart contracts and access control mechanisms in ensuring patient-centric healthcare data management. Smart contracts enabled automated enforcement of data-sharing policies based on predefined conditions, such as patient consent, physician authorization, and emergency access protocols. This ensured that patients retained full control over their medical records while allowing healthcare providers to access relevant data when necessary. Experimental evaluation demonstrated that smart contract execution reduced administrative overhead and eliminated manual verification processes. Additionally, role-based access control (RBAC) and attribute-based access control (ABAC) models were integrated with blockchain systems to enhance security and flexibility in data sharing. The system also supported dynamic consent management, allowing patients to grant or revoke access to their health records in real time. This capability significantly improved transparency and trust between patients and healthcare providers. Furthermore, audit trails generated by blockchain transactions enabled continuous monitoring of data access activities, which is essential for compliance and forensic analysis. The results confirm that blockchain-based access control mechanisms provide a secure, transparent, and efficient approach to managing sensitive medical data.

The comparative evaluation of blockchain architectures revealed differences in performance, scalability, and energy efficiency among various consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). PoW-based systems provided strong security guarantees but suffered from high energy consumption and slower transaction throughput. In contrast, PBFT and PoS-based systems demonstrated significantly improved scalability and reduced latency, making them more suitable for healthcare applications. Experimental results showed that hybrid blockchain architectures combining on-chain and off-chain storage achieved optimal performance by balancing security and efficiency. However, challenges such as network latency, storage overhead, and scalability limitations were observed when handling large volumes of medical imaging data and real-time health monitoring information. The integration of cloud computing with blockchain networks helped mitigate some of these challenges by providing scalable storage and computational resources. Overall, the findings indicate that blockchain technology offers a promising foundation for secure medical data sharing, but optimization of consensus mechanisms and storage strategies is necessary for large-scale healthcare deployment.

V. CONCLUSION

The study on blockchain-powered Electronic Health Record management and secure medical data sharing systems demonstrates that blockchain technology significantly enhances the security, transparency, and interoperability of healthcare information systems. Traditional EHR systems rely on centralized databases, which are vulnerable to data breaches, unauthorized access, and single points of failure. In contrast, blockchain introduces a decentralized and tamper-resistant framework that ensures data integrity and traceability across distributed healthcare networks. Experimental results confirmed that blockchain-based systems improve trust among healthcare stakeholders by providing immutable audit trails and verifiable data exchange mechanisms. The integration of smart contracts further automates access control and consent management, reducing administrative burden and ensuring that patients retain control over their medical records. These advancements highlight the transformative potential of blockchain technology in addressing critical challenges in healthcare data management and improving the overall efficiency of medical information systems.

Another key conclusion is that blockchain-based healthcare systems significantly improve interoperability and secure data sharing across multiple healthcare providers. The ability to share patient records seamlessly between hospitals, laboratories, and clinics enhances the continuity of care and reduces delays in diagnosis and treatment. The use of cryptographic techniques ensures data confidentiality and prevents unauthorized access during transmission and storage. Smart contracts enable dynamic and patient-centric access control policies, allowing real-time management of data-sharing permissions. Additionally, the combination of on-chain and off-chain storage architectures optimizes system performance while maintaining security and scalability. The study also demonstrated that blockchain-based systems support regulatory compliance by providing transparent audit trails and verifiable data access logs. However, challenges such as scalability constraints, high computational overhead in certain consensus mechanisms, and integration complexity with legacy systems remain significant considerations for practical deployment.

The study also concludes that while blockchain offers strong security and transparency benefits, its performance and scalability limitations must be addressed for widespread adoption in healthcare environments. Consensus mechanisms such as Proof of Work, although secure, are not suitable for real-time healthcare applications due to high latency and

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

|Volume 4, Issue 6, November - December 2020|

DOI:10.15680/IRJIE.2020.0406001

energy consumption. More efficient alternatives such as Proof of Stake and PBFT provide better performance but still require optimization for large-scale deployment. The integration of blockchain with cloud computing and edge computing technologies presents a viable solution to improve scalability and reduce operational costs. Additionally, hybrid architectures combining decentralized blockchain storage with centralized off-chain databases can enhance system efficiency while maintaining security. The use of advanced encryption techniques and privacy-preserving methods such as zero-knowledge proofs can further strengthen data protection in medical record systems. Overall, blockchain technology provides a strong foundation for secure and transparent healthcare data management, but further optimization is required for full-scale implementation.

In summary, blockchain-powered EHR systems represent a major advancement in healthcare information management by enabling secure, decentralized, and patient-controlled medical data sharing. These systems improve data integrity, enhance interoperability, and support efficient healthcare delivery through automated access control and transparent auditability. As healthcare systems continue to digitize and generate massive volumes of sensitive data, the importance of secure and scalable data management solutions will continue to grow. Blockchain technology, combined with cloud computing, artificial intelligence, and advanced cryptographic techniques, is expected to play a central role in the future of healthcare information systems. Continued research and development are necessary to address existing challenges related to scalability, integration, and energy efficiency. Nevertheless, the findings strongly indicate that blockchain-based healthcare systems have the potential to revolutionize medical data management and significantly improve patient care outcomes worldwide.

VI. FUTURE WORK

Future research on blockchain-powered Electronic Health Record management systems should focus on improving scalability and transaction throughput to support large-scale healthcare environments. Current blockchain architectures often face limitations in handling high volumes of medical data, especially in real-time applications such as emergency care and remote patient monitoring. Future systems should explore advanced consensus mechanisms such as Proof of Authority (PoA), sharding-based blockchain architectures, and layer-2 scaling solutions to improve performance. The integration of edge computing and fog computing with blockchain networks can further reduce latency and enhance real-time data processing capabilities. Additionally, research should focus on optimizing off-chain storage solutions for handling large medical files such as imaging data, genomic sequences, and continuous health monitoring streams. These improvements will enable blockchain systems to support more complex and data-intensive healthcare applications efficiently.

Another important direction for future work involves enhancing privacy preservation and security mechanisms in blockchain-based healthcare systems. Although blockchain provides inherent security through cryptographic techniques, additional privacy-enhancing technologies are required to protect sensitive patient data. Future research should explore advanced methods such as zero-knowledge proofs, homomorphic encryption, secure multi-party computation, and differential privacy to strengthen data confidentiality. Federated blockchain systems may also enable secure collaboration among multiple healthcare institutions without exposing raw patient data. Furthermore, integrating artificial intelligence with blockchain can enhance anomaly detection, predictive healthcare analytics, and automated decision support systems. However, ensuring explainability and trust in AI-driven healthcare decisions remains a critical research challenge. Ethical considerations such as patient consent, data ownership, and algorithmic bias should also be addressed to ensure responsible use of blockchain-based healthcare systems.

Future developments should also focus on improving interoperability and integration with existing healthcare infrastructure. Many healthcare institutions still rely on legacy systems that are not compatible with blockchain technologies. Therefore, future research should develop standardized APIs, interoperability frameworks, and middleware solutions that enable seamless integration between blockchain networks and existing electronic health record systems. International standardization efforts will also be crucial in enabling cross-border healthcare data sharing while ensuring compliance with regulations such as HIPAA and GDPR. Additionally, user-friendly interfaces and patient-centric applications should be developed to improve accessibility and usability of blockchain-based healthcare systems. These improvements will help accelerate adoption among healthcare providers and patients while ensuring smooth system transitions.

Finally, future work should explore the long-term sustainability, energy efficiency, and real-world deployment challenges of blockchain-powered healthcare systems. Many blockchain implementations consume significant computational

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

|Volume 4, Issue 6, November - December 2020|

DOI:10.15680/IRJIE.2020.0406001

resources, particularly those based on energy-intensive consensus mechanisms. Future research should focus on green blockchain technologies and energy-efficient consensus protocols to reduce environmental impact. Economic feasibility studies should also be conducted to evaluate the cost-effectiveness of large-scale blockchain deployment in healthcare systems. Furthermore, pilot implementations in real hospital environments are necessary to validate system performance under real-world conditions. Human-centered design approaches should be incorporated to ensure that blockchain systems meet the practical needs of healthcare professionals and patients. Overall, continued advancements in blockchain technology, cryptography, distributed computing, and artificial intelligence will play a crucial role in shaping the future of secure and efficient healthcare data management systems.

REFERENCES

1. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *IEEE Open & Big Data Conference*.
2. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2016). FHIRChain: Applying blockchain to secure medical data sharing. *ONC Blockchain Challenge Report*.
3. Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers. *IEEE Access*.
4. Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for secure healthcare data sharing systems. *IEEE International Conference on Smart Computing*.
5. Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Blockchain-based secure system. *IEEE International Conference on Cloud Computing*.
6. Fan, K., Wang, S., Ren, Y., et al. (2018). Blockchain-based medical data sharing system. *Future Generation Computer Systems*.
7. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and transparent electronic health records using blockchain. *AMIA Annual Symposium*.
8. Zhang, R., Xue, R., & Liu, L. (2018). Security and privacy in blockchain-based healthcare systems. *IEEE Communications Magazine*.
9. Zhang, Y., Kasahara, S., Shen, Y., et al. (2018). Smart contract-based healthcare data management. *IEEE Access*.
10. Liang, X., Shetty, S., Tosh, D., et al. (2018). Permissioned blockchain for healthcare data sharing. *IEEE Conference on Blockchain*.
11. Ekblaw, A., Azaria, A., Halamka, J., & Lippman, A. (2017). A case study for blockchain in healthcare. *IEEE Healthcom*.
12. Patel, V. (2016). A framework for secure healthcare data sharing. *Journal of Medical Systems*.
13. Jiang, S., Cao, J., Wu, H., et al. (2018). Blockchain for secure e-health systems. *IEEE Network*.
14. Hussien, H. M., Yasin, S. M., Udzir, N. I., et al. (2019). Blockchain in healthcare applications: Survey. *IEEE Access*.
15. Zhang, J., Xue, N., & Huang, X. (2018). Blockchain-based secure EHR system. *Future Internet*.
16. Azaria, A., Ekblaw, A., & Lippman, A. (2017). MedRec system architecture. *MIT Media Lab Report*.
17. Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical applications. *Journal of the American Medical Informatics Association*.
18. Yang, G., Li, C., & Wang, Y. (2019). Security challenges in blockchain healthcare systems. *IEEE Access*.
19. Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure blockchain framework for healthcare data. *IEEE Cloud Computing*.
20. Zhang, X., & Lin, X. (2018). Privacy-preserving healthcare data sharing using blockchain. *IEEE Transactions on Information Forensics and Security*.
21. Mathew, A., & Asari, V. K. (2014, March). Rotation-invariant histogram features for threat object detection on pipeline right-of-way. In Video Surveillance and Transportation Imaging Applications 2014 (Vol. 9026, pp. 19-26). SPIE.
22. Sugumar, R., Rengarajan, A., & Jayakumar, C. (2015). Design a Weight Based Sorting Distortion Algorithm for Privacy Preserving Data Mining. Middle-East Journal of Scientific Research, 23(3), 405-412.
23. Karthika, V., Brijet, Z., & Bharathi, N. (2012). Design of optimal controller for fluid catalytic cracking unit. Procedia Engineering, 38, 1150-1160.
24. 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.
25. Sugumar, R. B., & Anandharaj, K. (2016). Assessment of Bacterial Load in the Fresh Water Lake System of Tamil Nadu. Interl J Curr Microbiol App Sci, 5(6), 236-246.
26. Rengarajan, R. S. A. (2016). Secure verification technique for defending IP spoofing attacks.

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

|Volume 4, Issue 6, November - December 2020|

DOI:10.15680/IRJIE.2020.0406001

27. Mathew, A. R., & Al Hajj, A. (2017). Secure communications on IoT and big data. Indian Journal of Science and Technology, 10(11).
28. Alex, A. T., Asari, V. K., & Mathew, A. (2012, October). Gradient feature matching for expression invariant face recognition using single reference image. In 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 851-856). IEEE.
29. Sasidevi, J., Sugumar, R., & Priya, P. S. (2015). New-Multi-Phase Distribution Network Intrusion Detection. International Journal, 5(3).
30. Mathew, A., & Asari, V. K. (2013, March). Tracking small targets in wide area motion imagery data. In Video Surveillance and Transportation Imaging Applications (Vol. 8663, pp. 69-78). SPIE.
31. 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.
32. Alex, A. T., Asari, V. K., & Mathew, A. (2013, March). Gradient feature matching for in-plane rotation invariant face sketch recognition. In Image Processing: Machine Vision Applications VI (Vol. 8661, pp. 46-58). SPIE.
33. Natarajan, R., & Sugumar, R. (2014). A survey on attacks in web usage mining. International Journal of Innovative Research in Computer and Communication Engineering, 2(5), 4470-5.
34. Satyanarayana, D., Mathew, A. R., & Sathyashree, S. (2016). An Architecture for Wireless Communication Systems using Li-Fi technology. In 8th International Conference on Latest Trends in Engineering and Technology (ICLTET'2016) (pp. 37-41).
35. Mathew, A. R. (2017). Cloud Technology and the Challenges for Forensics Investigators. DEStech Transactions on Computer Science and Engineering.
36. Begum, R. S., & Sugumar, R. (2015). A Conceptual Comparison of Artificial Bee Colony and Particle Swarm Optimization.
37. Soundappan, S. J., & Sugumar, R. (2016). Optimal knowledge extraction technique based on hybridisation of improved artificial bee colony algorithm and cuckoo search algorithm. International Journal of Business Intelligence and Data Mining, 11(4), 338-356.
38. 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.
39. Sugumar, R., Rengarajan, A., & Jayakumar, C. (2018). Trust based authentication technique for cluster based vehicular ad hoc networks (VANET). Wireless Networks, 24(2), 373-382.
40. 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.
41. Priya, P. S., & Sugumar, R. (2014). Multi Keyword Searching Techniques over Encrypted Cloud Data. In IJSR.
42. 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.
43. 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.
44. Sugumar, R. (2014). A technique to stock market prediction using fuzzy clustering and artificial neural networks.
45. 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.
46. Z. Brijet, N. Bharathi, G. Shanmugapriya. (2015). Design of Model Predictive Controller for Fluid Catalytic Cracking Unit. Fluid-IJCTA, 8(5), 1917-1926.