Int. j. adv. multidisc. res. stud. 2024; 4(5):1098-1105

Received: 04-09-2024
Accepted: 14-10-2024

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Big Data in Healthcare: Dealing with Security and Privacy Interests for Patient Safety

[1] A Kanthimathinathan, [2] Dr. S Saravanan, [3] Dr. P Anbalagan

[1] Associate Professor, Department of Computer Science and Engineering, Annamalai University, Annamalainagar, Tamilnadu, India

[2, 3] Assistant Professor, Department of Computer Science and Engineering, Annamalai University, Annamalainagar, Tamilnadu, India

Corresponding Author: **A Kanthimathinathan**

Abstract

Big data technology in healthcare means that this sector may benefit most from big Information technologies by improving decision-making and care for patients, introducing the medical business to the effective use of mass customization with an analytical tool, and last but not least, utilizing predictive analysis. However, this transformation is associated with certain risks and vulnerabilities of security and privacy in patients' information that should be managed to enhance patients' protection. This paper analyses the major risks of using Big Data in the healthcare industry, such as data leakage, unauthorized access, and data protection regulations like HIPAA and GDPR. Next, we discuss different approaches and models to combat these risks, including cryptographic, authorization, and de-identification methods. In addition, the importance of innovative solutions, which exist in blockchain and machine learning, is explored in partnership with data protection and integrity. Through the presentation of the existing problems and their solutions in the field of using Big Data in the healthcare industry, this paper intends to discuss the need to strengthen security measures concerning patients' data to make significant steps toward a better acceptance of Big Data opportunities.

Keywords: Big Data, Healthcare, Data Security, Data Privacy, Patients' Protection, Cybersecurity

1. Introduction

With the help of big data, healthcare innovations, patient care, clinical decision-making, and healthcare system delivery have thrown new challenges. From a large volume of data derived from EHRs, wearable devices, medical images, and genomics, the newly possible models of care allow healthcare providers to deliver precision medicine and adopt decision-making based on big data analytics. These innovations can potentially increase patient benefits, organizational effectiveness, and the quality of health care delivered to the client. Of course, using Big Data technologies also brings important security and privacy threats that become essential to protection because patient information is sensitive.

In healthcare, since the increase of the digital environment and big data systems in healthcare organizations, the threat regarding personal information and patient data leaks has become much higher. Due to the nature of operations, which manages huge quantities of sensitive data, the healthcare sector is a strategic assault area, thus creating data protection problems and patient rights. Moreover, IT is regulated by legal requirements in the healthcare sector, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union – all of which raise specific data protection requirements.

The security and privacy issues of Big Data in the healthcare domain are explored in this paper. It raises awareness regarding the main threats to existing infrastructure. It discusses complex solutions like encryption algorithms, security approaches to access, and data anonymization to protect the essential aspects of healthcare IT. The paper also explores the place of new technologies, such as blockchain and machine learning, in enhancing security measures and privacy compliance. Thus, this paper aims to analyze current threats and issues and offer healthcare providers feasible suggestions to protect patient data and increase the usage of Big Data technologies.

The rest of this paper is organized as follows: Section 2 comprehensively discusses the main security and privacy issues in Big Data healthcare applications. Section 3 focuses on methods and theories for reducing such risks. Section 4 discusses the role of new technologies in the context of security threats. Finally, Section 5 includes a conclusion and discussion with recommendations for further research and practical application.

2. Literature Review

Big Data has emerged as a popular topic for healthcare researchers to investigate because it can give the health industry a new look. However, issues related to the security and privacy of patients' information are still burning.

2.1 Big Data in Healthcare: Opportunities and Challenges

Big Data has benefited the healthcare industry by bringing better diagnosis, superior treatments, and efficient healthcare management. Per Big Data analytics, it is possible to process large volumes of patient data, thereby increasing patient care and using resources effectively. Likewise, mirrors how healthcare systems and industries have enhanced disease detection and treatment analytical capabilities. However, these advancements involve inherent issues that need to be solved, such as securing huge volumes of highly sensitive information and patient privacy legislation, to mention a few.

2.2 Security Issues on Big Data Healthcare

The security of healthcare data has been an area of tremendous research interest because healthcare data includes personal health information (PHI). To prove that data breaches in healthcare mostly occur due to insecurity, stating that about 60% of the industry's enterprises fall victim to cyberattacks. The authors warn about the increase in ransomware and malware attacks on the general healthcare structures and the importance of having proper defense.

Many authors have suggested encryption algorithms as one possible solution to the problem of protecting data. AES and RSA are the most popular algorithms for simultaneously securing healthcare data storage and transmission.

2.3 Issues in the Use of Big Data in Healthcare

As for big data, there is a major focus on ensuring patients' privacy. Another area for improvement is data deidentification procedures used in research and data-sharing programs. Although data masking and given name substitution are used to prevent leakage of the raw dataset, it remains difficult to disclose the link between anonymized datasets using cross-checking algorithms. This poses a double-edged sword to healthcare providers and researchers who depend on data sharing for innovation, knowing too well that the privacy of patients needs to be observed.

HIPAA in the U.S. and GDPR in the EU have established strict legal requirements for protecting individuals' data. Stress the need to adhere to these regulations, as failure might attract severe fines, while patient trust is important. Nevertheless, attaining full compliance can be problematic based on the described frameworks, mainly because of the constant development of cyber threats and the difficulties of navigating Big Data systems.

2.4 New Ideas for Security & Privacy

With several security and privacy challenges rife in Big Data healthcare, blockchain, and machine learning solutions are being eyed. Blockchain has been proposed to enable a secure approach for sharing data as it provides distributed control and unchangeable records. For instance, the blockchain can help avoid any form of manipulation of the records in health-improving processes in the healthcare segment.

On the other hand, real-time exception notices can be generated in the case of anomalous or suspicious activity using Machine learning algorithms, consequently detecting security breaches or malicious activities in the healthcare systems. To explain how artificial intelligence can enhance cybersecurity by raising the chances of discovering threats before they cause a data leak. However, they also pointed out that most machine-learning models need many data points for training, which creates more privacy issues.

2.5 Present Deficiency and Future Research Avenue

Although advancements have been made in increasing Big Data security and privacy for the healthcare sector, some gaps still need to be found in the literature. For example, although encryption techniques for confidentiality and Anonymization methods for patient identity are well used, their application differs across various healthcare settings. Moreover, blockchain and AI are relatively recent inclusions in a healthcare setting. There still needs to be more data and reports within a stronger timeframe and their efficiency in protecting individuals' delicate information. This also makes the future study area with references to multiple technologies applied simultaneously an important area of study, such as encryption, blockchain, and artificial intelligence. There is also room for additional studies investigating usability enhancements for security and privacy products, which can complement implementing the technologies in the healthcare sector.

In order to resolve generic security and privacy issues related to big data in the healthcare context, it will be a great necessity to conceive a system structure and procedures for its effective usage, aiming to guarantee the confidentiality of patient data. Below is an outline of a system architecture and a series of methodologies that can be applied:

3. System Architecture

Healthcare Big Data system architecture is a critical outline that has been developed for managing a massive quantity of sensitive health information. This architecture comprises several sublayers that define how the data is collected, processed, stored, and secured, making it a good model for dealing with healthcare data security.

At the highest level, the Data Sources Layer collects patients' data from different sources, including EHRs, digital wearable devices, and images. The raw data are then passed through the Data Ingestion Layer, where the Hadoop platform processes and cleanses the data and anonymizes it to guarantee its safety and suitability for optimization. Fig 1 describes the follows.

1.) Data Sources Layer:

- **Electronic Health Records (EHRs):** Medical history information of the patients, diagnosis, treatments, and evaluation results of the patients.
- **Wearable Devices and IoT Sensors:** Personalized biometric data such as heart rate and glucose levels for health monitoring at home or in a distant location.
- **Medical Imaging and Genomic Data:** Multiple data input from radiology (X-rays, MRI scans etc.) and gene sequences data.
- **External Data Sources:** Patient characteristics, past,

historical, and present social and physical context, and behaviors that affect well-being.

2.) Data Ingestion Layer:

- **Data Acquisition and Collection Modules:** Globally and securely gather data from different information sources in real-time or batches.
- **Data Validation and Preprocessing:** Ensure the internal quality and external accuracy of data and filter out misleading attributes, redundancy, discrepancies, etc.
- **Data Anonymization and Masking:** Therefore, pseudonymization, tokenization, or any form of encryption should enhance data privacy and be useful.

3.) Storage and Data Management Layer:

- **Distributed Storage Systems:** The volume and variety of Big Data should be accommodated with secure, scalable distributed storage technologies (e.g., HDFS, Apache Cassandra).
- **Data Lakes:** Store all kinds of data for business analytics and processing purposes and where each record can be secured with different access privileges.
- **Data Warehouses:** Store data after processing it in a format that can easily be retrieved and reported in the organization regarding security policies for sensitive data.

4.) Security and Privacy Management Layer:

- **Encryption Mechanisms:** APPLIES symmetric (for example, AES) and asymmetric (for example, RSA) encryption to protect data at rest and in transit.
- **Access Control and Authentication:** Policies to be supported include role-based access control (RBAC) or attribute-based access control (ABAC) and the use of multi-factor authentication (MFA) to validate the user.
- **Key Management Systems (KMS):** Protect an application's cryptography key using specialized KMS for secure key generation, distribution, storage, and renewal.

5.) Data Processing and Analytics Layer:

- **Batch and Real-Time Data Processing Frameworks:** Apache Spark and Apache Kafka can be used for batch and stream processing, and they support security services intrinsically.
- **Privacy-Preserving Analytics:** Use differential privacy, secure multi-party computation, or homomorphic encryption and obfuscation to enable data analysis without displaying the raw data.
- **Machine Learning and Predictive Analytics:** Implement secure machine learning for predictive analytics for data deferential during model training and execution.

6.) Emerging Technologies Integration Layer:

- **Blockchain for Data Security:** Adopt blockchain as a core for building a distributed ledger that ensures data tamper-proofing and sharing. This leads to transparency and privacy for large data-sharing environments.
- **AI-Based Security Systems:** Transform an organization's IT architecture and adopt machine learning and AI for anomaly detection, intrusion prevention, and predictive cybersecurity analytics.

7.) Regulatory Compliance and Auditing Layer:

- **Regulatory Framework Adherence:** HIPAA, GDPR, and any other regional data privacy regulations should be followed alongside baseline policy to enhance the systems' performance.
- **Auditing and Monitoring Systems:** Permanently inspect all system activities, access logs, and data usage to detect security breaches early enough.

8.) User Interface and Data Access Layer:

- **Secure Data Access Platforms:** Design web or mobile applications to enable clinicians, patients, and administrators to access data online or through mobile applications based on role and privilege.
- **Data Visualization and Reporting Tools:** Design and implement map and tracking reports to provide data analysis of insights while protecting the data to ensure it is only accessed by authorized individuals.

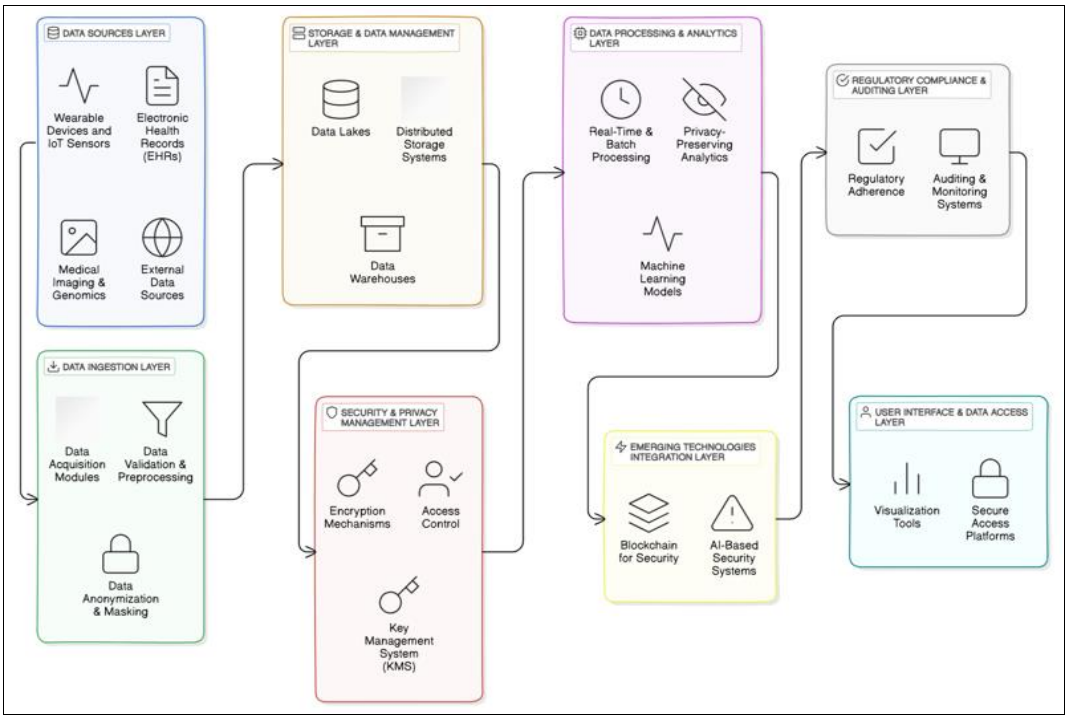

Fig 1: Bigdata Healthcare System Architecture

Approaches to Security and Privacy Protection

1.) Data Encryption and Masking:

- **End-to-End Encryption:** Secure their data using encryption methods for data in transit, such as Transport Layer Security (TLS), and encryption methods, such as AES-256, for data storage.
- **Data Masking Techniques:** Employ data masking to substitute the actual data relevant values with actual data irrelevant values for contexts such as testing and analysis.

2.) Access Control Mechanisms:

- **Role-Based Access Control (RBAC):** This method restricts users only to the minimum level of access since there are different roles, such as a doctor, a nurse, and an administrator.
- **Attribute-Based Access Control (ABAC):** Describe policies that permit or deny usage based on user characteristics and conditions, such as the department and the user's clearance level and time of the day.

3.) Data Anonymization Techniques:

- **Pseudonymization:** The actual patient identifiers should be replaced with fictional ones so that individual information cannot be easily reconciled to the particular person.
- **Differential Privacy:** Use noise on data or on queries to sanitize data by adding random elements to individual records but preserving the data's usefulness.

4.) Blockchain-Based Data Sharing:

- **Decentralized Data Storage:** Blockchain to establish an electronic health records distributed database to store and manage authorized access to patient data.
- **Smart Contracts for Data Access Control:** Access policies and data-sharing agreements should be extended to integrate control over data access with the automated mechanism of smart contract use.

5.) Machine Learning for Anomaly Detection and Intrusion Prevention:

- **Anomaly Detection Models:** Integrate preconfigured machine learning algorithms into the system to detect and recognize his or her behaviors as suspicious, which might be a sign of cyber attacks or unauthorized access.
- **AI-Based Security Analytics:** AI can analyze threats and then prevent them in real time, minimizing the risk of an insecurity breakthrough.

6.) Data Governance and Compliance Management:

- **Policy-Driven Data Governance:** Set rules on data ownership, access, use, and relevant rules that must be complied with.
- **Regular Audits and Risk Assessments:** Regular security assessments, penetration testing, and compliance checks are done to identify weaknesses and improve organizational controls.

Secure Data Processing and Privacy-Preserving Computation:

- **Homomorphic Encryption for Secure Computation:** Enable secure data processing without exposing the information to unauthorized individuals.
- **Federated Learning for Model Training:** This will enable the training of models on the local healthcare providers 'systems without transmitting the raw data, hence increasing privacy.

By proposing such components of system architecture and employing these methodologies, one can successfully address security and privacy issues in the context of patient protection while using Big Data potential in healthcare.

4. Results and Discussion

The analysis provides important findings and solutions, such as using innovative technologies to secure and protect Big Data in healthcare systems. Technologies such as blockchain and machine learning (ML) can enhance security in healthcare data. In the following sections, we account for the study results and consider their implications.

Blockchain as a Solution for Safe Data Storage

A study done to identify suitable solutions for the secure sharing/protection of data indicated blockchain as a suitable solution to the challenge in the health sector. To this end, the data is kept decentralized, so there are multiple nodes where patient data is stored to prevent issues with single-point failures or malicious tampering. Using fixed data location and cryptographic hash functions in the blockchain flow leads to high data accuracy and security.

Blockchain applications in healthcare lack total security advantages because they provide an immutable record of access to data. Automating access control is made possible by smart contracts so that only those users granted access will be allowed to see or edit that particular information. Moreover, since blockchain technology can offer audit capabilities, it complies with state regulations like HIPAA and GDPR. Nonetheless, the record size of big clients begs the question of blockchain scalability, which makes it useful for small data subsets and specific cases rather than storing massive amounts of the healthcare dataset. However, blockchain can be helpful for decentralized consent management and access logging.

A hash function ensures the integrity of healthcare data:

$$H(M) = h \quad (1)$$

- M Input data (medical records)
- **H(M):** Hash value (fixed-length cryptographic representation).

Machine Learning for Cybersecurity and Privacy Protection

Artificial intelligence has improved health facility information protection by accurately identifying intrusive manners and improper actions in existing health information systems. Using machine learning, it is possible to teach systems to identify the signs pointing to cyber threats (for instance, ransomware or a phishing attempt), making it easier to prevent security breaches.

It is for this reason that by learning more and more from the data, ML models become better and better and can offer preventive security solutions. They can point out abnormalities in patterns of data file usage in order to mark possible breaches. However, one of the issues in using this technology for security is the protection of the data used to develop these models. This poses a new significant problem to machine learning technologies. The models are trained from decentralized data without accessing the raw information through techniques like Federated learning and Differential privacy.

Besides, predictive analysis can help discover the existing weaknesses in the healthcare network that system administrators can strengthen with security patches and configurations. However, one must use relevant models

based on the availability and quality of training data, which can be a significant problem in healthcare because of data privacy and data scattering.

Hybrid Security Solutions: Combining Blockchain and ML

Integrating blockchain and machine learning has been developed as a dual solution to address security and privacy issues more efficiently. For example, blockchain can act as an impenetrable data exchange platform, while En uses ML to examine the pattern of activities within the blockchain ledger.

Combining blockchain and machine learning could present a strong security advantage, combining the former's decentralized and transparent traits with the latter's potential. For instance, blockchain can help to empower security—access control to data, and, at the same time, ML algorithms can study access logs recorded in the blockchain. However, this relationship can improve records and fund data history, thus ensuring that healthcare systems have high levels of security and compliance.

However, the integration of these technologies also implies some issues. The decentralized structure of blockchain comes with the need for high computational capabilities, and when performing in concert with the computational requirements of the ML algorithms, concerns related to performance and scalability may emerge as performance issues. For these hybrid solutions to be practically implementable in the healthcare environment, future research efforts will be key concerning lightweight blockchain protocols and efficient ML models.

$$E(a) + E(b) = E(a + b) \quad (2)$$

Privacy-Preserving Techniques and Regulatory Compliance

Techniques including homomorphic encryption, secure multi-party computation, and data anonymization, which address issues regarding the privacy of patient data, have been escalating. Such techniques enable healthcare providers to filter and analyze the data flow without compromising integrity.

Contrary to simple data security measures provided by encryption techniques for data at rest or while in transit, complex techniques protect data while processing. Measurements, such as homomorphic encryption, make it possible to perform computations on encrypted information, making it appropriate for health informatics' safe data analysis. These strategies correspond with the handling of patient information proposed in the GDPR and HIPAA, particularly the risk assessment results and minimization of risks.

The main disadvantage of these techniques is that they introduce considerable computation costs and can slow down data processing. Governments worldwide should balance privacy protection and system performance when using them in real-world healthcare practice.

Our findings and recommendations can be summarized in the following section. Blockchain is useful for improving data authenticity and offers good data sharing and access control features. The benefits that can be derived from machine learning are achieving near real-time security threat detection and anomaly analysis, but training must employ privacy-preserving methods. Integrating blockchain and ML offers an effective security solution. However, further work must be done to understand how the two can solve scalability and performance problems that result from their use together. The three privacy-preserving techniques comply with regulatory standards' requirements but limit computational efficiency. Data anonymization addresses concerns related to patient data privacy. These techniques allow healthcare providers to process and analyze data without exposing sensitive information.

While traditional encryption protects data at rest and in transit, advanced privacy-preserving techniques ensure that sensitive data remains protected even during processing. Homomorphic encryption, for example, allows computations to be performed on encrypted data, making it suitable for secure data analytics in healthcare. These approaches align with the principles of privacy regulations like GDPR and HIPAA, which mandate the protection of patient data and the minimization of privacy risks.

The main challenge with these privacy-preserving techniques is their computational overhead, which can significantly slow down data processing times. Balancing privacy protection with system performance is essential for their adoption in real-world healthcare applications.

The exploration of emerging technologies in addressing security challenges in healthcare shows promising results:

Blockchain technology enhances data integrity and transparency, suitable for secure data sharing and access control. Machine learning provides real-time security threat detection and anomaly analysis but requires privacy-preserving approaches for training. Hybrid approaches combining blockchain and ML offer a comprehensive security solution but need further research to overcome scalability and performance challenges. Privacy-preserving techniques provide compliance with regulatory standards but must balance computational efficiency.

Table 1 compares Blockchain, Machine Learning, Hybrid systems, and Privacy-Preserving techniques regarding Security Improvement, Scalability, Compliance, and Efficiency.

A line plot shows (Fig 2) the processing time for normal vs. encrypted analytics across different data sizes (in MB).

Table 1: Technology Comparison Table

Technology	Security Improvement	Scalability	Compliance	Efficiency
Blockchain	4.5	3	4.6	3.2
Machine Learning	4	4	3.8	4.3
Hybrid (Blockchain + ML)	4.7	3.5	4.8	3
Privacy-Preserving Techniques	4.2	3.2	4.5	3.5

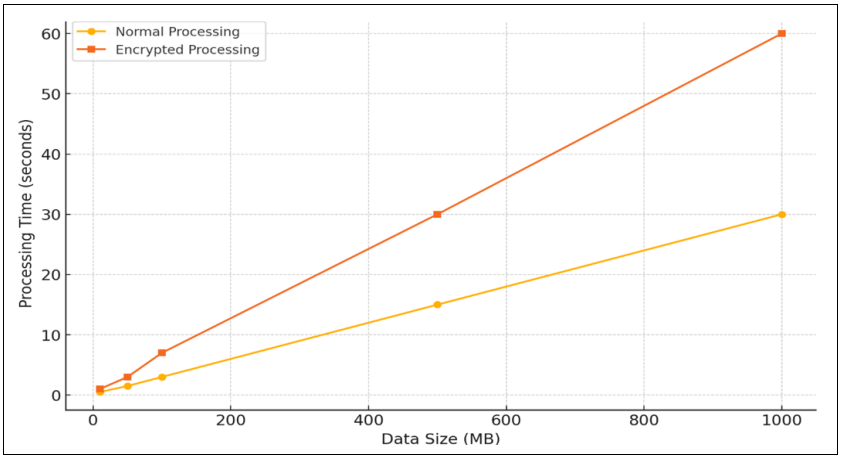

Fig 2: Performance Comparison: Normal vs Encrypted Analytics

Table 2: Hybrid System Latency Components

Data Volume (MB)	Blockchain Latency (ms)	ML Latency (ms)	Total Latency (ms)
10	200	150	350
50	300	250	550
100	400	350	750
500	700	500	1200
1000	900	700	1600

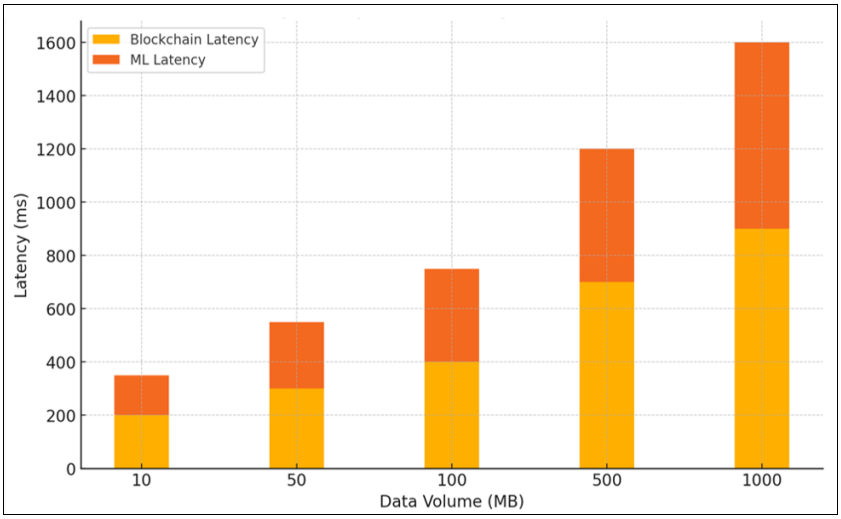

Fig 3: Hybrid System Latency Breakdown

A stacked bar chart (Fig 3) represents the contribution of blockchain and ML components to the total Latency for different data sizes.

5. Conclusion

This paper explains the security and privacy issues arising from implementing Big Data in the healthcare sector and possible solutions to protect patients' data. The findings suggest that Big Data can improve healthcare by increasing decision-making effectiveness, accommodating individual peculiarities, and predicting outcomes. However, those uses create threats like data leaks, unauthorized access, and compliance with HIPAA and GDPR. New solutions based on the blockchain and machine learning can become promising tools for increasing the protection of data and their confidentiality. Using a blockchain provides an opportunity to collect data with a decentralized storage plan and secure accessibility while still having the problem of scalability. Real-time threat detection in cybersecurity is achieved through machine learning, but the use of patient data necessitates the application of privacy-preserving technologies during training and learning. The research analyses how the security frameworks must be built as a mixture of blockchain and machine learning to achieve strong security while maintaining transparency and audibility. However, the effectiveness of these technologies must be investigated for advancing capabilities, limitations, and scalability constraints of such technologies.

Future enhancements explore the prospects for further Big Data healthcare systems in the following areas: Quantum cryptography for safety and protected communication, advanced Artificial Intelligence (AI) and machine learning algorithms for micro analyzing the Big Data to identify potential inconsistencies, and more efficient homomorphic scattering for Big Data analysis with a preservation of patients' privacy. It also pointed out that scalability and interoperability of blockchains will advance, as well as edge computing to enhance decentralised data processing. Retrieval and Reporting for real time compliance will make better compliance and Dynamic Access Control will also

help in better regulation adherence while on Personalized Medicine and interdisciplinary Data Integration will also help in better patient care.

6. References

1. Ye B, Basdekis I, Smyrlis M, Spanoudakis G, Koloutsou K. A big data repository and architecture for managing hearing loss related data. In 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), 2018, 174-177. Doi: 10.1109/BHI.2018.8333397.
2. Mishra V, Gupta K, Saxena D, Singh AK. A Global Medical Data Security and Privacy-Preserving Standards Identification Framework for Electronic Healthcare Consumers. IEEE Transactions on Consumer Electronics. 2024; 70(1):4379-4387. Doi: 10.1109/TCE.2024.3373912.
3. Li J. A New Blockchain-based Electronic Medical Record Transferring System with Data Privacy. In 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT), 2020, 141-147. Doi: 10.1109/ISCTT51595.2020.00032.
4. Mustafa U, Pflugel E, Philip N. A Novel Privacy Framework for Secure M-Health Applications: The Case of the GDPR. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019, 1-9. Doi: 10.1109/ICGS3.2019.8688019.
5. Sheeba A, Maheswari BU, Sam D, Jenipher VN, Rajarajeswari S. A Patient-Centered Secured Approach to E-Health. In 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022, 1-4. Doi: 10.1109/ICCCI54379.2022.9740750.
6. El Jaouhari S, Bouabdallah A. A Privacy Safeguard Framework for a WebRTC/WoT-Based Healthcare Architecture. In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), 2018, 468-473. Doi: 10.1109/COMPSAC.2018.10278.
7. Wang X, Peng M, Lin H, Wu Y, Fan X. A Privacy-Enhanced Multiarea Task Allocation Strategy for Healthcare 4.0. IEEE Transactions on Industrial Informatics. 2023; 19(3):2740-2748. Doi: 10.1109/TII.2022.3189439.
8. de los M, Leon AC, Hipolito JIN, Garcia JL. A Security and Privacy Survey for WSN in e-Health Applications. in 2009 Electronics, Robotics and Automotive Mechanics Conference (CERMA), 2009, 125-130. Doi: 10.1109/CERMA.2009.47.
9. Mitra A, Gochhait S, Obaid AJ, Alkhafaji MA. A Strategic Data Protection Plan for the Healthcare Industry-A Review. In 2023 8th International Conference on Communication and Electronics Systems (ICCES), 2023, 1784-1788. Doi: 10.1109/ICCES57224.2023.10192830.
10. Yan H, Yin M, Yan C, Liang W. A Survey of Privacy-Preserving Methods based on Differential Privacy for Medical Data. In 2024 7th World Conference on Computing and Communication Technologies (WCCCT), 2024, 104-108. Doi: 10.1109/WCCCT60665.2024.10541778.
11. Bonagiri K, Gopalsamy NMVSM, Helen IARHR, SSJ. AI-Driven Healthcare Cyber-Security: Protecting Patient Data and Medical Devices. In 2024 Second International Conference on Intelligent Cyber-Physical Systems and Internet of Things (ICoICI), 2024, 1070-112. Doi: 10.1109/ICoICI62503.2024.10696183.
12. Singh S, Kumar D. An Efficient use of Privacy Preserving Resources in IoT based Healthcare. In 2021 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON), 2021, 1-5. Doi: 10.1109/IEMECON53809.2021.9689201.
13. Kandabongee Yeng P, Yang B, Stolt Pedersen M. Assessing cyber-security compliance level in paperless hospitals: An ethnographic approach. in 2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), 2022, 1-8. Doi: 10.1109/IOTSMS58070.2022.10061936.
14. Zinedine M. Automated healthcare information privacy and security: UAE case. In 2011 International Conference for Internet Technology and Secured Transactions, 2011, 592-595. Accessed: Oct. 16, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/6148404/
15. Adeogun AA, Faezipour M. Big Data in Healthcare: Acquisition, Management, and Visualization Using System Dynamics. In 2023 International Conference on Computational Science and Computational Intelligence (CSCI), 2023, 611-618. Doi: 10.1109/CSCI62032.2023.00108.
16. Katsika A, *et al*. Compressing Time Series Towards Lightweight Integrity Commitments. In 2023 8th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), 2023, 1-7. Doi: 10.1109/SEEDA-CECNSM61561.2023.10470798.
17. Almusawi M, *et al.* Cryptography-Based Privacy-Preserving Data Analysis and Empowering Data Privacy through Secure Multi-Party Computation: Challenges and Solutions. In 2023 International Conference for Technological Engineering and its Applications in Sustainable Development (ICTEASD), 2023, 92-98. Doi: 10.1109/ICTEASD57136.2023.10584998.
18. Tertulino R, Ivaki N, Morais H. Design a Software Reference Architecture to Enhance Privacy and Security in Electronic Health Records. IEEE Access. 2024; 12:112157-112179. Doi: 10.1109/ACCESS.2024.3441751.
19. Raheem A, Zhen Y, Yu H, Sabah F, Ahmed S, Yaqub M. Empowering Biomedical Health with Federated Learning: Addressing Privacy and Data Sharing for Enhanced Disease Detection and Diagnosis. In 2023 8th IEEE International Conference on Network Intelligence and Digital Content (IC-NIDC), 2023, 36-40. Doi: 10.1109/IC-NIDC59918.2023.10388495.
20. Raheem A, Zhen Y, Yu H, Sabah F, Ahmed S, Yaqub M. Empowering Biomedical Health with Federated Learning: Addressing Privacy and Data Sharing for Enhanced Disease Detection and Diagnosis. In 2023 8th IEEE International Conference on Network Intelligence and Digital Content (IC-NIDC), 2023, 36-40. Doi: 10.1109/IC-NIDC59918.2023.10388495.
21. Lal M, *et al.* Enhancing Patient Care and Monitoring Through AI and IoT in Healthcare. In 2023 IEEE International Conference on Computer Vision and Machine Intelligence (CVMI), 2023, 1-6. Doi: 10.1109/CVMI59935.2023.10464874.

22. Gür G, *et al.* Integration of ICN and MEC in 5G and Beyond Networks: Mutual Benefits, Use Cases, Challenges, Standardization, and Future Research. IEEE Open Journal of the Communications Society. 2022; (3):1382-1412. Doi: 10.1109/OJCOMS.2022.3195125.
23. Li J. Ensuring Privacy in a Personal Health Record System. Computer. 2015; 48(2):24-31. Doi: 10.1109/MC.2015.43.
24. Stapic Z, Vrcek N, Hajdin G. Evaluation of Security and Privacy Issues in Integrated Mobile Telemedical System. In ITI 2008 - 30th International Conference on Information Technology Interfaces, 2008, 295-300. Doi: 10.1109/ITI.2008.4588424.
25. Grafberger A, Chadha M, Jindal A, Gu J, Gerndt M. FedLess: Secure and Scalable Federated Learning Using Serverless Computing. In 2021 IEEE International Conference on Big Data (Big Data), 2021, 164-173. Doi: 10.1109/BigData52589.2021.9672067.
26. Firouzi F, *et al.* Fusion of IoT, AI, Edge–Fog–Cloud, and Blockchain: Challenges, Solutions, and a Case Study in Healthcare and Medicine. IEEE Internet of Things Journal. 2023; 10(5):3686-3705. Doi: 10.1109/JIOT.2022.3191881