BIG HEALTHCARE DATA: ENHANCING SECURITY AND PRIVACY

Ali Hasan Kamil, Southern Technical University

ABSTRACT

Big data refers to the process of collecting, storing, processing, and turning data into something useful by using new tools and techniques. Big data allows businesses to monitor trends and recognize patterns, both of which can assist them in making better decisions for their companies. Large amounts of data are called "big data," Its defining characteristics include colossal velocities, wide variety, extensive ranges, useable value, and veracity. The fields of retail, customer service, healthcare, electronic commerce, marketing, finance, transportation, and logistics are just a few of the significant arenas in which big data can be applied. Big data analytics can provide many organizations, particularly those in the healthcare industry, with valuable new perspectives. Big data has the best potential to enhance consumer experiences, get important insights, predict disease outbreaks, prevent preventable diseases, and save healthcare costs. Despite these challenges, the healthcare business needs to must big data due to a lack of need for staff, IT infrastructure, and data privacy laws. Because health data is always changing, processing and analyzing it can be fraught with various issues on a conceptual, technical, legal, and ethical level. As one of the most pressing issues today, big data in the healthcare industry has assumed an increasingly significant role in recent years. The challenges posed by big data in the healthcare industry are examined in this research. I also provide a comprehensive healthcare data lifecycle that includes protection against breaches and threats. As a consequence of this, i will be able to come up with rules and systems that take into account every security concern. This study also proposes novel methods for authenticating users, encrypting data, maintaining anonymity, controlling access, and maintaining privacy. The most important contribution is a security threat model for the lifecycle of large amounts of healthcare data.

Keywords: Bigdata, Health Care Data, Bigdata Security and Privacy.

INTRODUCTION

The field of medicine, which counts as one of the commercial industries, will see big data take on an increasingly important function in the coming years. Big data is a term that describes a huge quantity of content that cannot be stored, addressed, or transformed into value by applying the techniques that have been used in the past. The growing popularity of the Internet and the computerized storage of different kinds of content, including health records, have all contributed to *"big data."* It has the potential to become a useful instrument for the personalization of medical treatment, which has the potential to save and improve lives, reduce waste, and provide superior medical care. When analyzing and using these datasets in clinical practice, many obstacles exist to overcome. Big data lets us condense and study these digital hidden treasures to discover trends and make predictions. Big data and mobile technologies can accelerate medical knowledge expansion, especially mobile devices, detectors, and wearable technology. Medical professionals' continuous and preventative monitoring of an individual's

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

health enables them to be notified immediately of any potential issues (UNDP, 2019). Constant monitoring of a person's health provides many obvious benefits. Still, it also puts them at a greater risk of harm because sensors are vulnerable to flaws and attacks from hackers. This puts them in a potentially life-threatening situation. Because of privacy and security issues, big data needs to play catch-up in the medical and healthcare industries. Due to this uncertainty, the use of more modern analytical technology within the healthcare industry needs to be improved. Maintaining patients' privacy is one of the most difficult difficulties when implementing big data in healthcare. Patients and healthcare providers alike are interested in learning who will have access to their data and what will be done with it. Establishing and refining federal laws that regulate the use of data is a necessary step in attracting additional investment in data-driven medical systems. In addition, the healthcare industry pointed out that a proactive, top-down, privacy- and security-centered strategy is required rather than a reactive, bottom-up one to safeguard patients and the business adequately (Pramanik et al., 2020). Hence, healthcare organizations need to take inventive, preventive, and proactive steps to prevent breaches and other security issues so that big data may be utilized more efficiently and quickly. This study addresses significant threats to health data security and discusses some intriguing related studies. I also go through some more recent technological developments that can help lessen such hazards. I focus my attention on the problem of protecting patients' privacy when it comes to big data in the healthcare industry, and I do so by citing several rules and guidelines issued by a variety of regulatory agencies as well as by providing an overview of some effective techniques. After that, I will cover some suggested approaches and processes documented in the scientific community to address security and privacy threats in the medical services sector. At the same time, I will highlight the limitations of these strategies and procedures as I go through the discussion.

Issues with Privacy and Security in Big Data

Big data confidentiality and user privacy protection are significant issues. One definition of privacy is "the state of not being seen," which is widely understood to mean *"the capacity to secure sensitive information impacting individually identifiable health information."* It emphasizes using and exercising control over persons' data, such as by formulating guidelines and establishing criteria for authorization, to ensure that patient information collection, sharing, and utilization is carried out appropriately. Security is typically defined as preventing unwanted access, even though availability and integrity are occasionally mentioned explicitly (Demirdogen et al., 2023).The primary goal is to prevent criminal activity and info loss to earn money.

Big Healthcare Data Security

Although healthcare firms store, keep and transfer vast volumes of data to facilitate the provision of effective and appropriate treatment, one of the disadvantages is the requirement for additional technical help and suitable protection. The reality that the healthcare business remains one of the most at risk of data breaches being revealed to the general public makes things more difficult. In actuality, data breaches can be caused by attackers who use data mining techniques to find sensitive information and then disclose it to the general public, which results in the breach. Even though putting security measures in place is still tough, the risks are increasing

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

because it is getting harder to get around security safeguards. Therefore, organizations must develop healthcare information security systems that protect critical resources, align the critical resources, align with critical resources, and align with statutory obligations imposed on the sector (Thirunavukarasu et al., 2022). One school of thought contends that "security in big data" describes data security, regulating access and system protection simultaneously. This is about the protection of personal information and other sensitive data. In this environment, healthcare companies need to develop cybersecurity measures and policies that protect their big data, linked software and hardware, and medical and administrative information from threats that originate from both within the company and outside the organization. These attacks can come from either inside the company or outside the company. To ensure that the necessary decisions are taken regarding the auditing, cost efficiency, reuse, and preservation of new or old data, the data lifecycle needs to be defined at the beginning of a project (Abouelmehdi et al., 2017). This framework considers the vulnerabilities of big data settings at different stages of the big data lifecycle. It also explores the big data lifecycle from the perspectives of the data provider, the data collector, the data miner, and the decision maker. The four interrelated phases of the paradigm described in Chen et al. (2020) were known as the gathering of data, the storage of data, the processing and analysis of data, and the development of knowledge. This model of a lifetime is always being improved, with the primary emphasis being placed on continual attention and continuous monitoring. To establish guidelines and processes that make sure handling of threats and assaults in each step of the big data life cycle, it is recommended to present a model which integrates the phases that are described in Cuzzocrea et al. (2022) with the phases that are mentioned in Hassan et al. (2021) and Yang et al. (2018) respectively. The following are the primary aspects that make up the big data lifecycle in the healthcare industry, shown in Figure 1.

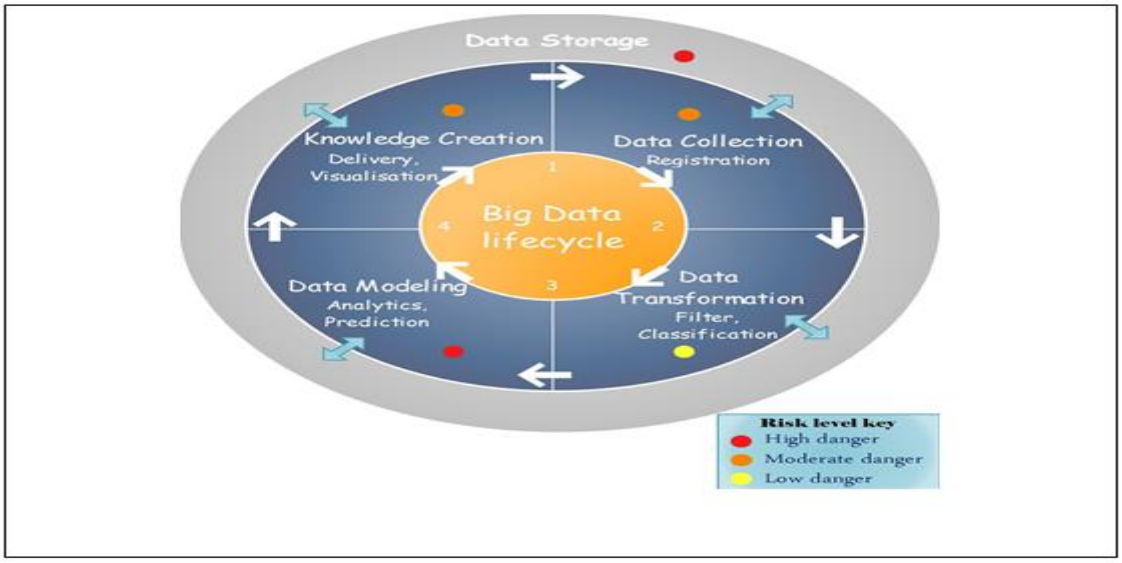

FIGURE 1
SECURITY FOR BIG DATA HEALTHCARE LIFE CYCLE

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

The phase of data collection: the first thing that should be done is this. It requires collecting data from various sources and organizing it into several formats. From a safety point of view, securing huge health data technologies should begin at the very beginning of a person's lifetime. This is a prerequisite. Therefore, it is crucial to collect data from trustworthy sources, protect patients' privacy (no plan must be given for finding particular people in the system), and ensure the confidentiality of this phase (Yang et al., 2018). Implementing advanced security measures is necessary to ensure that every information and data system is safe from unauthorized entry, disclosure, alterations, duplicated data, diversion, damage, abuse, or theft.

- **Phase of data transformation:** After the details have been collected and made available, the first step is to filter, classify, and convert the data in line with the conditions of the relevant analysis that is relevant. Prior to the analytics or modelling stages, data quality must be improved through material filtering, enhancement, and modification to get rid of or readily handle activity, misfits, data shortages, duplicate datasets, and other challenges. This is necessary to increase the accuracy of the data used in the analysis or modeling. In contrast, the information acquired may contain sensitive data, so it is necessary to adopt appropriate security measures when translating and storing the data (Yang et al., 2018; Shen et al., 2022). Certain security methods, such as a privacy-preserving approach, permutations, and data distribution, and access control (via a comprehensive set of files and records as a central source for permissions, software registration models, methods of authentication, and the customer settings), can ensure the safety of the data gathered.
- **Phase of data modelling**: After data are received, converted, and stored securely, analysis of the processing can begin. This is done to produce knowledge that can be beneficial. After the data have been saved in secure storage systems, this step will take place. During this stage of the process, guided data mining strategies are applied. These strategies include modelling for selecting characteristics and modeling for forecasting, in addition to category analysis, classification, and relationship. Also, having a multitude of learning strategy ensembles contributes to increased robustness and correctness regarding the finished product. However, on the other hand, establishing a trustworthy processing environment is necessary. At this time, data miners place a heightened emphasis on the utilization of robust data mining algorithms that are capable of retrieving sensitive information. So, the only people who should be working in this phase are those authorized to do so. In general, the data mining process, as well as the components of the network, need to be configured and protected against any attacks that are based on data mining and any potential security flaws (Shen et al., 2022).
- **Phase of knowledge generation**: Modelling can lead to both new facts and useful information that can be used by the people in charge of making decisions. This new information is considered sensitive, especially since it was gathered in a dangerous place. In fact, healthcare organizations are well aware that their sensitive data, which may include personally identifiable patient information, should not be made available to the general public (Tao et al., 2019). Consequently, achieving compliance with security standards should be one of the primary goals at this point.

At every point in the lifetime of big data, it is vital to provide storage for the data, ensure its integrity, and regulate who can access it.

Big Healthcare Data Privacy

In the most recent few years, there has been an increase in the number of sophisticated, persistent risks. These threats are assaults on systems of information that have been created to be extremely targeted, and their primary objective is to smuggle the data that the attacker stole. As a result, a breach of consumer privacy is regarded as an increasing worry in big data analytics,

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

making it difficult for businesses to deal with issues that are both relevant and significant at the same time. Information privacy establishes these access permissions through privacy policies and laws, such as deciding who can read personal data and financial, medical, and private information. Data security is responsible for regulating access to data at every stage of the data lifecycle (Tao et al., 2019). Concerns about patient privacy have been raised due to an incident detailed in Forbes magazine. According to the study's findings, Target Corporation provided teenage girls with gift certificates for newborn care without their parent's knowledge (Chen, et al., 2021). As a result, the big data industry now has to think about how to safeguard its analytics. No matter what changes are made to the software or the privacy legislation, developers must be able to attest that user information is protected and kept confidential.

Laws Governing Data Privacy

It is more important than ever before for healthcare providers to properly handle and protect individuals' personal information and recognize threats and legal obligations associated with processing such information. This is because the applicable data protection regulations are becoming an increasingly complex web. The rules and procedures that govern data privacy might vary widely from country to country. The table1 provides a list of important characteristics and the data privacy laws and policies of a few nations (Abouelmehdi et al., 2017).

This section provides a quick overview of some conventional strategies for protecting individuals' privacy in large data sets. Despite their long history of service in protecting patient privacy, the constraints inherent in their application have inspired the development of novel alternatives (Zhang et al., 2021).

De-Identification

As a standard procedure, doctors are trained to disregard data that could be used to pinpoint a specific patient. Patients can verify that sufficient patient identifiers have been removed using either the initial method, which necessitates the removal of particular identifiers, or the additional statistical method. In either case, the patient is allowed to do so. Yet, a hacker may be able to gain additional outside information that will assist in de-identifying the massive data set (Lv et al., 2022; Li et al., 2006). Protecting the confidentiality of big data sets requires better de-identification methods. The success rate of re-identification can be lowered by using efficient algorithms that safeguard users' privacy.

Table 1
SOME COUNTRIES LEGISLATION ON DATA PROTECTION

Country	Law	Details
U.S.A	HIPAA Act Patient Safety and Quality Improvement Act (PSQIA)	Requires the creation of national standards for transactions in electronic health care Gives those between the ages of 12 and 18 the right privacy Before disclosing any information about the health care provided to anyone, including parents a signed disclosure from the impacted required Work Products for Patient Safety must not be revealed 27. Any person who violates the secrecy clause faces civil fine Safeguard

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

	HITECH Act	the confidentiality and security of electronic health records
EU	Data Protection Directive	Safeguard people's fundamental freedoms and rights including their right to privacy when processing their data
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	Individuals have the right to understand the purposes behind the acquisition and use of their data. which obliges businesseste safeguard in prudently and securely
UK	Data Protection Act(DPA)	Gives people a way to manage information about themselves Transfers of personal data outside the European Economic Area are prohibited unless the destination country or territory guarantees sufficient degree of protection for the rights and liberties of data subjects
Russia	Russian Federal Law on Personal Data	Data operators must take "all essential technological and organisational necessary measures for securing personal data from unauthorised or accidental access." according to this requirement
India	IT Act and IT (Attendment) Act	For sensitive personal data or information use reasonable security procedures Offers recompense to anyone who suffers an unlawful loss or gain A person who discloses another person's personal information while performing services following the conditions of valid contract is subject to imprisonment and fine

K-Anonymity

While utilizing this tactic, the likelihood of successful re-identification will decrease whenever the value of k is increased. On the other hand, because it uses k-anonymization, it could lead to data distortions and the loss of further information (Sweeney, 2002; Kabalci,& Kabalci, 2019). Also, when anonymization is used, personal details (like a person's illness, for example) can be revealed to the public when quasi-identifiers, such as info, are merged with other public information.

L-Diversity

Group-based anonymization reduces the quantity of identifying information in datasets to protect the privacy of individuals. This (Distinct, Entropy, Recursive) paradigm builds on the k-anonymity's generalization and suppression techniques to further reduce the degree of detail in data representation, this (Distinct, Entropy, Recursive) paradigm builds on the k-anonymity's generalization and suppression techniques. This is done to guarantee that at least k distinct entries are at least k distinct entries transferred for each one (Jain et al., 2016; Lo'ai& Saldamli, 2021). Protecting identities at the level of k people is not the same as protecting the pertinent attribute values that were extended or suppressed, which is one of the issues with the k-anonymity model that the l-diversity model fixes. The K-anonymity paradigm has flaws, and this is one of them. This approach needs to be revised because it relies on the range of a delicate property, which opens the door to mistakes. If the number of sensitive attribute values for which L-diverse data is needed is extremely low, it is necessary to enter false data. While this bogus data will make the system more secure, it may make analysis more difficult.

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

T-closeness

Constitutes an improvement over anonymization that is based on L-diversity groups. The t-closeness model, also known as the Equal/Hierarchical distance model, is an extension of the l-diversity model. It differs from the l-diversity model by taking a new approach to interpreting attribute values. It takes into consideration the spread of the information values that are associated with that attribute (Lo'ai & Saldamli, 2021). The prevention of attribute disclosure is the key advantage of implementing this technique; nevertheless, it comes with the downside that the likelihood of reidentification rises in tandem with the quantity and variety of the data stored.

HybrEx

The hybrid execution model is an idea that can help protect users' privacy and confidentiality when using cloud computing. When an organization states that there is no risk to the user's privacy or data protection while exporting information or conducting computations using public clouds, the model will only use public clouds for data processing that is classified as public and data that is not sensitive. In contrast, the model uses their own private cloud to calculate and store sensitive and confidential data. When the software needs to connect to public or private data, the program is divided so that it can operate in private or public clouds (Stergiou et al., 2018).This allows the application to access both types of data simultaneously. It considers the highly confidential nature of the data and presents possibilities for collaboration with safety before actually carrying out the task. HybridEx's flaw is that, during the mapping stage, it just treats the cloud as an adversary rather than taking into account the key that is being generated on a private or public cloud (Zhang et al., 2018).

Identity-Based Anonymization

These strategies encountered difficulties when successfully combining anonymization, data confidentiality, and big data methodologies to evaluate usage data while simultaneously protecting user identities (Kshetri, 2014). To take full advantage of the many advantages cloud storage offers, Intel developed an open architecture for protecting users' privacy. This design provided options for both anonymizing and retracing user activity in web server logs. Enterprise data differs from the typical examples in the literature on anonymization in terms of its features throughout the implementation of the architecture process. Intel also discovered that the anonymized data was vulnerable to correlation attacks despite hiding clear Personal Identifying Info such as usernames and IP addresses. Once the researchers weighed the pros and cons of fixing these holes, they discovered that user agent data strongly reflects individual users. Once the researchers weighed the pros and cons of fixing these holes, they discovered that user agent data strongly reflects individual users. K-anonymity-based measures were employed in this analysis of the anonymization quality. At the same time, This study disc To evaluates data use while safeguarding user identities; these strategies ran into problems when they attempted to properly combine anonymization, data confidentiality, and big data technologies. Intel created an

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

open privacy protection design that allowed for multiple methods of de-identifying or re-identifying internet records to take advantage of the many advantages of cloud storage. This architecture was designed to protect users' personal information. Enterprise data differs from the typical examples found in the literature on anonymization in terms of its features throughout the design process. This difference may be found throughout the entire implementation of the architecture. In addition, Intel found that the data that had been anonymized was susceptible to correlation attacks, even though clear personally-identifying information like usernames and IP addresses had been hidden. After analyzing the potential advantages and disadvantages of addressing these vulnerabilities, the researchers found that information about the user agents strongly correlated with individual users. This study presents a case study of anonymization's application in a business, outlining the steps taken to protect sensitive company information during an investigation using big data methods. Measures based on k-anonymity were utilized to analyze the anonymization's quality. Concurrently, I realized that the anonymization process involves more than just concealing or generalizing specific properties.

A complete analysis of encrypted datasets is necessary to determine if they pose a security risk. Anonymisation entails a lot more than covering or extending certain properties.

Proposed Model

This research was broken down into six distinct steps specified in Figure 2. The first step involved gathering information from primary and secondary legal sources, such as legislation, case reports, by-laws, administrative rules, visiting websites, credible journals, news sources, and gatherings directly related to the terms. These sources included legislation, case reports, by-laws, and administrative rules. The second phase consisted of filtering this information by the regulations regulating medical devices and the privacy of medical data. After sorting these policies according to the criteria, preferences were made for government publications, journal proceedings, and other carefully picked sources. A collection of draft policies designed to represent existing policies was generated based on the applied criteria and filters. After that, standard policies that were derived from the laws and policy documents of the United States and the European Union were compared to the policies that had been developed. The comparison revealed a disparity between the law's effective control of healthcare business uses based on big data analytics, health data privacy, and the existing regulation in place. Legal professionals and politicians investigated this gap to reduce the number of false positives. In the end, a proposed set of guidelines was established. These guidelines were based on comparing policies and gaps that experts confirmed. Legislative and legal professionals were briefed on the proposed policy to solicit their comments and locate policies that directly compete with it. The findings of this inquiry were used to inform some proposals. The outcomes of this research led to suggestions that outlined a medical device regulation paradigm and protected the confidentiality of healthcare information. It was determined to examine several pieces of legislation in detail to determine if they were adequate and to identify any loopholes or problems with the laws that needed to be addressed immediately by policymakers. The Digital Security Act of 2018, the Information and

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

Communication Technology (ICT) Act of 2006, the Medical and Dental Council Act of 2010, and the Medical Practice: Private Clinics and Laboratories (Regulation) (Amendment) Ordinance of 1984 are just some of the laws that refer to primary data sources. Blog posts, journal articles, legal reviews, white papers, and reports compiled by foreign organizations are all examples of the types of secondary material found online. These are merely some instances among many.

The discussion, clarification, and analysis of the necessary legislation to establish its consequences and application can be stimulated by secondary data. Most of the time, those who interpret the law are judges and law professors.

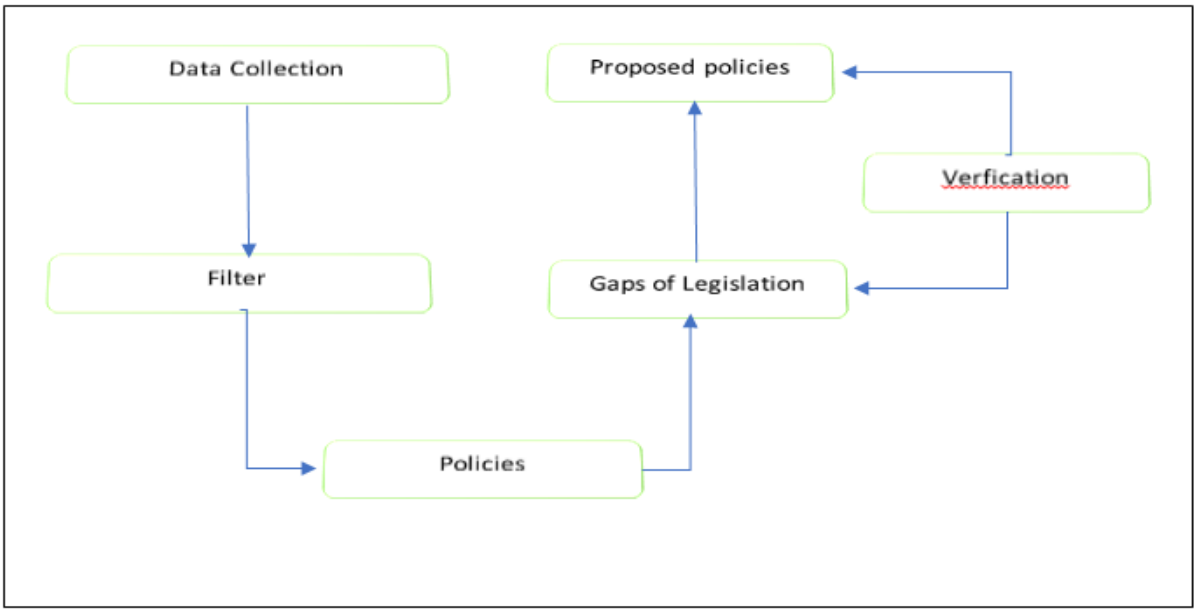

FIGURE 2
PROPOSED MODEL

Interpretation of primary data now frequently draws examples from secondary data. The first major work to contribute to developing privacy legislation in the United States was titled "The Proper Privacy" and was written by Warren and Brandeis (Warren and Brandeis, 1890The importance of secondary materials can sometimes be so great that national courts use them. When comparing AI-based medical gadgets to conventional ones, a large chasm opens up between the ideal and actual settings for quality assurance. This is because of the complexity of the system. It is necessary to store, manage, and transfer a substantial quantity of data for the big data lifecycle to yield the best possible results for efficient and cost-effective medical care. Appropriate technological and organizational safeguards must be put in place at each level of big data processing to maintain the confidentiality and safety of the data throughout its lifecycle. Data security refers to the confidentiality, integrity, and availability of data, in contrast to privacy protection, which refers to the appropriate use of information about data subjects. The users' health information privacy and security are put at risk due to inadequate preparation on the

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

technical and organizational fronts. In most cases, the legislation that governs data protection will address the problem of maintaining the confidentiality of data. Examples of technological methods include data management, synthetic data, controls for access, routine monitoring, and audits of security software. Establishing efficient legislative guidelines that regulate devices based on big data analytics is a necessary first step on the road to big data. The road to big data can only be started once these criteria are satisfied. This is necessary to preserve the confidentiality and integrity of patient health data.

CONCLUSION

Data governance and enforcement processes must be present in Iraq's current legal framework to protect patients' medical records' confidentiality. Governance of information and data enforcement devices are two such elements. The appropriate and responsible requirement for health data that underpins healthcare infrastructure and protects patient privacy should be prioritized in the drive to promote and construct a robust data privacy regime. This will ensure that the data is used appropriately. Policymakers should pass specific data protection regulations, with the EU's General Data Protection Regulation (GDPR) serving as a model, when feasible, to meaningfully establish one governance structure. Protecting health information while supporting the expansion of artificial intelligence will be a complex task within the context of AI. The medical industry can be improved through artificial intelligence, but only if the authorities create a framework that balances patient privacy and technological progress. The authorities need to take an interdisciplinary approach to build a just framework for data security. This is necessary because artificial intelligence presents several technical obstacles. To guarantee that it takes into account, by the law, the particular characteristics of the subject matter that is being regulated and provides an adequate safeguard, the structure ought to be designed in conjunction with scientists and professionals in the field of computer science Big data analytics receives scant consideration from authors, and even fewer discuss the difficulties posed by regulations. To keep up with the quickly evolving field of medical devices powered by artificial intelligence, it is crucial to keep a close eye on big data in the medical field and ensure that regulatory and legislative frameworks are continuously modified. Without the appropriate governance and control, the exponential growth of this industry has the potential to hinder breakthroughs in healthcare that are vital for achieving better health outcomes. When doing future research on patient privacy about medical technology powered by artificial intelligence, we recommend considering patients' perspectives.

REFERENCES

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017).Big data security and privacy in healthcare: A Review. *Procedia Computer Science*, *113*, 73-80.

Chen, J., Ramanathan, L., & Alazab, M. (2021). Holistic big data integrated artificial intelligent modeling to improve privacy and security in data management of smart cities. *Microprocessors and Microsystems*, *81*, 103722.

Chen, L., Zhang, N., Sun, H. M., Chang, C. C., Yu, S., & Choo, K. K. R. (2020). Secure search for encrypted personal health records from big data NoSQL databases in cloud. *Computing*, *102*, 1521-1545.

Citation Information: Kamil, A.k. (2024). Big healthcare data: enhancing security and privacy. *Journal of Management Information and Decision Sciences, 27* (1), 1-11.

Cuzzocrea, A., Leung, C. K., Olawoyin, A. M., & Fadda, E. (2022). Supporting privacy-preserving big data analytics on temporal open big data. *Procedia Computer Science*, *198*, 112-121.

Demirdogen, G., Işık, Z., & Arayici, Y. (2023). BIM-based big data analytic system for healthcare facility management. *Journal of Building Engineering*, *64*, 105713.

Hassan, S., Dhali, M., Zaman, F., & Tanveer, M. (2021). Big data and predictive analytics in healthcare in Bangladesh: regulatory challenges. *Heliyon*, *7*(6).

Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. *Journal of Big Data*, *3*, 1-25.

Kabalci, E., & Kabalci, Y. (2019). *From smart grid to internet of energy*. Academic Press.

Kshetri, N. (2014). Big data′ s impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134-1145.

Li, N., Li, T., & Venkatasubramanian, S. (2006). T-Closeness: Privacy Beyond K-Anonymity And L-Diversity. In *2007 IEEE 23rd international conference on data engineering*, 106-115.

Lo'ai, A. T., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. *Journal of King Saud University-Computer and Information Sciences*, *33*(7), 810-819.

Lv, Z., & Qiao, L. (2022). Privacy security risks of big data processing in healthcare. In *Big Data Analytics for Healthcare*, 247-263.

Meyerson, A., & Williams, R. (2004). On the complexity of optimal k-anonymity. In *Proceedings of the twenty-third ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, 223-228.

Pramanik, M. I., Lau, R. Y., Azad, M. A. K., Hossain, M. S., Chowdhury, M. K. H., & Karmaker, B. K. (2020). Healthcare informatics and analytics in big data. *Expert Systems with Applications*, *152*, 113388.

Shaqiri, B. (2017). *Exploring techniques of improving security and privacy in big data* (Doctoral dissertation, Ph. D. thesis, University of Information and Technology-Ohrid).

Shen, Y., Guo, B., Shen, Y., Duan, X., Dong, X., Zhang, H., ... & Jiang, Y. (2022). Personal big data pricing method based on differential privacy. *Computers & Security*, *113*, 102529.

Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. (2018). Security, privacy & efficiency of sustainable cloud computing for big data & IoT. *Sustainable Computing: Informatics and Systems*, *19*, 174-184.

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International journal of uncertainty, fuzziness and knowledge-based systems*, *10*(05), 557-570.

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660-671.

Thirunavukarasu, R., Gnanasambandan, R., Gopikrishnan, M., & Palanisamy, V. (2022). Towards computational solutions for precision medicine based big data healthcare system using deep learning models: A review. *Computers in Biology and Medicine*, 106020.

UNDP. (2019). 'Big Data' Can Cut Down Healthcare Costs, Increase Quality of Services. UNDP. https://www.bd.undp.org/content/bangladesh/en/home/presscenter/pressreleases/2019/02/12/_big-data_-can-cut-down-healthcare-costs–increase-quality-o f-se.html.

Yang, Y., Zheng, X., Guo, W., Liu, X., & Chang, V. (2018). . *Future Generation Computer Systems*, *86*, 1437-1455.

Zhang, J., Castiglione, A., Yang, L. T., & Zhang, Y. (2018). Recent advances in security and privacy in Social Big Data. *Future Generation Computer Systems*, *87*, 686-687.

Zhang, Y., Zhang, C., & Xu, Y. (2021). Effect of data privacy and security investment on the value of big data firms. *Decision Support Systems*, *146*, 113543.

Received: 01-Nov-2023, Manuscript No. JMIDS-23-14162; **Editor assigned:** 02-Nov-2023, Pre QC No. JMIDS-23-14162(PQ); **Reviewed:** 16-Nov-2023, QC No. JMIDS-23-14162; Revised: 18-Nov-2023, Manuscript No. JMIDS-23-14162(R); **Published:** 25-Nov-2023