Safeguarding Patient Data Security and Privacy in Healthcare

Anonymous Author(s)

ABSTRACT

This research presented in this report addresses the pressing issue of securing patient data in the healthcare sector, a challenge amplified by the increasing complexity of cyber threats and the critical nature of patient confidentiality. With the healthcare industry's reliance on electronic health records (EHRs) growing, traditional security measures have proven inadequate, necessitating the adoption of more sophisticated strategies. The project conducted explores the integration of advanced encryption methods and access control mechanisms, specifically focusing on the implementation of a secure database system designed to protect patient information. A thorough investigation of existing vulnerabilities laid the groundwork for this project, with particular attention to the use of the Advanced Encryption Standard (AES) and the establishment of a role-based access control (RBAC) system as pivotal elements of the proposed solution. Legal and ethical considerations, especially regarding data privacy and the safeguarding of personal health information, were of highest importance throughout the research, ensuring absolute compliance with security standards.

This project demonstrates the robustness of the implemented encryption and access control measures in bolstering the security and privacy of patient data. By incorporating AES, the system provided a robust defense mechanism against unauthorized access, ensuring data remained encrypted and secure across transmission and storage phases. RBAC simultaneously facilitated the allocation of access rights, coordinating data availability with user authorization levels, and thus directly addressing the sensitive nature of patient data in the digital realm. The effectiveness of these measures in safeguarding patient information underlines the potential of sophisticated security solutions in the healthcare domain. The report concludes with a discussion of potential future improvements, offering paths for further developing the secure database system by investigating state-of-the-art cryptography technologies and expanding their use throughout healthcare IT infrastructures. The research conducted not only highlights the importance of enhancing patient data security but also sets a pathway for further innovation in healthcare data protection, aiming to increase trust in digital healthcare systems.

KEYWORDS

Patient Data Security, Healthcare Privacy, Advanced Encryption Standard (AES), Role-Based Access Control (RBAC), Electronic Health Records (EHRs), Data Encryption Techniques, Secure Database Systems, Access Control Mechanisms, Healthcare Information Technology, Cybersecurity in Healthcare, Data Privacy Compliance, Ethical Considerations in Data Security, Secure Data Transmission, Data Integrity in Healthcare, Secure Patient Information Management, Cryptography in Healthcare Data, Security Vulnerabilities in Healthcare, Legal Frameworks for Data Protection, Privacy-Enhancing Technologies, Trust in Digital Healthcare Systems

1 MOTIVATION AND GOALS

In recent years, companies and organizations across various industries have been spending a substantial amount of effort on exploiting data, with the hope of gaining competitive advantages via better decision-making processes [21]. For the healthcare industry, while big data analytics plays a significant role in transforming the conventional decision-making process into more data-driven, resulting in more accurate health policy decisions, which eventually leads to better "agenda-setting, problem-defining, policy-discussing", it is still facing multiple challenges, and one of the biggest concerns is the security and privacy of health-related data [12]. Needless to say, the necessity for robust security measures has become paramount and a prominent focus. This project aims to address this need by implementing a secure database to store patient data within the healthcare context, effectively fortifying the security and privacy of patient-related medical information.

The motivation for this project stems from two fundamental factors: the profound impact that data plays in the healthcare industry, and the resulting need for infallible security measures to protect it. Patient data is of paramount importance in the healthcare industry as it contains sensitive and confidential information crucial for accurate diagnosis, personalized treatment plans, and overall healthcare management. It is further considered a solution to achieve cost-friendly and effective processing, delivery, and management of patient care [5]. Moreover, Patil and Seshadri [17] point out the significant potentials of big data in healthcare, including the improvement of patient outcomes, the prediction and prevention of diseases, and the gain of other valuable insights. However, these benefits come with costs: the threats to data security in healthcare. The impacts that data breaches have on patient data are well beyond traditional identity theft, potentially even endangering lives through erroneous personal health record information [18]. As a result, the need for robust and comprehensive data security measures is essential, as the role of patient data in healthcare mandates an environment where security and privacy are guaranteed [5].

This project's goal is to design and implement a secure database system dedicated to housing patient data within the healthcare domain. The primary focal points of our endeavor will be the integration of cutting-edge encryption methodologies and a sophisticated access control framework, both aimed at ensuring the utmost data security and privacy. To achieve this, firstly an in-depth analysis will be conducted to identify the root causes of prevalent issues facing the patient data we aim to protect. The in-depth analysis will involve a comprehensive examination of the current healthcare data landscape, identifying potential vulnerabilities, and understanding the specific challenges associated with data breaches and unauthorized access. This investigative phase will leverage insights from the research by Madavarapu et al. [19] to pinpoint critical areas for improvement, laying the groundwork for the implementation phase of our project.

Building upon this foundational understanding, we will implement state-of-the-art encryption techniques, as the ones described

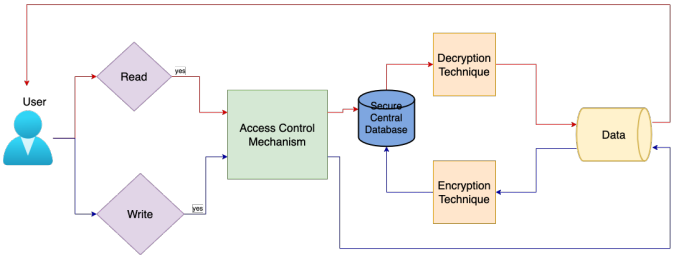

Figure 1: System Architecture Diagram

by Dharangan et al. [8], as a proactive measure to fortify patient data against potential vulnerabilities. As we delve into fortifying patient data against potential vulnerabilities, one prominent avenue we are exploring is the integration of Advanced Encryption Standard (AES). Recognized for its robust security and widespread adoption, AES aligns seamlessly with our proactive measures to enhance the confidentiality and integrity of healthcare data [8]. In the subsequent sections, we will shed light on how the incorporation of AES as a key component of our encryption strategy contributes to the overall security architecture, aligning with the cutting-edge principles advocated by contemporary research.

To complement our encryption scheme, we will implement a robust access control mechanism that will carefully assign user permissions based on predefined roles and trust levels [10]. Regarding this role-based access control, our system will implement a granular approach to assign permissions to patients and staff. For instance, healthcare professionals may be granted access to specific patient records based on their roles (e.g., doctors having broader access than administrative staff). Patients, on the other hand, will have controlled access to their own medical information, ensuring their privacy while empowering them with the ability to manage and monitor their data. The access control framework, inspired by the principles outlined by Butt et al. [10], aims to strike a balance between providing necessary access for healthcare professionals and maintaining strict controls to prevent unauthorized access, thereby reinforcing the overall security and privacy of patient data.

Overall, there are significant concerns surrounding the security and privacy of Electronic Health Records (EHRs), specifically regarding patient data. There is a prominent issue of worry among patients about the potential for their health information to be compromised during internet transmission, and a survey performed by Kala and Priya show that nearly half of patients are worried about a hacking incident [16]. This has led to a preference among healthcare providers for paper records due to perceived security advantages. In addition to security concerns, Kala and Priya highlight privacy issues, emphasizing the individual's right to control the access, modification, and sharing of their EHRs. Instances of misuse, whether intentional or accidental, by healthcare providers can lead to significant breaches of patient privacy. In response to these concerns, our proposed system, which combines Advanced Encryption Standard (AES) encryption with role-based access control (RBAC) on a PostgreSQL database, directly addresses these vulnerabilities. By implementing AES encryption, we ensure the secure transmission and storage of patient data, making it inaccessible to unauthorized parties [8]. Furthermore, RBAC allows for the precise control over who can access or modify this data, ensuring that only authorized personnel have access to sensitive information [10]. This approach not only mitigates the risk of security breaches but also enhances patient privacy, providing a comprehensive solution to the challenges outlined by Kala and Priya and fostering greater trust in digital health records management.

The overarching objective is to create a database architecture that not only upholds the principles of confidentiality, integrity, and availability but also establishes a secure and efficient system for managing patient data. In achieving this, it is important to identify the key impacts of our implementation by considering the specific beneficiaries of our healthcare database system.

The implementation of our system will be beneficial to a variety of stakeholders, including, but not limited to:

(1) Patients, who stand to gain the most. The secure database system directly addresses patient concerns about the confidentiality and integrity of their medical information. By implementing state-of-the-art encryption techniques and a sophisticated access control framework, patients can trust that their sensitive health information is protected against unauthorized access and breaches. This trust is crucial in the healthcare context, where the sharing of personal health information is essential for effective treatment. The significance of trust in the healthcare provider-patient relationship, and how security measures can enhance this trust, is highlighted by Kala and Priya, who emphasize the importance of privacy in medical care as a fundamental patient expectation and a critical component of healthcare systems [16].
(2) Healthcare professionals, including doctors, nurses, and administrative staff. Role-based access control (RBAC), as detailed by Butt et al., ensures that healthcare professionals have access to patient records based on their specific roles within the organization [10]. This tailored access prevents unauthorized viewing or modification of patient data, enhancing the security and efficiency of healthcare delivery. Healthcare professionals can rely on the integrity of the data they access, enabling accurate diagnoses, personalized treatment plans, and effective patient care management [5]. The secure system reduces the administrative burden on healthcare workers, allowing them to focus more on patient care rather than on data security concerns, thereby improving the overall healthcare service quality.
(3) Healthcare organizations employing professionals. Organizations stand to benefit from improved compliance with data protection regulations, reduced risk of data breaches, and the resulting legal and financial repercussions. The secure database system addresses the vulnerabilities and privacy issues emphasized by Kala and Priya, mitigating the risk of security breaches and enhancing patient privacy [16]. This not only protects the organization from potential fines and legal challenges but also bolsters its reputation as secure and trustworthy in the eyes of patients and the public. By prioritizing patient data security and privacy, healthcare organizations can foster a stronger relationship with their

clientele, contributing to patient satisfaction and trust. Furthermore, the adoption of advanced security measures, such as AES encryption and RBAC, allows these organizations to be more secure and efficient with their data management, ultimately reducing the prevalence of the issues that current implementations struggle with.

Furthermore, the broader healthcare industry will benefit from the advancement of secure data management practices, contributing to the overall evolution of healthcare technology and data security standards. Ultimately, the project aims to create a secure foundation that promotes trust and confidence in the healthcare system for all stakeholders involved.

This project report is structured as follows. In Section 2, we explore the contemporary landscape of research, contextualizing our project within existing contributions. Section 3 details our implementation of a secure database system for healthcare data, with a focus on the inner-workings of our encryption and access control schemes. Section 4 reflects on the challenges and successes encountered during the implementation, outlining valuable insights and the overall lessons learned. Section 5 navigates the intricate regulatory frameworks governing patient data, while the ethical aspects of responsible data management are covered in Section 6, both highlighting the necessity of consideration during the development of our project. Finally, Section 7 serves as a comprehensive evaluation, summarizing the current state of our project and proposing potential future directions.

2 RELATED WORK

The literature reviewed in this research can be grouped into two main categories based on the themes they cover and agree on: the importance of data in the healthcare industry, the corresponding challenges, and the solutions being proposed to combat those challenges.

2.1 Importance of data in the healthcare industry and the security challenges

The importance of data in the healthcare industry and the concerns about data security are widely discussed among different authors.

According to Abouelmehdi et al. [5], data has considerable potential in the healthcare industry with various values: improving patient outcomes, predicting epidemic outbreaks, avoiding preventable diseases, lowering healthcare delivery costs, and generally, improving life quality. To exemplify this idea, Abouelmehdi et al. [5] mention some projects utilizing data in healthcare, including "Be Healthy Be Mobile" launched by the World Health Organization, which collects the data in different approaches to "control, prevent and manage non-communicable diseases such as diabetes, cancer, and heart diseases." Similarly, Chao et al. [12] claim the benefits big data analytics can bring to healthcare institutions, followed by various examples to clarify this point. In detail, according to Chao et al., [12], big data analytics can support healthcare institutions in enhancing patient care, saving more lives, and cutting costs by recognizing and analyzing patterns and trends. Generally, healthcare institutions can achieve better results and more accurate decision-making, both health-related and monetary [12]. Moreover, Chao et al. [12] also discuss another aspect of advantages that data can bring to healthcare, which is the public health policies, in a way that a wide range of stakeholders is likely to significantly benefit from public health policies that are more accurate and more effective, thanks to the use of big data. Chao et al. [12] support this belief by mentioning the PolicyCLOUD [9] and beHEALTHIER [20], two platforms that are believed to apply big data analytics to achieve better healthcare policies successfully.

Despite these vast benefits, multiple concerns have arisen about the popularity and growth of big data analytics in the healthcare industry. One of the biggest concerns is data privacy breaches, as Kala and Priya [16] state that half of the patients are worried about the security of their electronic health record data when transmitted via the internet. According to Abouelmehdi et al. [5], there was an increase of 320% in the reported cases of hacking attacks on healthcare providers in 2016, and 81% of data breaches in that year came from hacking attacks. Moreover, Patil and Seshadri [17] state that the Health Insurance Portability and Accountability Act (HIPAA), while it exists in most healthcare data centers, does not guarantee the safety of patient data because HIPAA focuses more on ensuring privacy policies than on their implementation. However, these threats are not only from the healthcare or cloud service providers. Kwon and Johnson [18] provide a broader view of this issue, saying that market failures are to be blamed for the underinvestment in data security. In detail, Kwon and Johnson [18] analyze the dilemma where patients do not have a wide range of hospital or healthcare provider options to choose from, and it is also difficult for them to evaluate the data security level of each, which leads to the lack of incentives for organizations and institutions to invest in data security. As a result, the industry becomes an easy target for data breaches and hacking attacks [18].

2.2 Proposed solutions

The solutions discussed in related works for this research involve using the Advanced Encryption Standard (AES) encryption algorithm and implementing an access control framework.

Dharangan et al. [8] propose using the (AES) algorithm to encrypt healthcare data, especially image-based data. Pictures often contain susceptible and confidential information, for example, prescriptions or doctor appointments, and therefore hold no less importance than text-based data [8]. Under the experiment of utilizing AES to encrypt text-based and image-based data, Dharangan et al. [8] concluded that this method achieves a high level of security and, therefore, is appropriate for image encryption.

Butt et al. [10] propose an optimized version of the Role-Based Access Control mechanism as a solution to enhance the security level of data in an e-health cloud environment, aiming to protect the users and the data against unauthorized access from inside and outside. The idea of this mechanism is that the system assigns roles to users based on observed behavior [10]. Multiple tools and platforms are employed to implement this technique, including SQL Server to develop the module, which enables the administrators to decide general control access, and a .NET-based framework to verify and validate the trustworthiness of a user [10].

3 DESIGN AND IMPLEMENTATION

The primary objective of the project is to build a robust and secure database system to safeguard patient data within the healthcare domain. The main architecture of our system revolves around the integration of Advanced Encryption Standards (AES) and a role-based access control framework. These core elements collaborate to ensure the security and confidentiality of Electronic Health Records (EHRs), addressing challenges related to data integrity and access permissions. Our implementation consists of the PostgreSQL database with AES encryption, which provides a layer of data protection. Additionally, the role-based access control mechanism grants proper data accessibility to authorized users. This combination provides a resilient system against data breaches, thus enhancing patient trust and privacy.

3.1 Architecture

The system architecture includes several key components: Users, Access Control Mechanism, Secure Central Database, Data, and Encryption and Decryption Techniques.

- **User:** This represents the end-users who will interact with the system, such as patients, doctors, and administrative staff.
- **Access Control Mechanism:** Before any data can be read or written, users must go through this mechanism, which determines whether they have the necessary permissions.
- **Secure Central Database:** This is the main storage for the sensitive patients' data. This is where encrypted data and encryption keys will be stored.
- **Data:** Represents the actual patient data stored within the database. This would include sensitive information that must be protected.
- **Encryption Technique:** When data is written to the database, it passes through this component to be encrypted, ensuring that it is stored securely.
- **Decryption Technique:** When data is read from the database, it is decrypted through this component so that it can be presented to the user.

The system follows distinct flows for reading and writing data, denoted by red and blue lines as shown in Figure 1. Red indicates the decryption path for accessing data from the database, while blue signifies the encryption path for storing new data.

3.2 Implementation

The system's implementation is as follow:

- **Data Collection:** We extracted relevant data from the MIMIC-III Clinical Database, which includes patient personal information, admission status, and their respective stays. In addition, we did extensive data cleaning and pre-processing to ensure accuracy and consistency.
- **Database Creation:** A PostgreSQL database instance is created to serve as the central storage for patient data. The database schema is configured to accommodate the specific data fields required by the MIMIC-III Clinical Database.
- **UI Component:** A user interface is developed to provide an interactive mechanism to the system. It allows access to patient records for various user roles, including patients, doctors, and administrative staff.
- **Access Control:** A role-based access control mechanism is implemented within the system to regulate user access based on defined roles (doctor, nurse, patient, administrator, etc.) and permissions.
- **Encryption and Decryption Techniques:** An Advanced Encryption Standard (AES) algorithm is integrated into the system to encrypt sensitive patient data before storing it in the PostgreSQL database. Additionally, encryption keys are generated and securely stored in the database, thus preventing unauthorized access to sensitive data.

3.3 Tools and Technologies

The project utilizes a variety of tools and technologies, including:

- **Python:** Serves as the primary programming language, utilized for data processing, system logic, and integration.
- **SQLAlchemy:** Interacts with PostgreSQL to enable database operations, including creating database models, executing queries, and managing database.
- **PostgreSQL:** Acts as the central database for patient data.
- **PyCryptodome:** Used for encryption, decryption, hashing, and authentication.
- **Flask:** Used for user interface, handling HTTP requests, and integrating with the backend logic.

The design and implementation of this project offer an approach to develop a secure and efficient database system dedicated to protecting and managing patient data. By integrating Advanced Encryption Standard (AES) with role-based access control (RBAC), the system is able to address unauthorized intrusions and maintain the integrity and confidentiality of sensitive health data.

4 ANALYSIS

Use this section to describe the analysis of your project that you conducted, and whether the results are meaningful or not.

Also, discuss what all you learned from the project, especially what mistakes to avoid in the future.

5 LEGAL CONSIDERATIONS

The development and implementation of a secure database system for patient data in a healthcare setting, especially one which utilizes advanced encryption and access control mechanisms, intersect with various legal frameworks, necessitating a careful examination of relevant laws and regulations. Each of these legal instruments brings a set of guidelines and requirements that significantly influence the design and operational protocols of our database system, ensuring that patient data is not only secure but also handled in strict compliance with both domestic and international privacy standards.

HIPAA [1] sets the standard for the protection of sensitive patient data in the U.S., mandating that all entities dealing with protected health information (PHI) adhere to rigorous privacy and security measures. This act becomes especially relevant when considering the AES encryption and RBAC implemented in our project, as HIPAA explicitly requires the safeguarding of PHI from unauthorized access, a core goal of our database system. The HITECH

Act [2], building on HIPAA, introduces specific provisions on the technology used in healthcare, particularly emphasizing the secure use of Electronic Health Records (EHRs) and enhancing HIPAA's enforcement mechanisms.

GDPR [3], although a regulation enforced within the European Union, applies to any organization handling the data of EU citizens. It emphasizes the rights of individuals over their personal data, including the right to access, correct, and erase their data, which necessitates a level of flexibility and transparency in how our system manages patient information. The CCPA [4], similarly to GDPR, grants California residents increased control over their personal information collected by businesses, further emphasizing the importance of robust access control and data management practices to comply with individuals' privacy requests.

Amidst these established regulations, it is also crucial to explore emerging legislation that may further influence the legal landscape of healthcare data protection. Among these are the anticipated updates to HIPAA, aiming to enhance and modernize privacy practices to better align with current healthcare and technological advancements. Additionally, the proposed Data Privacy Act of 2023 [13] seeks to update the Gramm-Leach-Bliley Act [14] to strengthen the protection of nonpublic personal information, a move that could indirectly influence healthcare data management by setting new standards for data privacy within the financial sector. Furthermore, the introduction of the Health Data Use and Privacy Commission Act [11] signals a bipartisan effort to identify and close privacy gaps associated with emerging technologies not currently covered by HIPAA, demonstrating an effort to ensure comprehensive health data protection with rapidly changing technologies [6].

These existing acts and new developments emphasize the necessity for our healthcare data management system to be designed with flexibility and foresight, ensuring ongoing compliance with current and evolving legal requirements for the safeguarding of patient privacy.

6 ETHICAL CONSIDERATIONS

The ethical considerations surrounding the development and implementation of a secure database system for healthcare, particularly one that leverages advanced encryption and access control mechanisms, are deeply intertwined with the principles laid out in the ACM Code of Ethics [7]. The following principles offer a robust guide for the complex ethical considerations associated with handling sensitive patient data in a healthcare setting.

- **Avoid Harm (1.2):** This principle is paramount as the secure database system must ensure the utmost protection of patient data against breaches, unauthorized access, or any form of compromise that could lead to harm such as identity theft, financial loss, or misuse of personal health information. The design and implementation of encryption and access controls are directly aimed at mitigating these risks, emphasizing the importance of protecting individuals' health, safety, and privacy.
- **Respect Privacy (1.6):** The sensitivity of patient information necessitates a rigorous approach to privacy, where data is handled with the highest level of confidentiality. Our project aligns with this principle by adopting advanced encryption methods and access control mechanisms that ensure data is accessible only to authorized personnel, thereby respecting the privacy and autonomy of the patients whose data we are entrusted with.
- **Respect Confidentiality (1.7):** In line with respecting privacy, this principle further emphasizes the obligation to protect confidentiality of patient information. Our system's deployment of strong encryption techniques and strict access controls is designed to maintain the confidentiality of the health data, ensuring that patient information is shielded from any unauthorized disclosure.
- **Give Comprehensive and Thorough Evaluations (2.5):** The dynamic nature of cybersecurity threats requires constant evaluation of the system's security measures. This principle guides our project towards continuous assessment of the encryption and access control effectiveness, ensuring the system's resilience against evolving threats and vulnerabilities.
- **Ensure High Standards (3.1):** The sensitivity of healthcare data demands excellence in every step of the database system's development and operation. Our project is committed to high standards in selecting and implementing encryption algorithms and access controls, driven by the ethical obligation to protect patient data with the most reliable and effective security measures available.

Adhering to these principles from the ACM Code of Ethics ensures that the project not only meets its technical objectives but also upholds the ethical responsibilities towards patients and healthcare providers. By embedding these ethical considerations into the project's core, we aim to foster trust and confidence in the digital handling of healthcare data, ensuring that all actions are conducted with integrity, respect for privacy, and a commitment to harm avoidance.

7 CONCLUSIONS

This research provides a comprehensive exploration of advanced security measures for the crucial task of safeguarding patient data security and privacy within healthcare systems, an endeavor necessitated by the escalating cyber threats and the importance of maintaining patient confidentiality. Through the integration of advanced encryption methods and role-based access control mechanisms, specifically the implementation of a secure PostgreSQL database system, we've created a robust foundation for protecting patient information against unauthorized access and potential breaches.

The current state of our work includes the successful collection and pre-processing of patient data from the MIMIC-III Clinical Database [15], followed by the secure storage of this data within our developed database system. This milestone marks a significant step towards achieving our project's objectives, setting the groundwork for the data security implementations of our system.

Looking ahead, the project's next phases will focus on the development of a user interface (UI) component, allowing users an intuitive platform to access and manipulate data. Additionally, the

implementation of AES will further reinforce the security framework of our database system, ensuring that patient information remains protected both in transit and in storage. We will then create a sophisticated role-based access control mechanism. These enhancements will ensure that users can interact with the system efficiently while maintaining strict access protocols and encryption techniques to protect patient data privacy and security at all times.

Future directions for this work could extend into several key areas. Firstly, the exploration of more advanced cryptographic solutions could offer stronger security guarantees for patient data. Secondly, integrating machine learning algorithms could potentially enhance the system's ability to detect and respond to anomalous access instances, identifying security breaches before they occur. Thirdly, expanding the system's capabilities to include more granular access controls and audit logs could provide clearer insights into data access patterns and improve compliance with healthcare regulations.

In conclusion, while significant strides have been made in enhancing the security and privacy of patient data within healthcare systems, there is still much to be done. The landscape of cyber threats continues to evolve, demanding that our efforts to protect patient data do the same. By pursuing the outlined future work and remaining vigilant to evolving threats, we can continue to build upon the foundation provided by our research, aiming not only to meet but exceed the standards of patient data protection, fostering greater trust in digital healthcare systems.

REFERENCES

[1] 1996. Health Insurance Portability and Accountability Act (HIPAA). https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[2] 2009. Health Information Technology for Economic and Clinical Health (HITECH) Act. https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf.

[3] 2016. General Data Protection Regulation (GDPR). https://gdpr-info.eu/.

[4] 2018. California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa.

[5] Karim Abouelmehdi, Abderrahim Beni-Hessane, and Hayat Khalouf. 2018. Big healthcare data: preserving security and privacy. *Journal of Big Data* 5, 1 (2018), 1. https://doi.org/10.1186/s40537-017-0110-7

[6] Alder, Steve. 2022. Bipartisan Legislation Introduced to Modernize Health Data Privacy Laws. https://www.hipaajournal.com/bipartisan-legislation-introduced-to-modernize-health-data-privacy-laws/.

[7] Association for Computing Machinery. 2018. ACM Code of Ethics and Professional Conduct. ACM, New York. https://www.acm.org/code-of-ethics.

[8] Dharangan B, Praveen J, Selva Chandru M, S. Rajagopal, and B. Jegajothi. 2022. Secure Cloud-based E-Health System using Advanced Encryption Standard. In *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)*. 642–646. https://doi.org/10.1109/ICESC54411.2022.9885501

[9] Ofer Biran, Oshrit Feder, Yosef Moatti, Athanasios Kiourtis, Dimosthenis Kyriazis, George Manias, Argyro Mavrogiorgou, Nikitas M. Sgouros, Martim T. Barata, Isabella Oldani, María A. Sanguino, Pavlos Kranas, and Samuele Baroni. 2022. PolicyCLOUD: A Prototype of a Cloud Serverless Ecosystem for Policy Analytics. *Data & Policy* 4 (2022), e44. https://doi.org/10.1017/dap.2022.32

[10] Ateeq Ur Rehman Butt, Tariq Mahmood, Tanzila Saba, Saeed Ali Omer Bahaj, Faten S. Alamri, Muhammad Waseem Iqbal, and Amjad R. Khan. 2023. An Optimized Role-Based Access Control Using Trust Mechanism in E-Health Cloud Environment. *IEEE Access* 11 (2023), 138813–138826. https://doi.org/10.1109/ACCESS.2023.3335984

[11] Bill Cassidy and Tammy Baldwin. 2022. Health Data Use and Privacy Commission Act. https://www.congress.gov/bill/117th-congress/senate-bill/3620. Legislation proposed to analyze and improve health data privacy laws.

[12] Kang Chao, Md Nazirul Islam Sarker, Isahaque Ali, R.B. Radin Firdaus, Azlinda Azman, and Maslina Mohammed Shaed. 2023. Big Data-Driven Public Health Policy Making: Potential for the Healthcare Industry. *Heliyon* 9, 9 (September 2023), e19681. https://doi.org/10.1016/j.heliyon.2023.e19681

[13] Congress. 2023. Text - H.R.1165 - 118th Congress (2023-2024): Data Privacy Act of 2023. https://www.congress.gov/bill/118th-congress/house-bill/1165/text.

[14] Federal Trade Commission. 1999. Gramm-Leach-Bliley Act. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

[15] Alistair Johnson, Tom Pollard, and Roger Mark. 2016. MIMIC-III Clinical Database (version 1.4). https://doi.org/10.13026/C2XW26. https://doi.org/10.13026/C2XW26

[16] M. Kumari Kala and M. Priya. 2023. A Comprehensive Survey on the IoT - Based Electronic Healthcare Records Security, Privacy Issues, and Countermeasures Using Blockchain Technology. In *2023 International Conference on Innovations in Engineering and Technology (ICIET)*. 1–8. https://doi.org/10.1109/ICIET57285.2023.10220624

[17] Harsh Kupwade Patil and Ravi Seshadri. 2014. Big Data Security and Privacy Issues in Healthcare. In *2014 IEEE International Congress on Big Data*. 762–765. https://doi.org/10.1109/BigData.Congress.2014.112

[18] Juhee Kwon and M. Eric Johnson. 2015. Protecting Patient Data-The Economic Perspective of Healthcare Security. *IEEE Security & Privacy* 13, 5 (2015), 90–95. https://doi.org/10.1109/MSP.2015.113

[19] Jhansi Bharathi Madavarapu, Radha Krishna Yalamanchili, and Venkata Naresh Mandhala. 2023. An Ensemble Data Security on Cloud Healthcare Systems. In *2023 4th International Conference on Smart Electronics and Communication (ICOSEC)*. 680–686. https://doi.org/10.1109/ICOSEC58147.2023.10276231

[20] Argyro Mavrogiorgou, Spyridon Kleftakis, Konstantinos Mavrogiorgos, Nikolaos Zafeiropoulos, Andreas Menychtas, Athanasios Kiourtis, Ilias Maglogiannis, and Dimosthenis Kyriazis. 2021. beHEALTHIER: A Microservices Platform for Analyzing and Exploiting Healthcare Data. In *2021 IEEE 34th International Symposium on Computer-Based Medical Systems (CBMS)*. 283–288. https://doi.org/10.1109/CBMS52027.2021.00078

[21] Foster Provost and Tom Fawcett. 2013. Data Science and its Relationship to Big Data and Data-Driven Decision Making. *Big Data* 1, 1 (February 2013), 51–59. https://doi.org/10.1089/big.2013.1508