

## Article

# A Novel Cloud Enabled Access Control Model for Preserving the Security and Privacy of Medical Big Data

Abdullah Alabdulatif <sup>1</sup>, Navod Nieranjan Thilakarathne <sup>2,\*</sup> and Kassim Kalinaki <sup>3</sup><sup>1</sup> Department of Computer, College of Sciences and Arts in Al-Rass, Qassim University, Al-Rass 51452, Saudi Arabia; a.alabdulatif@qu.edu.sa<sup>2</sup> Department of ICT, Faculty of Technology, University of Colombo, Colombo 00700, Sri Lanka<sup>3</sup> Department of Computer Science, Islamic University in Uganda (IUIU), Mbale P.O. Box 2555, Uganda; kalinaki@iuiu.ac.ug

\* Correspondence: navod.nieranjan@ict.cmb.ac.lk

**Abstract:** In the context of healthcare, big data refers to a complex compilation of digital medical data collected from many sources that are difficult to manage with normal technology and software due to its size and complexity. These big data are useful in various aspects of healthcare, such as disease diagnosis, early prevention of diseases, and predicting epidemics. Even though medical big data has many advantages and a lot of potential for revolutionizing healthcare, it also has a lot of drawbacks and problems, of which security and privacy are of the utmost concern, owing to the severity of the complications once the medical data is compromised. On the other hand, it is evident that existing security and privacy safeguards in healthcare organizations are insufficient to protect their massive, big data repositories and ubiquitous environment. Thus, motivated by the synthesizing of the current knowledge pertaining to the security and privacy of medical big data, including the countermeasures, in the study, firstly, we provide a comprehensive review of the security and privacy of medical big data, including countermeasures. Secondly, we propose a novel cloud-enabled hybrid access control framework for securing the medical big data in healthcare organizations, and the result of this research indicates that the proposed access control model can withstand most cyber-attacks, and it is also proven that the proposed framework can be utilized as a primary base to build secure and safe medical big data solutions. Thus, we believe this research would be useful for future researchers to comprehend the knowledge on the security and privacy of medical big data and the development of countermeasures.

**Keywords:** security; public cloud; access control; encryption; private cloud; data privacy; big data; healthcare; Internet of Things (IoT)



**Citation:** Alabdulatif, A.; Thilakarathne, N.N.; Kalinaki, K. A Novel Cloud Enabled Access Control Model for Preserving the Security and Privacy of Medical Big Data. *Electronics* **2023**, *12*, 2646. <https://doi.org/10.3390/electronics12122646>

Academic Editors: Abdul Majeed and Xiaohan Zhang

Received: 6 May 2023

Revised: 3 June 2023

Accepted: 8 June 2023

Published: 13 June 2023

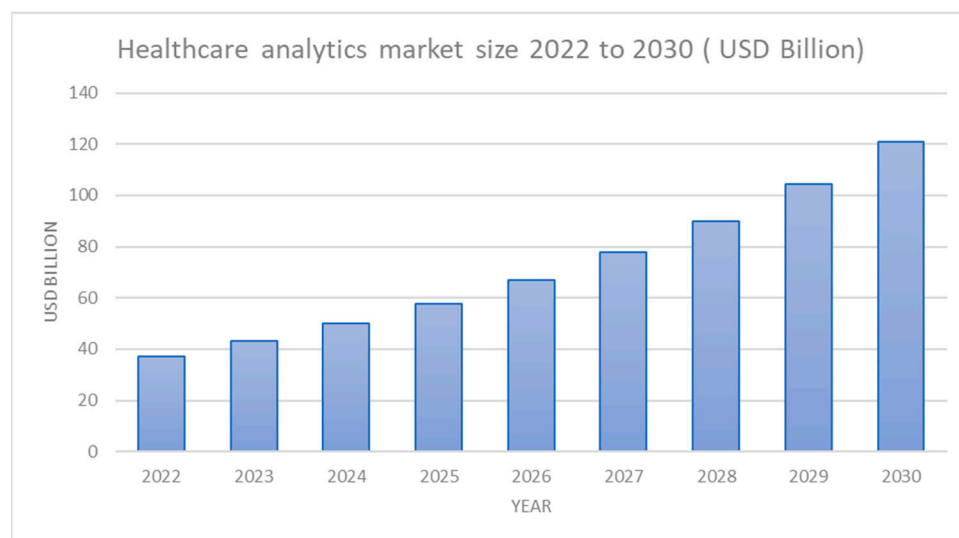


**Copyright:** © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Big data is a term that describes a significant amount of complicated and massive data sets that cannot be examined using typical computer approaches where the data might be structured, unstructured, or semi-structured [1]. The exact definition of the term “Big Data” is continuously evolving, where a data collection is considered “Big” if it has a size ranging from a few terabytes to several petabytes [2]. On the other hand, even though the data can be apportioned into three categories as above mentioned, the main focus is on unstructured big data [2]. When the data becomes unstructured and complex, they cannot be maintained and handled by traditional relational databases, which necessitates novel mechanisms to analyze this large volume of complex data [3–5]. In simple terms, big data refers to the ever-changing nature of our world [4,6], as everything changes around us in every second we spend. For instance, according to the latest statistics, during one single day, more than five hundred terabytes of data become ingested into the databases of Facebook, a social media networking company, owing to the billions of user transactions that are happening daily (audio and video uploads, content creations, message exchanges, and

user comments) [4,6]. Moreover, the New York Stock Exchange is another example, which generates one terabyte of trade data per single day [4–6]. Modern businesses/organizations use the insights from this big data to discover consumer shopping habits/patterns, for targeted marketing and advertising, to offer personalized medical plans for patients, to monitor the health condition from wearable devices, and for real-time monitoring of networks for cyber security attacks [7]. One of the most significant things is every industry nowadays uses big data for their future planning of businesses, to predict what will happen next, and to identify their customer behavior by inferring insights from past data [4–6]. Healthcare, telecommunication, and financial services are some domains that highly reap the benefits of this big data [5]. According to recent estimates [5,7], the healthcare big data analytics market size could reach more than \$120 billion by 2030, as shown in Figure 1 [4–7], which showcases that big data is becoming a high necessity asset for healthcare.

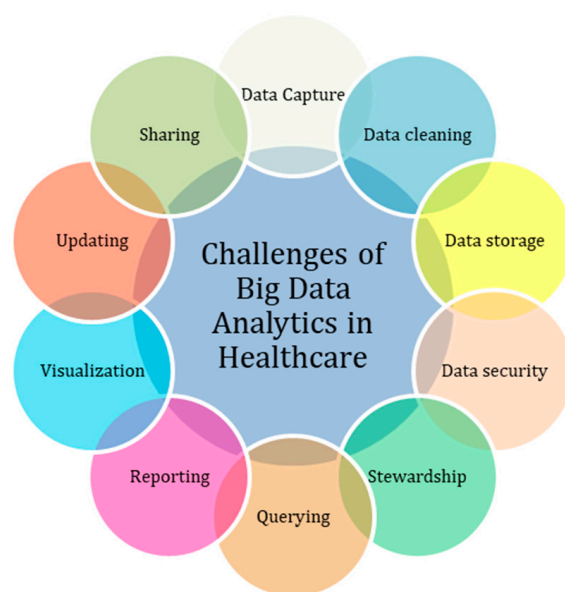


**Figure 1.** Healthcare analytics market size from 2022 to 2030.

Big data in the healthcare context is a complex collation of digital medical data acquired from several sources that are challenging to handle with standard technology and Software owing to its large volume and complexity [1]. According to [1,2], this medical big data can also interchangeably be referred to as Multimedia Medical Big Data (MBD), as the data is acquired from a variety of sources. This medical big data mainly consist of patient data in the form of digital health records or Electronic Health Records (EHRs), data from written notes and prescriptions of physicians, medical imaging, insurance, laboratory, medical journals, pharmacy, and other administrative and medical environmental data, and data collected from machines and sensors which form what is referred to as the Internet of Things (IoT) and social media data, for instance, data from social networking sites and blog entries [7–15]. All these massive amounts of data have enormous potential in improving the efficiency and quality of healthcare, detecting health hazards before they are onset, predicting outbreaks of epidemics [4], controlling human health by diagnosing diseases at an early stage, and aiding in improved decision-making. Even though medical big data offer greater benefits for the goodness of mankind, there are a variety of challenges that hinder the optimal growth of technology, in which the key challenges are data storage, data capture, data cleaning, and data security and privacy, as depicted in Figure 2 [1,2].

According to [1–6], the majority of researchers that used artificial intelligence (AI) and big data analytics in medical diagnosis did not place priority on data privacy and security, which could eventually jeopardize the lives of patients. Even though collecting data in healthcare may be highly beneficial for diagnosing the patient's condition and for further research, we must also consider the adverse consequences that technology brings, which could eventually endanger the lives of innocents. Digitalization in the medical industry

is reaching a tipping point where the rapid use of new technologies such as IoT, mobile computing, and cloud computing has posed new difficulties to big data in healthcare. As a result, it is essential to address cyber security concerns throughout the generation, collection, storage, sharing, exchange, and use of medical big data [1,2]. Medical big data, on the other hand, is comprised of three types of physical states [2], that is, files and images, video and data flow, and text and language, which indicate the unstructured nature of all these medical data. As medical big data often consist of patient pathological information and Personal Identification Information (PII), protecting the privacy of medical big data is deemed essential thing. Otherwise, if the patient's personal information is revealed by any means, it will affect the patient's reputation and life, as well as pose severe moral and ethical issues [2–6].



**Figure 2.** Top 10 challenges of big data analytics in healthcare.

As previously said, medical big data has many advantages and has a lot of potential for revolutionizing healthcare, but it also has a lot of drawbacks and problems, of which security and privacy are of utmost concern, among many other challenges. The security and privacy concerns that target medical big data are being increased annually, posing doubt in the mind of researchers and medical organizations about the reliability and safety of medical care. Nevertheless, healthcare organizations have discovered that current security and privacy measures are not adequate for safeguarding their big data repositories and pervasive environment [3,5,7,8]. Thus, it is essential to recognize the limitations of present security and privacy solutions and envisage future research paths to maintain a safe and trustworthy medical big data environment, which was our main motivation behind this research work. Thus, motivated by the fact of designing safe and trustworthy medical environments, in the study, we have provided a comprehensive review of medical big data and present a novel access control model for improving the security and privacy of medical big data. In this regard, the main contributions of the study are highlighted in Section 1.1.

### 1.1. Contributions of the Study

Big data and related analytical tools are continually aiding in the administration, measurement, and control of massive amounts of data generated in the healthcare industry [1–7], posing a variety of security and privacy issues. In this aspect, this research provides a brief overview of security and privacy problems, as well as the current state of security and privacy solution deployment for medical big data. Nonetheless, toward improving the security and privacy of medical big data, we have proposed a novel access control model that can be used to secure medical big data environments.

The significant contributions of our study are indicated below.

- A comprehensive overview of the role of big data in medical care is presented.
- An overview of privacy and security implications of medical big data is presented.
- A comprehensive examination of strategies and techniques for addressing security and privacy challenges in medical big data, along with key components based on the available literature, is provided.
- A comparison of similar research is highlighted.
- Designed a novel access control model for improving the security and privacy of medical big data, which can be used as a primary base to build safe medical big data solutions.

## 1.2. Outline of the Study

The remainder of the research is structured into six sections. Following the introduction, the Section 2 provides a brief explanation of big data, highlighting major aspects and offering significant information about medical big data. Following that, we give a brief discussion on the privacy and security of medical big data in Section 3, along with protective methods, with a brief description of these preventative measures and a comparison of associated studies. Our proposed access control model is highlighted in Section 5, with the analytical results obtained and evaluations of it. Finally, we conclude our research in the Section 6 with the conclusions we derived.

## 2. Big Data

This section underlines the fundamental characteristics of big data and provides a preface on medical big data, emphasizing how it varies from “Big Data” in general.

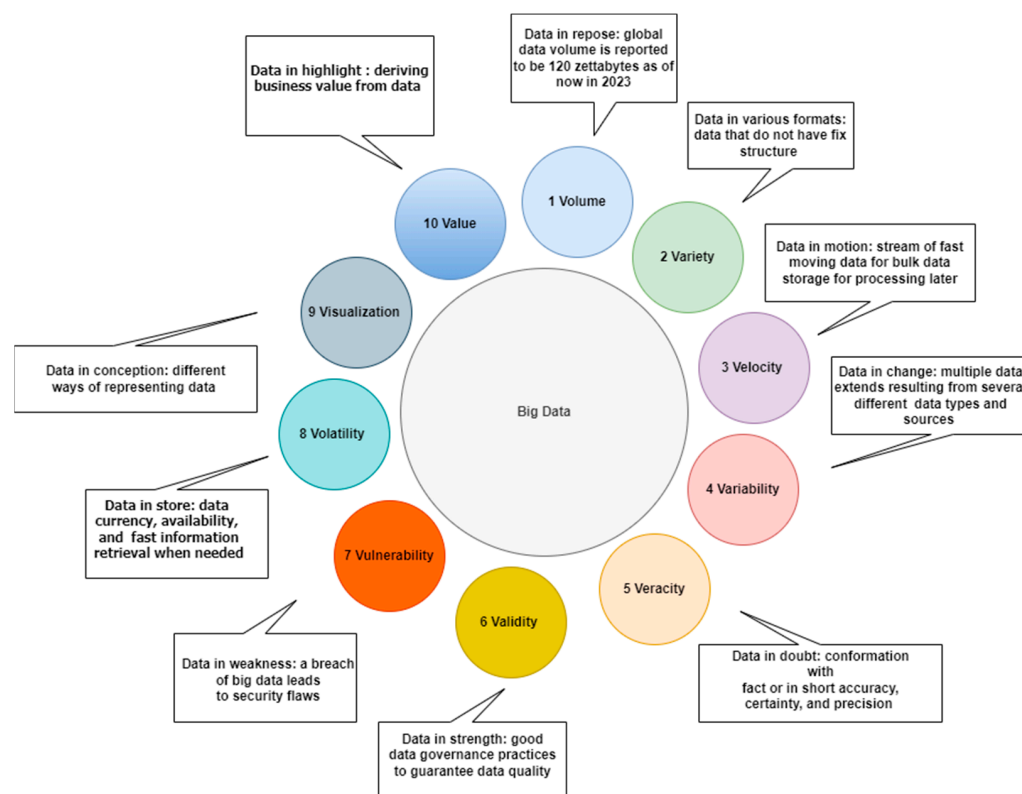
### 2.1. Characteristics of Big Data

Big data, in general, can be categorized based on the following characteristics, which are earlier known as the three V's. Now, this has extended towards five V's to ten V's, as shown in Figure 3 [1–6].

1. Volume—Big data involves massive amounts of data, ranging from gigabytes to petabytes and beyond [1–6].
2. Variety—Big data comes in many different forms, including structured data, semi-structured data, and unstructured data. It may include text, audio, video, images, social media data, and other data types [1–6].
3. Velocity—Big data is generated at an unprecedented rate, often in real-time or near real-time. This means that it needs to be processed quickly to derive insights from it. How rapidly data is produced and processed to meet demands determines its actual potential [1–6].
4. Variability—Big data can be highly variable, both in terms of the data itself and how it is generated. This means that it may require different processing techniques and tools depending on the specific data and the goals of the analysis [1–6].
5. Veracity—Big data may contain errors, inconsistencies, and inaccuracies. It is important to ensure that the data is accurate and reliable before using it for analysis [1–6].
6. Validity—Validity refers to the accuracy and relevance of the data to the specific problem being addressed. In other words, the big data must be appropriate for the intended use and must accurately reflect the real-world phenomenon it is intended to measure [1–6].
7. Vulnerability—When data is compromised, it raises a lot of worries about how vulnerable it is to security and privacy assaults [1–6].
8. Volatility—This is related to the life cycle of data, which refers to how long-outdated data should be preserved before being discarded [1–6].
9. Visualization—This enables users to gain insights from large and complex datasets. By using visualization tools, users can explore and analyze data more intuitively

and interactively, making it possible to uncover insights that might otherwise be missed [1–6].

10. Value—Big data has the potential to provide significant value to organizations, but this requires the ability to extract meaningful insights and derive actionable intelligence from the data [1–6].



**Figure 3.** Ten V's of big data.

In summary, big data is a rapidly growing field that has significant implications for businesses and organizations in various industries. Understanding the characteristics of big data is crucial for effectively managing and analyzing these vast amounts of data and extracting valuable insights to make informed decisions.

## 2.2. Big Data Applications

Since 2010, big data has been in the limelight, and it is increasingly being employed in a variety of economic, social, and professional settings [11–14,16–23]. For a better understanding, Table 1 outlines the categorization of applications areas where big data is now used [1,5,7–11,14,15].

In general, big data allows a company to store and handle enormous amounts of data at rapid speeds to obtain the most useful information/insights from them. To examine diverse and abundant data and turn raw data into information to improve decision-making processes, several tools and approaches are necessary which is known as Big Data Analytics (BDA), which refers to the tools and methods for transforming large amounts of data into information that can be used for further analysis. BDA is a technology that combines IT, business professionals, and data scientists, where it is concerned with gaining deeper insights from the underlying data. Different big data tools can be employed depending on the problem and the type of data to be examined in a typical big data environment. Table 2 provides a summary of these various tools and approaches [1–6].

**Table 1.** Big data applications.

Domain	Applications
Healthcare	Disease prediction, medical research, providing quality medical care, cost reduction of medical treatments, identify the diseases at early stages and identifying the best possible treatment plans, and pandemic surveillance
Public sector	Surveillance, environmental protection, power generation and consumption (smart grid), tax reduction, public welfare
Education	Track student performance, improve student learning, and provide student guidance.
Entertainment	Manage content for a target audience, measure the performance, and measure the feedback.
Banking	Analyzing business, customer habit analysis, prognostic analytics
Industry	Improve the manufacturing process, improve the quality of products, and reduce errors.
Transportation	Intelligent transport systems, traffic control, traffic congestion management, identifying the best possible route (Google Maps), revenue management.

**Table 2.** Big data analytics tools and techniques.

Technique	Tools
Map Reduce	Oozie, Flume, Pig, Hive
NoSQL	Cassandra
Storage	HDFS

### 2.3. The Role of Big Data in Healthcare

Big data usage in healthcare has increased over recent years owing to the increased adoption of IoT devices in healthcare, where most data come from medical records [2]. This vast amount of data has the potential to revolutionize healthcare, assisting disease diagnosis, clinical decision support systems, better management of medical resources, pandemic surveillance, real-time condition analysis, population health management, food safety management, and so on [2–4,6,24]. As an example, detecting cancerous situations necessitates the collection of petabytes of data from multiple sources from the patients, in order to determine the stage of the disease and to have an idea of survival percentage [5]. Furthermore, by focusing more on the preventative aspect and offering customized care based on continuous monitoring, the medical big data paradigm is decreasing overall healthcare costs while increasing the quality of care. Based on the literature related to medical big data [1,20], big data assists and is involved with medical care in various aspects by offering big data analytical capabilities. For a better understanding, the following highlight the benefits of big data in healthcare.

- **Offer patient-centric care:** In patient-centric care, medical big data assist in making timely decisions based on the evidence inferred from the clinical data [1–3].
- **Offering a predictive analysis of diseases:** Based on the evidence inferred from the underlying medical data, this helps to predict the spread of diseases and virus outbreaks and offers ample time to take necessary actions [1,4–8].
- **Real-time patient condition monitoring:** Through the data collated from the Medical IoT devices, such as a variety of sensing devices and wearable devices (e.g., fitness trackers) helps to monitor the condition of patients in real-time [3–5,7,8].
- **Improving medical treatments and quality of care:** Based on the current condition and the status inferred from the medical big data, this provides opportunities for medical staff to review the treatment plans and revise the plans considering the current condition of the patient [3–5,7,8].



- **Lowering the mortality rate:** Because big data allows for early detection and diagnosis of illnesses, it ensures that the appropriate decisions are made at the right time and in a timely way, lowering patient morbidity and mortality [5,7–9,15].
- **Better communication between patient and healthcare provider:** Big data improves the communication between healthcare providers and patients by allowing them to share their ideas/prescriptions/advice/views through social medical sites, and telemedicine tools [5,7–9,15].
- **Improves public health surveillance and response:** Big data, in conjunction with AI and data analysis tools and platforms, aids in the study of disease patterns, the tracking and tracing of disease outbreaks and dissemination, and public health surveillance [5,7–9,15].
- **Detection of security flaws and medical fraud:** Big data, in conjunction with AI techniques, aids in the detection of security anomalies and frauds in healthcare that originate from internet-connected devices and medical networks [5,7–9,15].
- **Improved patient participation:** Owing to the up-to-date and real-time insights provided by the medical big data it gives a sense of satisfaction to patients and facilitates them to take any decisions about their wellbeing [8–11,14,15].
- **Reduced cost of care:** By enabling patients and medical staff to make timely and up-to-date and optimized decisions, big data allows to cut down unnecessary costs involved with patient care and the medical environment [8–11,14,15].
- **Precision medicine:** Big data is used to create personalized treatment plans for patients based on their genomic and clinical data [25].
- **Drug development:** Big data is used to identify potential drug targets and improve the efficiency of clinical trials [26].

In terms of medical big data applications, all big data-related medical applications can be apportioned into four key application types: as shown in Table 3.

**Table 3.** Big data applications in healthcare.

Reference	Application	Description
[25,27–29]	Patient-centric care	In patient-centric care, big data is used to design personalized treatment plans based on the patient's condition.
[30–33]	Predictive analysis	The application of predictive analytics allows clinicians, healthcare organizations, and health insurance providers to explain the possibility of their patients getting specific medical illnesses, such as heart difficulties or diabetes.
[34–37]	Real-time monitoring	Big data facilitates monitoring the state of patients with the use of medical equipment and the IoT and offers continuous real-time monitoring capabilities, which makes it feasible to begin therapy and intervention at an earlier stage.
[26,38,39]	Improving patient treatment	The collection and analysis of large amounts of data help medical professionals and relevant stakeholders to make better-informed choices regarding patient care and service provision.

#### 2.4. Sources of Medical Big Data

The sources of medical big data come from a variety of sources and may vary depending on the context [11–14,16–20]. As it is essential to get to know the source of this big data, in the following, we highlight the key sources that the big data currently originates in a healthcare setting.

- Medical devices (sensors/machine-generated) data

Medical devices, such as MRI machines, X-ray machines, and other medical imaging equipment, generate large amounts of data that can be used for diagnosis and treatment planning. Wearable devices, such as fitness trackers and smartwatches, also generate health data that can be used for population health management and disease prevention [1–3].

- Human-generated data

This comprises data created by people interacting with medical systems such as electronic health record systems, which frequently include semi-structured and unstructured data such as laboratory test results, clinical notes, hospital admission notes, treatment, outcomes, and so on [2–4,6].

- Social media and behavioral data

Social media and online forums provide a platform for patients to share their health experiences and provide insights into patient preferences and behaviors. This data can be used to improve patient engagement and develop patient-centered care models [1–6].

- Biometric data

Biometric data often involves data that may be obtained from individuals, such as signatures, fingerprints, genetics, blood pressure, retinal scan, heart rate, as well as medical images [1–6].

- Epidemiological data

This includes various sources of statistical data and data from medical surveys [1–6].

- Public health surveillance data

Public health surveillance data includes data from disease registries, disease surveillance systems, and public health programs. This data is used to monitor disease outbreaks, track disease trends, and evaluate public health interventions [40–42].

- Administrative claims data

Insurance claims data contains information on healthcare utilization, including procedures, diagnoses, and treatments. This data can be used to identify healthcare trends and patterns, evaluate healthcare quality, and reduce costs [1–6].

- Genomics data

Advances in genomics have led to the creation of large datasets containing genetic information. This data can be used to identify disease risk factors, develop personalized treatments, and improve healthcare outcomes [6,43,44].

### 3. Preamble on Security and Privacy of Big Data

In terms of medical big data, many studies, whitepapers, and business reports [1,15], suggested if properly applied, big data can be used to determine the correct treatments plans based on the patient's condition, assurance of public and community health, improve the diagnosis process and improve the accuracy of clinical decisions, ensure proper management within medial organizations and ensure long term sustainability of the medical industry. However, several researchers have pointed out that this would be somewhat difficult owing to the security and privacy challenges, among many other challenges, such as needed expertise and technological skills, heterogeneity, and complexity pertained to medical big data [11–14].

According to [2], security and privacy risks related to big data in the medical industry may be seen in four stages:

1. Data collection
2. Data transfer
3. Data storage
4. Data consumption and sharing

Security of medical big data often involves having protection against unauthorized access while ensuring fundamental information security concepts that are confidentiality, integrity, and availability, which focus totally on protecting the data from a variety of cyber-attacks. On the other hand, privacy is defined as protecting sensitive information from unauthorized disclosure, such as PII included with medical data. Further privacy is



mainly focused on developing appropriate policies and authentication and authorization procedures towards guaranteeing that patient private data are collected, shared, and used appropriately [20–23,45].

In [10], the researchers proposed a secure big data analytics framework for the Health Information System (HIS), which is made up of five components that may be used to manage medical big data in a typical healthcare setting, as shown in Figure 4.

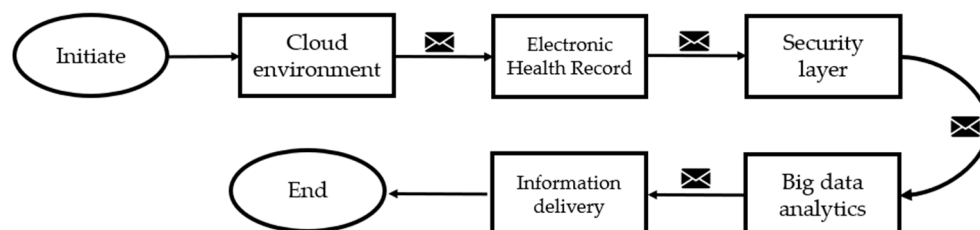


Figure 4. HIS.

The suggested HIS framework's initial component is a cloud environment that offers a variety of user services and permits data exchange. In a typical medical context, the second component is the Electronic Health Record (EHR), which is used to collect and integrate patient data from numerous data sources. The security layer is the third component, and it is used to manage different security and privacy problems related to the underlying medical big data, such as authentication, authorization, data confidentiality, and availability. To provide such medical services, the security layer is comprised of cryptographic encryption algorithms such as RSA, RC4, AES and authentication techniques such as Two Factor Authentication (2FA), and One Time Password (OTP) for allowing access only to authorized users. Further, it also comprises access control mechanisms for authorizing users to execute tasks based on the granted access control privileges. The fourth layer comprises big data analytics tools to obtain insights from the raw medical data collated. Finally, the fifth component, which is the information delivery layer, takes care of delivering this medical information to relevant destinations and providing information services [9]. With this, what we have understood is that security and privacy protection mechanisms should be an integral part of the medical big data life cycle from the point of data generation to the data processing and information dissemination stage, where we can provide optimal protection to underlying medical big data [46,47].

In this regard, we plan to present a quick review of what actions may be performed to preserve the security of medical big data in the next part, followed by our proposed access control framework.

### 3.1. Big Data: Privacy and Security Protection Mechanisms

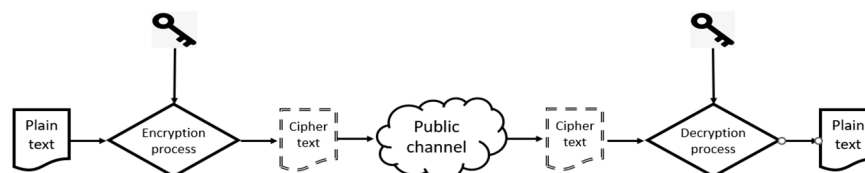
The main goal of this section is to provide a quick overview of available privacy and security protective strategies for protecting medical big data [47–54].

- Encryption

Encryption involves transforming original data from the readable form into an encoded form which is known as cipher text, to prevent unauthorized access to the original data. The encryption method is the most commonly used to protect the confidentiality and integrity of data at storage or during the transfer process. Once the data is encrypted using an appropriate encryption algorithm, using decryption, the cipher text can be transferred back to the original data, as depicted in Figure 5. This encryption can be performed at different levels, such as database level, protocol level, disk-level, and file level, to protect the underlying data. In this regard, in a typical medical setting, a variety of private key cryptographic algorithms and public key algorithms are used to encrypt medical records [23,46,47,55–58].

Even though encryption appears to be the most common solution for protecting the confidentiality and integrity of data, when they are deployed in a resource-constrained

environment, particularly in the resource-constrained medical IoT environment, these algorithms may place an additional load on these resource-constrained IoT devices, which may sometimes affect data communication and proper device functioning. As previously said, these cryptographic algorithms may be divided into two categories based on the algorithm and the number of keys and private and public key cryptography. In private key cryptography or symmetric key cryptography, one key is used wherein the public key cryptography or asymmetric key cryptography two keys known as public and private are used [53], where it is believed that public-key cryptographic algorithms are more secure than private ones.



**Figure 5.** The encryption and decryption flow.

Table 4 depicts the commonly used encryption algorithms that are already available for protecting medical big data in the resource-constrained medical IoT environment.

**Table 4.** Common encryption algorithms that can apply for protecting data in medical environments.

Encryption Algorithm	Employed Technology	Details	References
Data Encryption Standard (DES)	Symmetric key encryption	DES is a symmetric encryption algorithm that uses the same key for both encryption and decryption processes.	[59]
Triple Data Encryption Standard (3DES)	Symmetric key encryption	Triple DES is an advanced version of DES, in which the encryption process passes three rounds during the execution time, as well as the decryption process, unlike in DES, which passes one round only.	[56–58]
Advanced Encryption Standard (AES)	Symmetric key encryption	The encryption and decryption processes use the same key, whereas the length of the key changes frequently in AES.	[60,61]
RSA Encryption	Asymmetric key encryption	This employs a public-key encryption algorithm, which uses two keys: a public key for the encryption process and a private key for the decryption process.	[62,63]
Twofish Encryption	Symmetric key encryption	This employs symmetric key encryption, which proved to be efficient with medical IoT devices with lower processing power.	[64]
Elliptic curve cryptography (ECC)	Asymmetric key encryption	This employs asymmetric key encryption, which is based on the Elliptic curve theory. This has been proven to be efficient in working with resource-constrained IoT devices owing to the low resource consumption nature, which results in improved security when dealing with IoT healthcare applications.	[60,65,66]

Based on these common encryption algorithms, it is evident that there are already algorithms capable of effectively working on resources constrained medical applications, such as Twofish and ECC algorithms.

- Implementation of Access Control mechanisms

Users can manage their data thanks to access control, which determines their identity based on preset regulations that prohibit unauthorized users from accessing resources.

Medical servers, as well as important medical equipment and data, are only accessible to permitted devices and people, thanks to access control systems [1,5]. Access control may be utilized with a variety of encryption schemes, including symmetric and asymmetric encryption, as well as attribute-based encryption [11–14].

- Data auditing

Personal Health Information (PHI) comprises a variety of pathological facts about patients, such as mental health, medical history, and medical test findings, which might be used for profit by attackers [3]. As a result of the high value of this data, a simple data breach might threaten consumers' privacy. As a result, any action that includes the creation or processing of this medical data, as well as its receiving, storage, or transfer, is required to be audited regularly to detect any security flaws [13,16–18].

- Mechanisms for network layer protection

Most medical networks are now constructed on a restricted domain with a network defensive perimeter to guard the internal network against cyber security attacks that may come through the public Internet [7]. This outer medical network layer protects the healthcare institution by preventing outside cyber security attacks from breaching the internal network. In this regard, the network has built up with network defensive techniques and devices such as intrusion prevention systems, intrusion detection systems, firewalls, honeypots, web application firewalls and denial of service protection mechanisms, etc. [18,20,21].

- Data governance

The practice of appropriately controlling and managing medical data is referred to as data governance in healthcare. The objective is to provide a consistent data format that integrates industry standards as well as local and regional norms, allowing for successful data management across all sorts of medical organizations [46,47,50–54,67].

- Authentication

The process of authenticating a user's identification is known as authentication. Insufficient authentication protection schemas might allow intruders to breach internal medical networks and obtain access to sensitive medical data residing in the medical organization. Thus, it is necessary for the frequent authenticating of all users and devices who are accessing medical resources. On the other hand, this user and device authentication is critical for medical systems because it guarantees that data is properly ascribed and that information in the system is only available to authorized parties [23,46,47,51–54].

- Data minimization

Data minimization techniques advise limiting the collection of PHI, however, only to the medical data that is highly essential, as well as the retaining/archiving of sensitive medical data only for as long as the users request [2–4]. This data minimization technique may also lead to reducing the overall archiving and storage cost [48–53].

- Real-time security analytics

Because of the increasing threats, analyzing security and privacy threats and forecasting threat sources in real-time is critical in the healthcare industry. The healthcare business is currently dealing with a slew of sophisticated threats, including ransomware, Distributed Denial of Service (DDoS), and all sorts of malware [10,13,45]. Furthermore, social engineering attacks are becoming more common, and the hazards associated with them are difficult to forecast without taking human cognitive behavior into account. As the healthcare industry embraces developing big data technologies to make better decisions, real-time security analytics should be a major component of any security solution for detecting security and privacy breaches before they occur [52].

### 3.2. Related Work and Discussion

Following an overview of medical big data, privacy and security of medical big data, and protection mechanisms, we provide a summary of related work conducted by other researchers, as shown in Table 5, to emphasize the significance of our study.

**Table 5.** Comparison of related work.

Reference	Survey/Review	Research	Focus on Security	Employed Technologies	Summary of the Scope of the Study
[1]	✗	✓	✓	AI (Machine learning)	The authors present a brief overview of big data and its role in medical care in this study. Further, they also propose a design of a novel secure medical information system to handle medical data in a healthcare environment.
[2]	✗	✓	✓	Cloud computing	In an urban computing environment, the researchers looked at the danger of security and privacy leaks across the life cycle of medical big data.
[3]	✗	✓	✓	Fog computing, Cryptography	The researchers in this study focused on deploying a fog computing facility to secure confidential medical data in the cloud.
[8]	✓	✓	✓	NA	The researchers examined the security and privacy aspects of medical big data, as well as potential solutions.
[9,68]	✓	✗	✓	NA	As they analyze state-of-the-art security and privacy concerns about medical big data, the researchers focus on existing data privacy, data security, and users' access control techniques.
[10]	✗	✓	✗	Mobile computing, Cloud computing	The researchers presented a framework for a mobile cloud-based medical information system based on big data analytics.
[11,14]	✗	✓	✓	IoT, Cryptography	The researchers discussed and proposed a secure industrial IoT architecture for processing the big data collated from sensors for medical applications. They further highlight how data privacy and security are poised to persist as a pivotal facet of healthcare within the IoT ecosystem.
[12]	✗	✓	✗	NA	The researchers presented a management system based on big data to make appropriate healthcare judgments in this study.
[13]	✓	✗	✗	NA	The researchers provide an overview of the current state of big data applications in medical care as well as the problems that governments and healthcare stakeholders face, and the opportunities and possibilities that medical big data presents.
[19]	✓	✗	✓	NA	The researchers examine the legal and ethical problems that big data poses to patient privacy.
[69]	✗	✓	✓	Blockchain, Cloud computing	The study presents a Quantum Cloud-as-a-service for an efficient, scalable, and secure solution for complex Smart Healthcare computations. Their novelty resides in the usage of Quantum Terminal Machines (QTM) and Blockchain technology to enhance the feasibility and security of the proposed architecture.
[20]	✓	✗	✓	NA	The study investigated healthcare data fragmentation, ethical and usability challenges, as well as security and privacy concerns in terms of big data.
[70]	✗	✓	✓	Blockchain, Cryptography	The study proposed a secure Block Chain based mechanism for managing and sharing Electronic Medical Records in medical Big Data using a cryptographic Hash Generator (CHG) in a Hadoop Distributed File System (HDFS)

Table 5. Cont.

Reference	Survey/Review	Research	Focus on Security	Employed Technologies	Summary of the Scope of the Study
[21]	✗	✓	✓	Distributed computing	The researchers presented a brief overview of medical big data and proposed a distributed model for protecting patient data.
[52]	✓	✗	✓	NA	The researchers present a brief review of security and privacy issues in terms of healthcare big data.
[51]	✓	✗	✓	NA	In this study, the research highlights the viable security solutions for medical big data.
[50]	✓	✗	✗	NA	The researchers explore the various use cases of medical big data in their study
[49]	✓	✗	✓	NA	The researchers present a brief review of security challenges in terms of big data, including the solutions for protecting big data.
[71]	✗	✓	✓	Federate learning	The authors put forth an innovative privacy-preserving framework that leverages federated learning to enable big data analysis in IoMT-based environments while ensuring the anonymity of users.
[48]	✗	✓	✓	Blockchain	The researchers devised a blockchain access management method for safeguarding big data.
[72]	✓	✗	✗	NA	The researchers have discussed the big data challenges in the study including the recent status of these challenges.
[73]	✓	✗	✗	NA	The authors present a quick overview of big data in healthcare, as well as recent developments and difficulties.
[74]	✓	✗	✓	NA	The researchers study the potential of blockchain technology for protecting healthcare data hosted within the cloud.
[75]	✓	✗	✓	NA	In this study, the researchers focused on the security and privacy of big data and presented a brief overview of security and privacy requirements.
Our work	✗	✓	✓	Cloud computing, Cryptography	The study presents a comprehensive overview of the role of big data in medical care with an evaluation of the privacy and security implications of such medical big data. Further, we also provide countermeasures summarizing the available literature, highlighting what has been achieved in recent years. On the other hand, we also present a novel access control model for improving the security and privacy of medical big data, which can be used as a base for developing such countermeasure solutions to safeguard from such security and privacy implications.

According to the summarized literature, it is evident that most of the research that has been conducted in recent years employed AI, cloud computing, fog computing, mobile computing, cryptography, and blockchain for developing security solutions for protecting medical big data.

#### 4. System Design and Implementation

Having provided a brief overview of medical big data and its security and privacy implications along with protection mechanisms, the main intention of this section is to highlight our proposed novel access control model for improving the security and privacy of medical big data. Overall, access control determines the user's identity and prohibits unauthorized users from accessing resources. Based on that, we intended to design a novel access control model that prevents unauthorized users from accessing into medical big data stored in the cloud environment. In general, access control models can be divided into three

main categories as Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). For a better understanding, a brief comparison of the above-mentioned access control models is listed on the following Table 6.

**Table 6.** Comparison of access control models.

Access Control Model	Access is Granted	Access Permissions	Examples	Security Implications
DAC	Based on the identity of the user	Permissions are defined on the access control list.	Old versions of Windows/UNIX operating systems	Easily vulnerable to exploit
MAC	Given by the system administrator	The administrator has the full authority to change the security clearance of an object and users.	Most of the military applications	Vulnerable to exploit
RBAC	Based on the role assigned to an end user by the system administrator	An administrator offers a role to a user that includes pre-defined system rights and privileges. After a user has been allocated a role, he or she can only access system resources and complete specified duties described by the designated role. Further, the system administrator centrally manages the responsibilities allocated to users.	Google Cloud, Microsoft Azure/Most of the enterprise applications	More secure and resilient than the MAC and DAC models

According to the reviewed literature, the RBAC model is more advantageous than the MAC and DAC models, but it also has certain problems that must be fixed before it can be deployed. On the other hand, according to the literature, a typical RBAC model can be further improved by including different cryptographic schemes. Thus, the goal of our proposed model is to offer reliable and strong security for medical big data stored in the cloud by utilizing a hybrid cloud architecture and a hybrid cryptographic schema.

Our analysis of the relevant literature has allowed us to weigh the merits and drawbacks of various access control schemes and previous research in this area. Afterward, we decided to adopt a hierarchical RBAC model in our planned architecture since it appears to be effective at delivering the granular security, we need for our access permissions. Our model will be distinguished from all other existing or proposed models by its use of a hybrid cloud architecture (a combination of private and public cloud) and a hybrid encryption schema (RAS 1024-bit and AES 128-bit algorithm) to provide a high level of security. We have employed the AES algorithm to encrypt and decode medical big data stored in the public cloud and the RSA to encrypt the secret key created by the AES and other associated metadata. Our suggested access control system is primarily composed of the entities: a private cloud, public cloud, super user, data owner, management authority, overriding user and end users. The overview of our proposed model is depicted in Figure 6.

As depicted, all the pertinent medical data that has to be accessible by relevant stakeholders will be kept on the public cloud. Data owners, in this scenario, relevant hospital employees such as physicians, radiologists, and so on, would upload all the data obtained from various medical devices to the public cloud. This data will be encrypted using the AES encryption technique when uploaded to the public cloud. The medical organization uses a private cloud to store essential data and metadata, such as encryption keys. A private cloud typically consists of a single server or data center located within the healthcare organization.

Access to this data residing in the public cloud must be permitted by administrative authorities in the healthcare organization before end users or any other users can access it. In this context, the end users might be thought of as the medical personnel, insurance providers, and caregivers who need access to the data housed in the public cloud. Nevertheless, end users are not permitted to make any changes to the public cloud's data or to have any sort of direct communication with the private cloud. Anything having to do with the public cloud falls under the purview of the administrative authority, which also oversees the management of the role hierarchy. When end users seek access to data stored



in the cloud, the managing authority will be present to manage their roles accordingly. Data in the cloud is made available to users based on the roles they have been given and the permissions they have been granted by the governing body. For a better understanding, each of the components of the access control model is explained further as follows.

- Public cloud

The public cloud is responsible for keeping all aggregated medical data, and it is generic storage that is outside of the medical organization's authority. (e.g., Azure, Amazon), thus only encrypted bulky data will be saved. End users and data owners in the medical organization connect directly with this.

- Private cloud

A private cloud can be thought of as an internal data center or server that is situated within a healthcare facility. The private cloud is used solely for the storage of sensitive and confidential data, such as encryption keys and access permissions, among other things. Because the amount of data that is stored in a private cloud is significantly less than that which is retained in a public cloud, using a private cloud takes significantly less processing power and hence has lower expenses. As a result of the fact that this private cloud is an integral component of the organizational infrastructure, medical organizations have the ability to impose their very own security regulations. (For example, using firewalls and honeypots to maximize private cloud security). Thus, this will add an additional layer of protection.

- Administrative authority

A trusted authority within the organization that can authorize role managers and end users to do specific actions. In the event that some users within the organization have an urgent need to access data, the administrative authority can specify settings for such users as override users, thereby providing entire access to the encrypted medical data that has been stored.

- Managing authority

Managing authority oversees role-user relations (role hierarchy). In general, managing authority create roles and categorize encrypted data based on end-user requests, organizational context, and user level. Using the principle of least privilege, the managing authority will grant roles to permitted end users so that these users can access the required data. Managing authority allows for the creation of new roles, which can improve our role-based access schema. These new roles can inherit properties and attributes from higher-level roles. Further, management authority also has the ability to revoke users and restrict the creation of daily roles.

- Data owners

Data owners in medical organizations upload data to the public cloud. He/she can define the relationship between roles and permissions for uploaded resources, ensuring that only authorized users with adequate permission can access encrypted data.

- End user

Any authorized party, whether internal or external, wishes to access the data stored in the cloud.

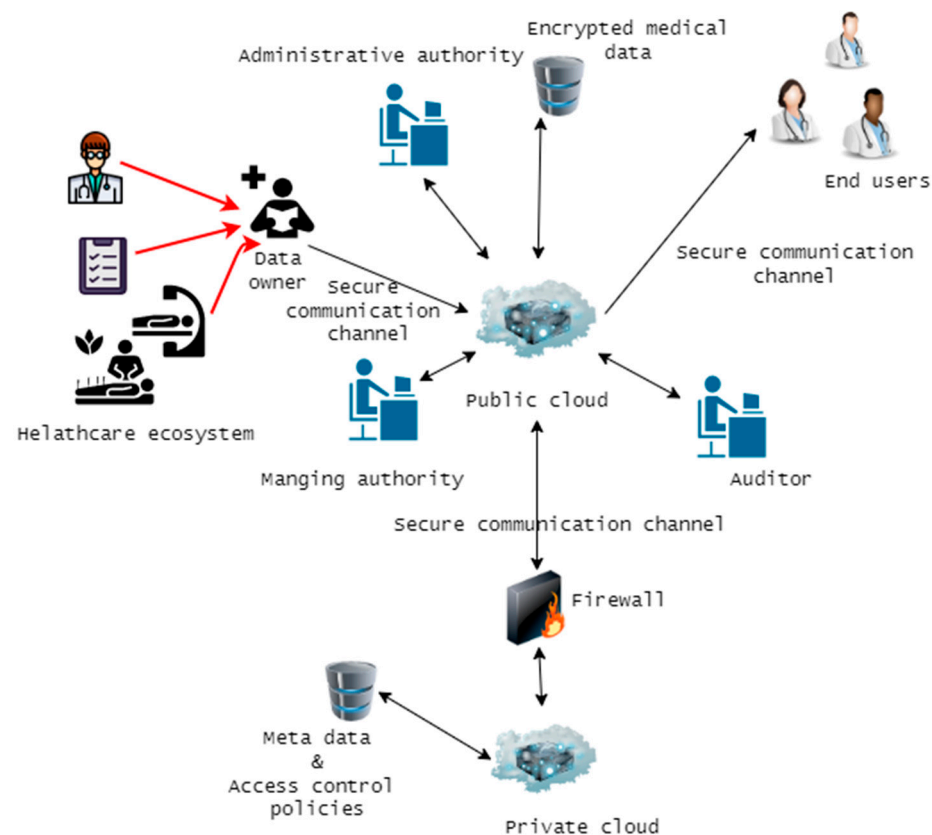
- Auditor

An auditor will keep an eye on system transactions, how users act, and any strange things that happen in the system.

- Override user

In certain circumstances, users within an organization may need immediate access to data in an emergency. Thus, the administrative authority is able to generate parameters for

override users and add them to the system in real-time, with the override user subsequently having complete access to stored big data.



**Figure 6.** Overview of the proposed access control model.

#### Role Based Encryption (RBE)

In general, in the role-based access control model we employed, access rules and users are both mapped to a particular role. Relevant and authorized users are given and assigned roles based on their functionalities and responsibilities within the medical organization. Permissions are given and assigned for the roles instead of users. Thus, users who have been assigned to a particular role only can access the data. Overall, the RBE schema is used to develop and enforce the RBAC system. In the RBE schema, roles are arranged in a hierarchy such as a tree structure where one role can inherit the properties from other roles.

As aforementioned RBE scheme is able to handle role hierarchies where one role can inherit the properties from another role. In general, users can be added at any time into the role even after the owner has encrypted the data, and the owner does not have to re-encrypt the data if they want to add a new user to any of the roles. Also, a user can be revoked at any time from the role, and after revoking, they will not be authorized anymore to access any of the encrypted data. Revoking the users does not affect role hierarchy and user management as well.

In our model, RBE helps to enforce the RBAC policies on encrypted data stored on the cloud, which act as the foundation for our proposed access control model.

Figure 7 shows an example of RBE. It consists of four roles created in a hierarchical structure. According to Figure 7, role R2 inherits the properties from roles R4 and R3, and role R1 inherits from role R2.

As an example, suppose the data owner runs an encryption logic and encrypts the Message  $M$  using role R3. Assume that role R1 has a set of user members  $U1, U2, U3$

$$R1 = \{U1, U2, U3\}$$

User U1 wants to decrypt the data encrypted by an owner. Now because role R1 is inherited from R2, and R2 is inherited from R3, user U1 from role R1 is authorized to access and decrypt the message *M*. Then user U1 can successfully decrypt the message *M* by performing decryption logic.

After reviewing the key aspects of our model in the previous part, we will now examine the model's workflow as depicted in Figure 8.

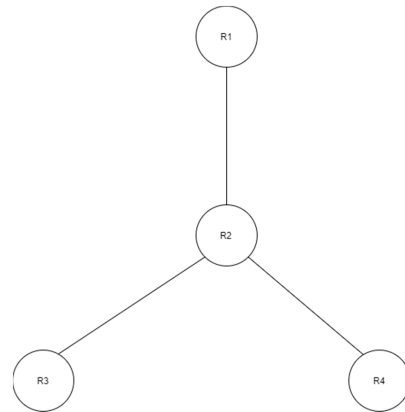


Figure 7. RBE role hierarchy.

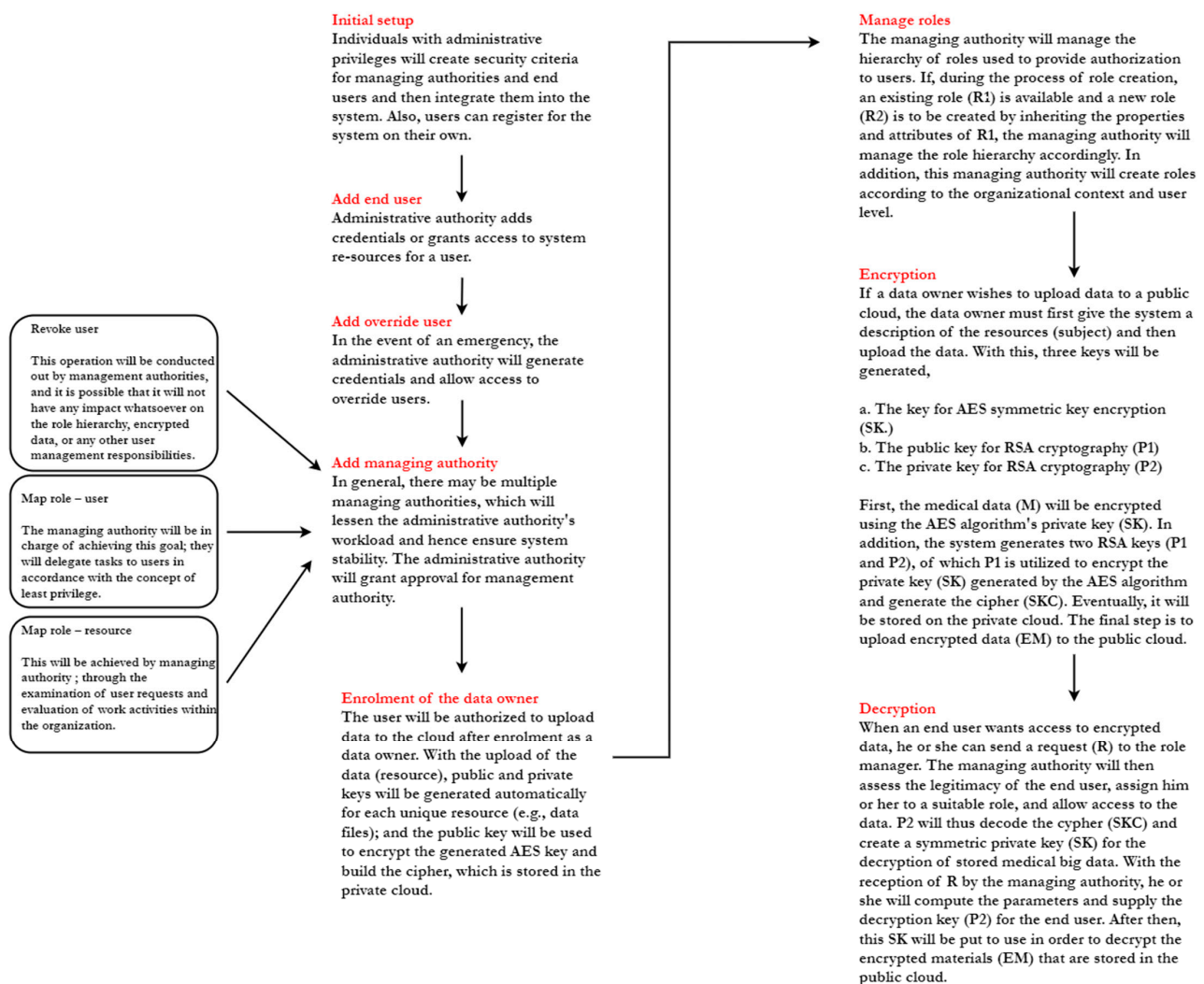


Figure 8. Workflow of the proposed access control model.

## 5. Implementation Results and Discussion

To demonstrate the validity of our proposed model, we deployed it in a real cloud environment with Microsoft Azure. We utilized Visual Studio 2019 integrated development environment with C# and the ASP.NET web development framework to design our data storage access control model. For the deployment, we utilized a Microsoft Azure cloud instance comprised of a single core, 50 GB of storage, and 4 GB of RAM. In order to depict a private cloud, we utilized an Azure SQL server instance with an integrated firewall and 2 GB of storage, as doing this in a real-world setting would be more expensive and takes time. A virtual private network tunnel has been created between the public and private cloud, and we assumed that all medical data would be sent to this public cloud, where our access control model has been implemented as a Software as a service (SAAS) on the cloud. Figure 9 showcases the steps involved in the design of our access control model. The first step involves designing the data storage access control mode using C# and ASP.NET programming languages. The second and third steps involve choosing a public cloud instance and choosing a private cloud. Upon successful selection, the design model was deployed as SAAS in the public cloud. Figures 10 and 11 demonstrate the implemented model in the cloud.

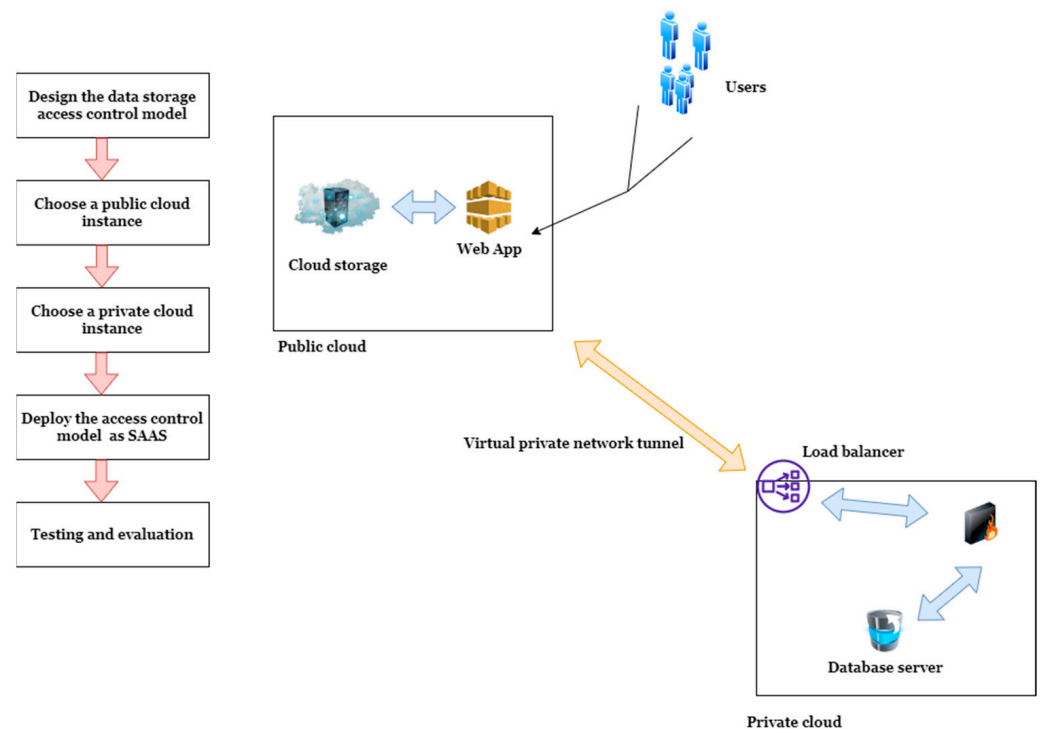


Figure 9. Steps involved in the design of our access control model.

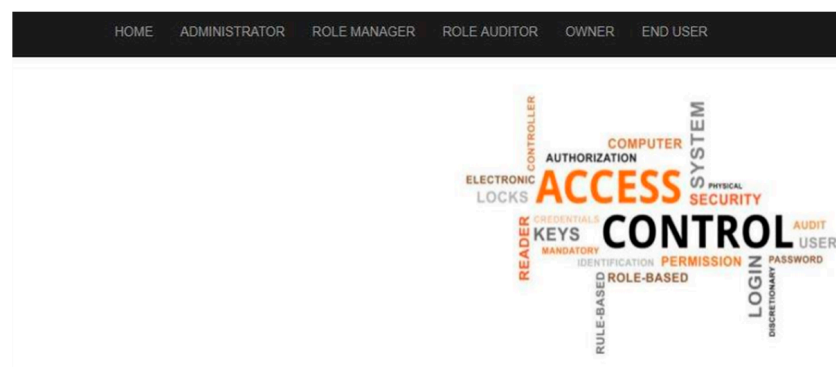
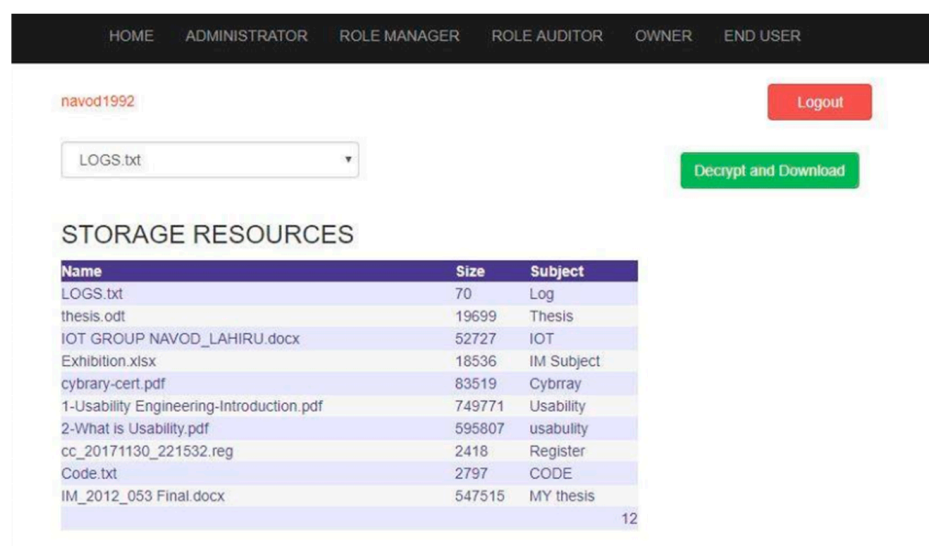


Figure 10. Cloud deployed model.



**Figure 11.** End user requests for cloud resources.

As we have used the AES symmetric key algorithm for the encryption and decryption of the input data, the AES symmetric key encryption algorithm uses the key generated by the cryptographic Random Number Generator (RNG) using the implementation provided by the cryptographic service provider (CSP) in .NET software development framework. On the other hand, public key encryption performs using the implementation of the RSA algorithm provided by CSP. Further, using AesManaged Class in the .NET framework, the AES algorithm was also implemented.

Table 7 presents the tools/components we used for the design/testing and evaluation of our access control model with their purpose.

**Table 7.** Components we have used for deployment and testing.

Purpose	Tools/Components
Integrated development environment	Visual Studio 2019
Programming languages	C#/ASP.NET
Public cloud	Microsoft Azure cloud instance
Private cloud	Azure SQL server instance
Software for data integrity testing	MD5 and SHA Checksum Utility
Tools used for initial reconnaissance	DNSenum and DMitry
Tools used for port and service scanning	Nmap
Tools used for vulnerability analysis	SPARTA, VEGA, and OWASP Zed Attack Proxy

Upon the successful deployment, we tested our model for performance, data integrity, security implications, and functional requirements, which are discussed in detail in forthcoming sections.

### 5.1. Performance Testing

In order to determine how well the implemented model works, we experimented with it using files of different sizes and assessed how long it took to encrypt and decrypt data while maintaining the same connection bandwidth. Figure 12 illustrates the amount of time required for encryption as well as for decryption, for the same file under the same connection bandwidth.

The y-axis shows time in milliseconds, and the X-axis represents the size in bytes.

Based on the results, we were able to extrapolate that the encryption time required more time than the decryption time, and we can see that the amount of time required for both encryption and decryption progressively increases as the size increases.

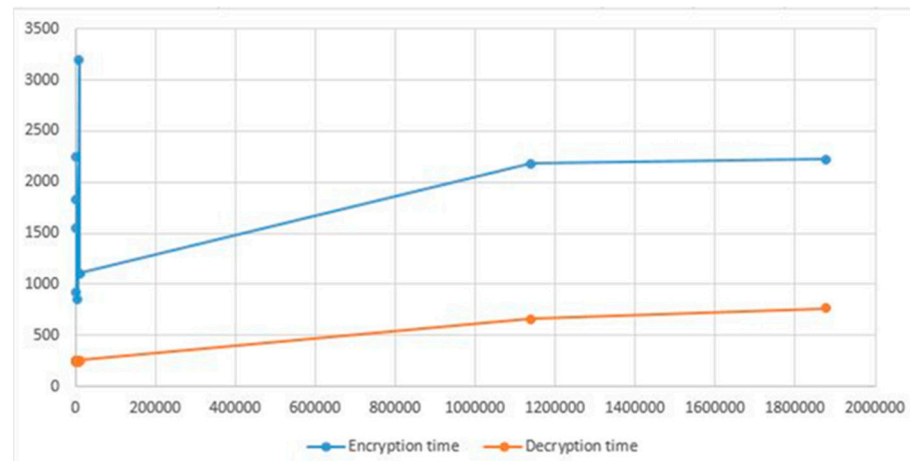


Figure 12. Encryption and decryption time.

### 5.2. Data Integrity Testing

In order to ensure that the data stored in cloud resources are accurate, data integrity testing has been carried out, as depicted in Figure 13. We were able to do this by comparing and verifying the SHA-512, SHA-1, SHA-256 and MD5 values of the original cloud resources as well as the decrypted cloud resources that were downloaded. It provided the same value for the integrity of the data for both the original resources and the ones that were downloaded. As a result, we came to the conclusion that the integrity of the files containing the resources was maintained throughout the process of encryption and decryption. This demonstrated that our approach was both reliable and trustworthy.

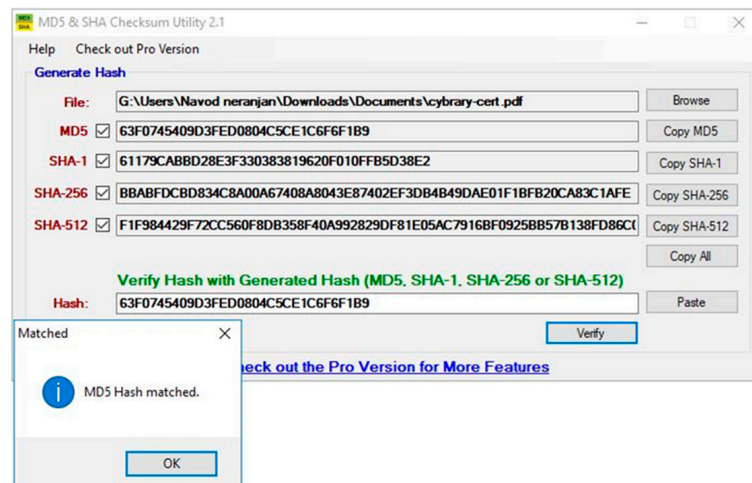


Figure 13. Testing for data integrity.

### 5.3. Security Implication Testing

To verify the security implications against cyber-attacks, three vulnerability assessment activities has conducted in a cloud environment, which are discussed in detail in the following.

1. Initial Reconnaissance
2. Port and service scanning,
3. Vulnerability analysis

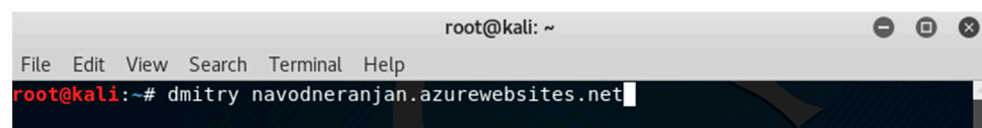


Initial reconnaissance was carried out with the assistance of the programs DNSenum and DMitry. After that, we carried out a Nmap scan in order to locate ports that were left open and collect further data. The tools SPARTA, VEGA, and OWASP Zed Attack Proxy were then utilized in order to do the vulnerability analysis.

Upon the successful deployment of our model into the cloud, first, we used DNSenum and DMitry (Deepmagic Information Gathering Tool) for reconnaissance of our target host, as shown in Figures 14 and 15. DNSenum is a tool that is designed for the purpose of enumerating DNS information about a domain. DMitry is a UNIX/(GNU) Linux Command Line Application coded in C. It has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, TCP port scan, WHOIS lookups, and more.

```
root@kali:~# dnsenum http://navodneranjan.azurewebsites.net
```

Figure 14. DNS enumeration using DNSenum.

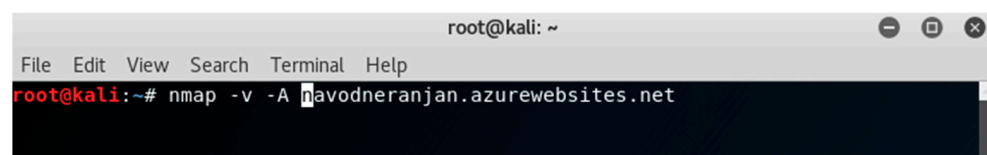


```
root@kali:~# dmity navodneranjan.azurewebsites.net
```

Figure 15. Reconnaissance using DMitry.

Afterward, in an attempt to identify the potential attack surface, we examined the name servers associated with the domain name (Hosted URL), where we were able to gather the host IP address and DNS information about our host.

Upon gathering the required information (IP address and DNS information), we then performed a Nmap scan to find out about open ports and gather more information about our host, as shown in Figure 16.



```
root@kali:~# nmap -v -A navodneranjan.azurewebsites.net
```

Figure 16. Deep reconnaissance using Nmap.

Upon completing the scanning process, we managed to gather all open ports of our target host, SSL certificate information, and server information, outlined in the following.

- Open ports: Port 80 (TCP) and Port 443 (TCP)
- Server information: Microsoft IIS server 8.0
- SSL certificate information: Public key encrypted SSL connection that uses 2048 bits key.

As there were two open ports and it is protected by a public load balancer and a firewall built into the Azure public cloud, we then analyzed our target host using SPARTA and VEGA vulnerability analysis tools to check if any vulnerabilities are there to exploit. The acquired findings demonstrated that our model could resist the majority of the cyberattacks because the test results did not display any common vulnerabilities and exposures (CVE). Hence, with that, we have proven that our access control model can withstand the latest cyber-attacks as no vulnerabilities are present.

#### 5.4. Functional Requirement Analysis

In order to verify the functional needs of our model, we compared it to standard access control models available for cloud computing that are available in the literature. Our comparison was focused on the similarities and differences in the functions and features that all these types of models provide, as shown in Table 8. From the comparison, it is evident that our access control model features all the criteria outlined in Table 8 as opposed

to other sorts of access control models. In Table 8, Yes, will be denoted as Y, and No will be denoted as N.

#### 1. Least Privilege principle

Whenever a user requests to access a resource, the role manager will look for available roles to grant the least access privileges for the user, or else the role manager will create a new role and assign access permissions and resources and assign for the user. In simple terms, this is all about granting only needed permissions for the users to access resources.

#### 2. Separation of duties

Separation of duties is a principle that is supported by the least privilege principle, and it aims to partition tasks and duties associated with roles in order to prevent granting too much authority to a single user.

#### 3. Scalability

Our model is mainly introduced for an organizational level and but it can be scalable as per the environment. If there are a large number of users, there should have several role managers and system administrators to handle the user requests and role management as per our designed model.

#### 4. Auditing

Our model provides a convenient way of auditing the underlying transactions in the access control system. Those auditing and log information would be collected by the role auditor and check the underlying transactions and user behavior.

#### 5. Policy management

Our model supports policy management (Add, Revoke, Add constraints), and it would help to organize relations between users, administrators, and data owners.

#### 6. Flexibility of configuration

Our model is flexible enough to be configured in the cloud computing environment both as a SAAS and Platform as a Service (PAAS).

#### 7. Delegation of capabilities

To make our model more flexible and allows for flexible role management, a delegation of capabilities is essential between all the stakeholders, which has already been demonstrated through this research.

#### 8. Hybrid cloud architecture

Our model uses employs a hybrid cloud architecture (public cloud and private cloud) to enhance the security of our model.

#### 9. Role hierarchy management

Role manager manages the role hierarchy; hence, newly created roles can inherit the access permission and assigned resources from the existing roles in our model, and it will help to provide hierarchical role-based access control.

### 5.5. Discussion

In the research, we employed a cryptographic role-based access control system with a hybrid cloud architecture, with the aim of demonstrating a novel role-based access control model for medical organizations to upload their medical big data in the cost-effective public cloud while storing mission-critical access control-related data in the private cloud. Overall, we believe, apart from healthcare, that the proposed system can be adopted in various other domains as it implements the hierarchical cryptographic role-based access control policies based on the job function and user requests in an organization for providing secure data storage in a real cloud environment. Even though there are underlying security mechanisms employed by public cloud services, such as Microsoft Azure, AWS, and Google

Cloud, if the hosted web services are vulnerable enough to exploit, it may lead any attackers to compromise the system endangering the lives of patients. However, in our research, we have relied totally on the public cloud and employed a hybrid cloud architecture to deploy our software-based access control model and proved it could withstand cyber-attacks and offer many convenient facilities compared to other models. On the other hand, in light of the cost, as we relied mostly on the public cloud, only a low cost would be spent to design the access control model compared to other available solutions outlined in Table 5.

**Table 8.** Analysis of functional requirements.

Comparison Criteria	DAC	MAC	RBAC	Our Model
Least privilege principle	N	N	Y	Y
Separation of duties	N	N	Y	Y
Scalability	N	N	Y	Y
Auditing	Y	Y	Y	Y
Policy management	Y	N	Y	Y
Flexibility for configuration	N	N	Y	Y
Delegation of capabilities	Y	N	N	Y
Hybrid cloud architecture	N	N	N	Y
Role hierarchy management	N	N	Y	Y
Fine-grained access control	N	N	Y	Y

On the whole, big data has undeniable benefits for the healthcare industry, without any doubt. Security and privacy, on the other hand, are key issues that big data in healthcare faces as of now, according to the literature we have reviewed. Based on the summarization (see Table 5), it is evident that many researchers have contributed to this subject, where many have conducted surveys/reviews and research towards security and privacy aspects of medical big data. Further, medical information is always vulnerable to security concerns such as inappropriate patient information disclosure, unauthorized use of patient information, unauthorized data loss, and many more, as we discussed earlier. As a result, the relevant stakeholders in healthcare should take appropriate actions toward the protection of this medical data so that the data can be protected. On the other hand, when designing/setting up the medical environment and designing and deployment of security solutions, the relevant stakeholders should think that security and privacy protection should be an essential and integral part of the big data life cycle, which is data generation [75–79], data processing and data storage where optimal protection can be guaranteed to the underlying big data. For the healthcare system to profit from the use of big data in healthcare, the following resolves should be made for the effective utilization of big data so that maximum protection can be guaranteed:

- Healthcare data should be sufficiently safeguarded and secured as security and privacy risks are imminent.
- When studying big data in healthcare, tools that assure maximum protection for underlying big data need to be employed.
- Healthcare data should be protected throughout its life cycle by adopting the above-mentioned and discussed security mechanisms.
- The adoption of an audit trail system should be an added advantage, as all the transactions can be traced.

## 6. Conclusions

The use of big data has the potential to transform healthcare to new levels. However, challenges such as security and privacy impede the success of the technology, which must be addressed urgently. In this study, the security and privacy aspects associated with medical

big data were examined, and the need for security and privacy preventive mechanisms was also discussed. Further, a novel cloud-enabled hybrid access control model was proposed that can be used to construct safe medical big data solutions. The review we have performed emphasized that security and privacy preventive mechanisms should be an integral part of the medical big data lifecycle, from data generation to processing and storage. The study also collated knowledge and proposed that secure patient data management is an essential part of global healthcare. The proposed novel access control model for medical big data was evaluated, and related work was summarized. Overall, the proposed access control model can be utilized for organizations, both for commercial and non-commercial purposes, where access control can be categorized according to job functions in the organization. By doing so, the proposed model enables relevant stakeholders to store and access medical big data in a secure way. We have experimented role-based encryption and used it for implementing role-based access control for public cloud storage using hybrid cryptographic schema and hybrid cloud architecture, as the architecture itself provided more security and reliability. Even though there are underlying security mechanisms used by public cloud services such as Microsoft Azure, AWS, Google Cloud, and Alibaba Cloud, if the web applications or hosted services are vulnerable enough to exploit, it may lead any of the attacker to compromise the entire ecosystem. When the time goes by and as technology evolves, all our data will be in the cloud, including big data, rather than having them on physical data storage. Eventually, storage and hosting costs for the cloud may go down, and attacks for the cloud may increase to compromise confidential data on the cloud. Hence the proposed access control model can be improved by better encryption schema and empowered by rigid efficient authentication schema as per the future work. On the other hand, the proposed model can be integrated with artificial intelligence-enabled solutions for designing more robust, secure access control models for real-time threat detection and prevention. The contributions of this study aim to pave the way for future researchers to work in this area, recognizing that security and privacy are paramount concerns for researchers in this field.

**Author Contributions:** Methodology, A.A. and N.N.T.; Software, N.N.T.; Validation, N.N.T.; Investigation, N.N.T.; Resources, N.N.T.; Writing—original draft, N.N.T.; Writing—review & editing, A.A. and K.K.; Funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by Qassim University.

**Acknowledgments:** Researchers would like to thank the Deanship of Scientific Research, Qassim University for funding the publication of this project.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Kaur, P.; Sharma, M.; Mittal, M. Big Data and Machine Learning Based Secure Healthcare Framework. *Procedia Comput. Sci.* **2018**, *132*, 1049–1059. [CrossRef]
2. Jiang, R.; Shi, M.; Zhou, W. A Privacy Security Risk Analysis Method for Medical Big Data in Urban Computing. *IEEE Access* **2019**, *7*, 143841–143854. [CrossRef]
3. al Hamid, H.A.; Rahman, S.M.M.; Hossain, M.S.; Almogren, A.; Alamri, A. A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography. *IEEE Access* **2017**, *5*, 22313–22328. [CrossRef]
4. Mae, R. 22 Big Data Applications & Examples | Built in. 2022. Available online: <https://builtin.com/big-data/big-data-examples-applications> (accessed on 4 February 2023).
5. David, T. What Is Big Data? Introduction, Types, Characteristics, Examples. 2023. Available online: <https://www.guru99.com/what-is-big-data.html> (accessed on 4 February 2023).
6. Batko, K.; Ślęzak, A. The use of Big Data Analytics in healthcare. *J. Big Data* **2022**, *9*, 1–24. [CrossRef]
7. Christo, P. 25+ Impressive Big Data Statistics for 2023. 2023. Available online: <https://techjury.net/blog/big-data-statistics/#gref> (accessed on 4 February 2023).
8. Abouelmehdi, K.; Beni-Hessane, A.; Khaloufi, H. Big healthcare data: Preserving security and privacy. *J. Big Data* **2018**, *5*, 1–18. [CrossRef]

9. Siddique, M.; Mirza, M.A.; Ahmad, M.; Chaudhry, J.; Islam, R. A survey of big data security solutions in healthcare. In *Security and Privacy in Communication Networks: 14th International Conference, SecureComm 2018, Singapore, 8–10 August 2018, Proceedings, Part II*; Springer International Publishing: Cham, Switzerland, 2018; Volume 255, pp. 391–406. [\[CrossRef\]](#)
10. Youssef, A.E. A Framework for Secure Healthcare Systems Based on Big Data Analytics in Mobile Cloud Computing Environments. *Int. J. Ambient. Syst. Appl.* **2014**, *2*, 1–11. [\[CrossRef\]](#)
11. Manogaran, G.; Thota, C.; Lopez, D.; Sundarasekar, R. Big Data Security Intelligence for Healthcare Industry 4.0. In *Cybersecurity for Industry 4.0*; Springer: Cham, Switzerland, 2017; pp. 103–126. [\[CrossRef\]](#)
12. Manogaran, G.; Thota, C.; Lopez, D.; Vijayakumar, V.; Abbas, K.M.; Sundarsekar, R. Big Data Knowledge System in Healthcare. *Stud. Big Data* **2017**, *23*, 133–157. [\[CrossRef\]](#)
13. Jee, K.; Kim, G.H. Potentiality of Big Data in the Medical Sector: Focus on How to Reshape the Healthcare System. *Health Inf. Res.* **2013**, *19*, 79–85. [\[CrossRef\]](#)
14. Karatas, M.; Eriskin, L.; Deveci, M.; Pamucar, D.; Garg, H. Big Data for Healthcare Industry 4.0: Applications, challenges and future perspectives. *Expert Syst. Appl.* **2022**, *200*, 116912. [\[CrossRef\]](#)
15. Miah, S.J.; Camilleri, E.; Vu, H.Q. Big Data in Healthcare Research: A survey study. *J. Comput. Inf. Syst.* **2021**, *62*, 480–492. [\[CrossRef\]](#)
16. Pranjali Bora. Big Data in Healthcare: All You Need to Know. Digital Authority Partners (DAP). 2022. Available online: <https://www.digitalauthority.me/resources/big-data-in-healthcare/> (accessed on 11 February 2023).
17. Jagadeeswari, V.; Subramaniaswamy, V.; Logesh, R.; Vijayakumar, V. A study on medical Internet of Things and Big Data in personalized healthcare system. *Health Inf. Sci. Syst.* **2018**, *6*, 14. [\[CrossRef\]](#) [\[PubMed\]](#)
18. Kankanhalli, A.; Hahn, J.; Tan, S.; Gao, G. Big data and analytics in healthcare: Introduction to the special section. *Inf. Syst. Front.* **2016**, *18*, 233–235. [\[CrossRef\]](#)
19. Price, W.N.; Cohen, I.G. Privacy in the age of medical big data. *Nat. Med.* **2019**, *25*, 37–43. [\[CrossRef\]](#) [\[PubMed\]](#)
20. Olaronke, I.; Oluwaseun, O. Big data in healthcare: Prospects, challenges and resolutions. In *Proceedings of the FTC 2016—Proceedings of Future Technologies Conference, San Francisco, CA, USA, 6–7 December 2016*; pp. 1152–1157. [\[CrossRef\]](#)
21. Sarkar, B.K. Big data for secure healthcare system: A conceptual design. *Complex Intell. Syst.* **2017**, *3*, 133–151. [\[CrossRef\]](#)
22. Thilakarathne, N.N.; Kagita, M.K.; Gadekallu, T.R. The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study. *SSRN Electron. J.* **2020**. [\[CrossRef\]](#)
23. Thilakarathne, N.N. Review on the Use of ICT Driven Solutions Towards Managing Global Pandemics. *J. ICT Res. Appl.* **2021**, *14*, 207–225. [\[CrossRef\]](#)
24. Arvind, K.S.; Vanitha, S.; Suganya, K.S. Pandemic Management Using Internet of Things and Big Data—A Security and Privacy Perspective. In *IoT and Big Data Analytics for Smart Cities*; Chapman and Hall: London, UK; CRC: Boca Raton, FL, USA, 2022; pp. 159–173. [\[CrossRef\]](#)
25. Hulsén, T.; Jamuar, S.S.; Moody, A.R.; Karnes, J.H.; Varga, O.; Hedensted, S.; Spreafico, R.; Hafner, D.A.; McKinney, E.F. From big data to precision medicine. *Front. Med.* **2019**, *6*, 34. [\[CrossRef\]](#)
26. Kavidopoulou, A.; Syrigos, K.N.; Makrogikias, S.; Dlamini, Z.; Hull, R.; Marima, R.; Skepu, A.; Koumoulos, E.P.; Bakas, G.; Vamvakaris, I.; et al. AI and Big Data for Drug Discovery. In *Trends of Artificial Intelligence and Big Data for E-Health*; Springer International Publishing: Cham, Switzerland, 2022; pp. 121–138. [\[CrossRef\]](#)
27. Raghupathi, W.; Raghupathi, V. Big data analytics in healthcare: Promise and potential. *Health Inf. Sci. Syst.* **2014**, *2*, 1–10. [\[CrossRef\]](#)
28. Patel, S.; Patel, A. A big data revolution in health care sector: Opportunities, challenges and technological advancements. *Int. J. Inf. Sci. Technol.* **2016**, *6*, 155–162. [\[CrossRef\]](#)
29. Kim, M.-J.; Yu, Y.-S. Development of Real-time Big Data Analysis System and a Case Study on the Application of Information in a Medical Institution. *Int. J. Softw. Eng. Its Appl.* **2015**, *9*, 93–102. Available online: <https://www.earticle.net/Article/A251363> (accessed on 5 February 2023). [\[CrossRef\]](#)
30. Chawla, N.V.; Davis, D.A. Bringing big data to personalized healthcare: A patient-centered framework. *J. Gen. Intern. Med.* **2013**, *28*, 660–665. [\[CrossRef\]](#) [\[PubMed\]](#)
31. Kuriyan, J.; Cobb, N. Forecasts of Cancer and Chronic Patients: Big Data Metrics of Population Health. *arXiv* **2013**, arXiv:1307.3434.
32. Abinaya, K. Data Mining with Big Data e-Health Service Using Map Reduce. *Int. J. Adv. Res. Comput. Commun. Eng.* **2015**, 123–127. [\[CrossRef\]](#)
33. Wang, L.; Alexander, C.A. Big data analytics as applied to diabetes management. *Eur. J. Clin. Biomed. Sci.* **2016**, *2*, 29–38. [\[CrossRef\]](#)
34. Shinde, K.V. A real time monitoring system in healthcare with hadoop. *Res. Journey Int. Multidiscip. E-Res. J.* **2016**. Available online: <https://researchjourney.net/upload/April-May-June%202016/3-K%20.V.%20SHINDE%20-%20Supplementary%20Issue-international%20conference-Cover%20page%20-Editorial%20Board%20-Index.pdf> (accessed on 5 February 2023).
35. Luo, J.; Wu, M.; Gopukumar, D.; Zhao, Y. Big data application in biomedical research and health care: A literature review. *Biomed. Inform. Insights* **2016**, *8*, BII.S31559. [\[CrossRef\]](#)
36. Balladini, J.; Rozas, C.; Frati, E.; Vicente, N.; Lima, C.O.L. Big Data Analytics in Intensive Care Units: Challenges and applicability in an Argentinian Hospital. *J. Comput. Sci. Technol.* **2015**, *15*, 61–67. Available online: <http://www.merriam-webster.com/dictionary/continuous> (accessed on 11 February 2023).



37. Boukenze, B.; Mousannif, H.; Haqiq, A. A conception of a predictive analytics platform in healthcare sector by using data mining techniques and Hadoop. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2016**.
38. Herland, M.; Khoshgoftaar, T.M.; Wald, R. A review of data mining using big data in health informatics. *J. Big Data* **2014**, *1*, 2. [\[CrossRef\]](#)
39. Belle, A.; Thiagarajan, R.; Soroushmehr, S.M.R.; Navidi, F.; Beard, D.A.; Najarian, K. Big data analytics in healthcare. *Biomed. Res. Int.* **2015**, *2015*. [\[CrossRef\]](#)
40. Salerno, J.; Knoppers, B.M.; Lee, L.M.; Hlaing, W.W.M.; Goodman, K.W. Ethics, big data and computing in epidemiology and public health. *Ann. Epidemiol.* **2017**, *27*, 297–301. [\[CrossRef\]](#) [\[PubMed\]](#)
41. Vayena, E.; Salathé, M.; Madoff, L.C.; Brownstein, J.S. Ethical Challenges of Big Data in Public Health. *PLoS Comput. Biol.* **2015**, *11*, e1003904. [\[CrossRef\]](#)
42. Pastorino, R.; De Vito, C.; Migliara, G.; Glocker, K.; Binenbaum, I.; Ricciardi, W.; Boccia, S. Benefits and challenges of Big Data in healthcare: An overview of the European initiatives. *Eur. J. Public Health* **2019**, *29*, 23–27. [\[CrossRef\]](#)
43. Kalinaki, K.; Thilakarathne, N.N.; Mubarak, H.R.; Malik, O.A.; Abdullatif, M. Cybersafe Capabilities and Utilities for Smart Cities. In *Cybersecurity for Smart Cities*; Springer: Cham, Switzerland, 2023; pp. 71–86.
44. Martin-Sanchez, F.; Verspoor, K. Big data in medicine is driving big changes. *Yearb. Med. Inf.* **2014**, *9*, 14–20. [\[CrossRef\]](#)
45. Alli, A.A.; Kassim, K.; Mutwalibi, N.; Hamid, H.; Ibrahim, L. Secure Fog-Cloud of Things: Architectures, Opportunities and Challenges. In *Secure Edge Computing*, 1st ed.; Ahmed, M., Haskell-Dowland, P., Eds.; CRC Press: Boca Raton, FL, USA, 2021; pp. 3–20.
46. Thilakarathne, N.N.; Kagita, M.K.; Gadekallu, T.R.; Maddikunta, P.K.R. The Adoption of ICT Powered Healthcare Technologies towards Managing Global Pandemics. *arXiv* **2020**, arXiv:2009.05716.
47. Mahendran, R.K.; Velusamy, P. A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. *Comput. Commun.* **2020**, *153*, 545–552. [\[CrossRef\]](#)
48. Uchibeke, U.U.; Schneider, K.A.; Kassani, S.H.; Deters, R. Blockchain Access Control Ecosystem for Big Data Security. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1373–1378. [\[CrossRef\]](#)
49. Benjelloun, F.-Z.; Lahcen, A.A. Big Data Security. In *Web Services: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2019; pp. 25–38. [\[CrossRef\]](#)
50. Kuo, M.H.; Sahama, T.; Kushniruk, A.W.; Borycki, E.M.; Grunwell, D.K. Health big data analytics: Current perspectives, challenges and potential solutions. *Int. J. Big Data Intell.* **2014**, *1*, 114. [\[CrossRef\]](#)
51. Rao, S.; Suma, S.N.; Sunitha, M. Security Solutions for Big Data Analytics in Healthcare. In Proceedings of the 2015 2nd IEEE International Conference on Advances in Computing and Communication Engineering, ICACCE 2015, Dehradun, India, 1–2 May 2015; pp. 510–514. [\[CrossRef\]](#)
52. Patil, H.K.; Seshadri, R. Big data security and privacy issues in healthcare. In Proceedings of the 2014 IEEE International Congress on Big Data, BigData Congress, Anchorage, AK, USA, 27 June–2 July 2014; pp. 762–765. [\[CrossRef\]](#)
53. Iadarola, G.; Poli, A.; Spinsante, S. Compressed Sensing of Skin Conductance Level for IoT-based wearable sensors. In Proceedings of the 2022 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Ottawa, ON, Canada, 16–19 May 2022; IEEE: Piscataway, NJ, USA; pp. 1–6.
54. Iadarola, G.; Disha, D.; De Santis, A.; Spinsante, S.; Gambi, E. Global Positioning System measurements: Comparison of IoT wearable devices. In Proceedings of the 2022 IEEE 9th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Pisa, Italy, 27–29 June 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 213–218.
55. Casaccia, F.; Iadarola, G.; Poli, A.; Spinsante, S. CS-Based Decomposition of Acoustic Stimuli-Driven GSR Peaks Sensed by an IoT-Enabled Wearable Device. In *IoT Technologies for Health Care: 8th EAI International Conference, HealthyIoT 2021, Virtual Event, 24–26 November 2021*; Springer International Publishing: Cham, Switzerland, 2021; pp. 166–179.
56. Ramya Devi, R.; Vijaya Chamundeeswari, V. Triple DES: Privacy Preserving in Big Data Healthcare. *Int. J. Parallel. Program.* **2020**, *48*, 515–533. [\[CrossRef\]](#)
57. Abiodun, M.K.; Awotunde, J.B.; Ogundokun, R.O.; Adeniyi, E.A.; Arowolo, M.O. Security and Information Assurance for IoT-Based Big Data. *Stud. Comput. Intell.* **2021**, *972*, 189–211. [\[CrossRef\]](#)
58. Ramachandra, M.N.; Rao, M.S.; Lai, W.C.; Parameshachari, B.D.; Babu, J.A.; Hemalatha, K.L. An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard. *Big Data Cogn. Comput.* **2022**, *6*, 101. [\[CrossRef\]](#)
59. Sarosh, P.; Parah, S.A.; Bhat, G.M.; Muhammad, K. A Security Management Framework for Big Data in Smart Healthcare. *Big Data Res.* **2021**, *25*, 100225. [\[CrossRef\]](#)
60. Fatima, S.; Hussain, S.; Shahzadi, N.; Din, B.U.; Sajjad, W.; Saleem, Y.; Aun, M. A Secure Framework for IoT Healthcare Data Using Hybrid Encryption. In Proceedings of the 2022 International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETEECTE), Lahore, Pakistan, 2–4 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7. [\[CrossRef\]](#)
61. Gadde, S.; Amutharaj, J.; Usha, S. A security model to protect the isolation of medical data in the cloud using hybrid cryptography. *J. Inf. Secur. Appl.* **2023**, *73*, 103412. [\[CrossRef\]](#)



62. Sharma, K.; Agrawal, A.; Pandey, D.; Khan, R.A.; Dinkar, S.K. RSA based encryption approach for preserving confidentiality of big data. *C-Comput. Inf. Sci.* **2022**, *34*, 2088–2097. [\[CrossRef\]](#)
63. Sharma, D.; Kawatra, R. Security Techniques Implementation on Big Data Using Steganography and Cryptography. *Lect. Notes Netw. Syst.* **2023**, *517*, 279–302. [\[CrossRef\]](#)
64. Jayasankar, T.; Bhavadharini, R.M.; Nagarajan, N.R.; Mani, G.; Ramesh, S. Securing Medical Data using Extended Role Based Access Control Model and Twofish Algorithms on Cloud Platform. *Eur. J. Mol. Clin. Med.* **2021**, *8*, 2021. Available online: [https://ejmcm.com/article\\_6677\\_f9876c57ebfe46bd9508546774432d82.pdf](https://ejmcm.com/article_6677_f9876c57ebfe46bd9508546774432d82.pdf) (accessed on 18 February 2023).
65. Nayak, L.; Jayalakshmi, V. A Study of Securing Healthcare Big Data using DNA Encoding based ECC. In Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021, Coimbatore, India, 20–22 January 2021; pp. 348–352. [\[CrossRef\]](#)
66. Sreedevi, A.G.; Harshitha, T.N.; Sugumaran, V.; Shankar, P. Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review. *Inf. Process. Manag.* **2022**, *59*, 102888. [\[CrossRef\]](#)
67. Jiang, R.; Han, S.; Yu, Y.; Ding, W. An access control model for medical big data based on clustering and risk. *Inf. Sci.* **2023**, *621*, 691–707. [\[CrossRef\]](#)
68. Ahtesham, M. Bigdata Applications in Healthcare: Security and Privacy Challenges. *Lect. Notes Netw. Syst.* **2022**, *455*, 231–240. [\[CrossRef\]](#)
69. el Azzaoui, A.; Sharma, P.K.; Park, J.H. Blockchain-based delegated Quantum Cloud architecture for medical big data security. *J. Netw. Comput. Appl.* **2022**, *198*, 103304. [\[CrossRef\]](#)
70. Marichamy, V.S.; Natarajan, V. Blockchain based Securing Medical Records in Big Data Analytics. *Data Knowl. Eng.* **2023**, *144*, 102122. [\[CrossRef\]](#)
71. Nair, A.K.; Sahoo, J.; Raj, E.D. Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing. *Comput. Stand Interfaces* **2023**, *86*, 103720. [\[CrossRef\]](#)
72. Kashyap, R.; Piersson, A.D. Big Data Challenges and Solutions in the Medical Industries. In *Handbook of Research on Pattern Engineering System Development for Big Data Analytics*; IGI Global: Hershey, PA, USA, 2018; pp. 1–24. [\[CrossRef\]](#)
73. Kalejahi, B.K.; Meshgini, S.; Yariyeva, A.; Ndure, D.; Maharramov, U.; Farzamnia, A. Big Data Security Issues and Challenges in Healthcare. *arXiv* **2019**. [\[CrossRef\]](#)
74. Esposito, C.; de Santis, A.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [\[CrossRef\]](#)
75. Khaloufi, H.; Abouelmehdi, K.; Beni-Hssane, A.; Saadi, M. Security model for Big Healthcare Data Lifecycle. *Procedia Comput. Sci.* **2018**, *141*, 294–301. [\[CrossRef\]](#)
76. Jain, P.; Gyanchandani, M.; Khare, N. Big data privacy: A technological perspective and review. *J. Big Data* **2016**, *3*, 1–25. [\[CrossRef\]](#)
77. Thilakarathne, N.N.; Priyashan, W.D.M.; Premarathna, C.P. Artificial Intelligence-Enabled IoT for Health and Wellbeing Monitoring. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies, ICCCNT 2021, Kharagpur, India, 6–8 July 2021. [\[CrossRef\]](#)
78. Thilakarathne, N.N.; Weerasinghe, H.D.; Welhenge, A.; Kagita, M.K. Privacy Dilemma in Healthcare: A Review on Privacy Preserving Medical Internet of Things. In Proceedings of the 2021 12th International Conference on Computing Communication and Networking Technologies, ICCCNT 2021, Kharagpur, India, 6–8 July 2021. [\[CrossRef\]](#)
79. Wang, B.; Li, L. Research Progress in Biomedical Big Data. *Prog. China Epidemiol.* **2022**, 391–400. [\[CrossRef\]](#)

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.