International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

# Data Security in Healthcare the Safety of Data with Cybersecurity

**Pachiyappan C.**

Assistant Professor, Department of Computer Science and Engineering, GKM College of Engineering and Technology

**Abstract:** ***The increasing reliance on digital technologies has made the healthcare sector a prime target for cyber-attacks. With the rising need for data security and compliance, this article examines the importance of cybersecurity in healthcare, the associated risks, and the strategies required to protect patient information andensure continuity of care. Healthcare organizations are particularly vulnerable and targeted by cyberattacks because they possess so much information of high monetary and intelligence value to cyber thieves and nation-state actors. The targeted data includes patients' protected health information (PHI). Cybersecurityis critical for patient safety; it has an unreliable track record. Breach of infrastructure has resulted in millions of health records being stolen, potentially putting patients' lives at risk. This necessitates the integration of Cybersecurity into patient safety. Before these attacks, many security experts struggled to persuade corporate executives of the necessity of cyber security. cybersecurity asa patient safety, enterprise risk, and strategic priority and instill it into the hospital's existing enterprise, risk management, governance, and business-continuity framework. The main aim of this paper is the development of recent techniques applicable to crypt Analysis hash function, mainly from the SHA family. Recently proposed attacks on MD5 & SHA motivate a new hash functiondesign. It is designed not only to have higher security but also to be faster than SHA-256. This method is very useful for attacking.***

**Keywords**: Healthcare Cybersecurity, Cloud Computing, SHA-256 Algorithm, cryptographic hash function, patient privacy distributed cloud storage, Electronic Health Records (EHR), Access control, medical management system

## 1. Introduction

**Data Security**

Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places all over the globe. Data security and privacy protection are the two main factors of user's concerns about cloud technology. Though many techniques on the topics of cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in cloud architecture.

## 2. System Overview

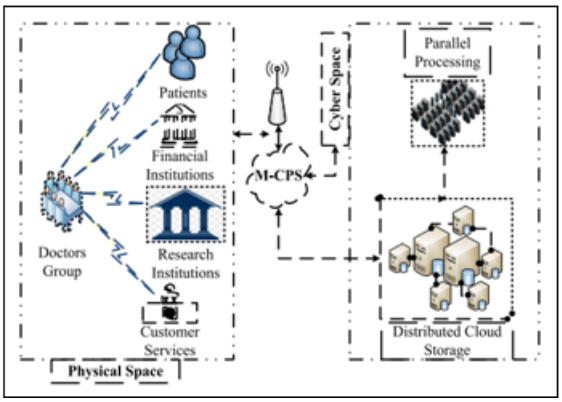


**Figure 1.1**

Cloud computing has become an indispensable facet of modern information technology, offering on-demand access to a spectrum of computing resources like storage, servers, databases, networking, and software. This paradigm shift empowers businesses and organizations to scale their operations with agility and cater to dynamic business demands. The architectural diagram serves as a foundational guide to comprehending the core components and their intricate interplay within a cloud computing system.

a) **Physical Space: The Cornerstone of Cloud Infrastructure**

**Global Network of Data Centers:** These geographically dispersed facilities house the physical servers, storage units, and networking equipment that constitute the bedrock of the cloud infrastructure. Data centers are meticulously engineered to ensure:

**Reliability:**

Redundant power supplies: Mitigate the impact of power outages by ensuring a continuous flow of electricity to critical systems.

Backup cooling systems: Safeguard against temperature fluctuations and prevent equipment overheating.

Multiple network connections: Guarantee data transmission continuity even in case of primary network failures.

**Security:**

Stringent access control measures: Rigorous protocols governing physical and logical access to data centers and cloud resources.

Advanced security surveillance: Employing security cameras, motion detectors, and other monitoring tools to deter unauthorized access.

Intrusion detection and prevention systems: Continuously monitor network activities for malicious attempts and safeguard against cyberattacks.

**Scalability:**

Modular design: Data centers are built with the capacity to incorporate additional servers, storage devices, and network equipment seamlessly to accommodate the burgeoning demand for cloud resources.

Infrastructure planning: Strategically allocating resources across geographically distributed data centers to enhance fault tolerance and disaster recovery capabilities.

**b) Distributed Cloud Storage: A Redundant and Scalable Foundation**

**Data Replication:** Fortifies data security by creating copies of critical data across multiple servers within the cloud storage infrastructure. This approach ensures data remains available even if a server malfunctions. In the event of a server failure, data can be retrieved from the replicated copies on other servers, minimizing downtime and data loss.

**Data Fragmentation and Erasure Coding:** Enhances data resiliency by distributing data fragments across various servers. Erasure coding techniques add redundancy to the data fragments. Even if a certain number of fragments are lost due to server failures, the remaining fragments can be used to reconstruct the original data. This technique offers a space-efficient approach to data protection.

**Elastic Storage:** Cloud storage solutions are inherently scalable. Users can effortlessly augment or diminish their storage capacity based on their evolving requirements. This eliminates the need for businesses to invest in upfront hardware and manage capacity limitations associated with traditional on-premises storage solutions.

**c) Customer Services: A Multifaceted Cloud Service Delivery Model**

**Cloud Service Providers (CSPs):** These entities act as the forerunners of cloud computing, providing a comprehensive array of services to customers. They manage the underlying cloud infrastructure and offer a diverse service portfolio, including:

**Infrastructure as a Service (IaaS):** This service model offers fundamental building blocks like virtualized servers, storage, and networking. Customers have complete control over the operating system, applications, and data deployed on these virtualized resources.

**Platform as a Service (PaaS):** This service model provides a platform for developing, deploying, and managing applications. PaaS offerings typically include pre-configured environments with essential middleware, development tools, and database services.

**Software as a Service (SaaS):** This service model delivers on-demand access to software applications over the Internet. Users can leverage these applications without the need for software installation or maintenance on their local machines.

**Service Delivery and Management:** Cloud service providers equip users with a comprehensive toolkit and Application Programming Interfaces (APIs) to effectively manage their cloud resources. These tools encompass functionalities such as:

**Provisioning:** A streamlined process for setting up and configuring cloud resources like virtual machines and storage.

**Monitoring:** Real-time insights into resource utilization, performance metrics, and cost analysis.

**Management:** Features to dynamically scale resources up or down as needed, automate routine tasks, and configure access controls for enhanced security.

## 3. Modules

### 1) System Model

In our system model, four entities are involved, as shown in they are the trusted Administrator, the Doctor, the nurse, the patient, and the cloud. The Administrator is responsible for patient registration and revocation. The Doctor owners are those who will outsource their healthcare data to the cloud. To SHA 256 access control while preserving data privacy by using the SHA method again we can't decrypt the original data Once we create we can't modify the data. Doctor encrypt their healthcare data before outsourcing. To access this encrypted data, the data patient submits his role attributes to the cloud. Upon receiving the role attributes, the cloud retrieves the encrypted data and returns it to the patient. All the data will be more secure and reliable to access the data anywhere at any time.

### 2) Healthcare Cybersecurity

Improve an organization's awareness of cybersecurity risk management in systems, people, assets, data, and capabilities that provide a consistent language for internal and external stakeholders to comprehend, assess, and manage cybersecurity risk. Ensure the delivery of vital services by developing and implementing necessary safeguards. Create and implement efforts to maintain resilience strategies and restore service performance that a cybersecurity event has impacted. It may be used to assist in identifying and prioritizing activities for lowering cybersecurity risk. It may be used to manage cybersecurity risk across large enterprises or to deliver vital services inside a company. There are specific cybersecurity outcomes described in the Framework, references to relevant examples, and guidance on accomplishing them.

### 3) Hashing the Medical data

Hashing is a mutation of a string of characters into a limited fixed-length key that addresses the initially entered string. The process is utilized in databases to store and recover data securely as it helps to access the data in the fastest possible manner with the help of digests or hash values. The hash values are preimage-resistive as they cannot be decrypted by any of the third-party users except the confidential user In this paper, a modified cryptographic approach of SHA-256 is utilized for the security of a confidential medical database involving the insurance of a patient. SHA-256 is a part of the family of SHA-2-based hashing where a character string is mutated to a 256-bit digest. There are two novelties in this particular work. First is the modification of the compression function in the SHA-256 algorithm. Second is the appending of the data of a few textboxes into a single input text and hashing it to obtain a secured output.

### 4) Revoking Role Attributes

In conventional schemes, when a data Administrator wants to revoke several role attributes, say A′ they can revoke all Doctors, Nurses, and patients. We observe that, when the data attributes share very few repeated role attributes in healthcare data, then we only need to update secret shares for very few role attributes. When the data attributes share many repeated role attributes in healthcare data, though we need to update the secret shares for some role attributes, conventional schemes have to update the secret share for all the role attributes of all the affected data. patient or doctor tried the wrong key multiple times we can block the particular users.

### SHA-256 Algorithm

SHA-256 is a cryptographic hash function that takes an input of a random size and produces an output of a fixed size. Hash functions are powerful because they are 'one-way'. What this is means is, it is possible for anyone to use a hash function to produce an output when given an input; however, it is impossible to use the output of the hash function to reconstruct it's given input. SHA-256 is a one-way function that converts a text of any length into a string of 256 bits. This is known as a hashing function. In this case, it is a cryptographically secure hashing function, in that knowing the output tells you very little about the input. It is a modified version of SHA1, which in turn is a modified SHA0. All three are now broken, to some extent.

- Note 1: All variables are 32-bit unsigned integers and addition is calculated modulo 232 • Note 2: For each round, there is one round constant k[i] and one entry in the message schedule array w[i], $0 \leq i \leq 63$
- Note 3: The compression function uses 8 working variables, a through h
- Note 4: Big-endian convention is used when expressing the constants in this pseudocode, and when parsing message block data from bytes to words, for example, the first word of the input message "abc" after padding is 0x61626380

### 1) Doctor Registration

Table Doctor Registration

| Name | Type | Collection |
|---|---|---|
| id | int(2500 | |
| did | varchar(250) | latin1_swedish_ci |
| dname | varchar(250) | latin1_swedish_ci |
| dpassword | varchar(250) | latin1_swedish_ci |
| dmailid | varchar(250) | latin1_swedish_ci |
| dtypes | varchar(250) | latin1_swedish_ci |
| dgender | varchar(250) | latin1_swedish_ci |
| dlocation | varchar(250) | latin1_swedish_ci |
| dnumber | varchar(250) | latin1_swedish_ci |
| status | varchar(250) | latin1_swedish_ci |
| hashcode | varchar(250) | latin1_swedish_ci |
| nimage | varchar(250) | latin1_swedish_ci |

### 2) Patient Registration

**Table:** Patient Registration

| Name | type | Collection |
|---|---|---|
| Id | int(2500 | |
| Pid | varchar(250) | latin1_swedish_ci |
| Pname | varchar(250) | latin1_swedish_ci |
| ppassword | varchar(250) | latin1_swedish_ci |
| pmailid | varchar(250) | latin1_swedish_ci |
| Ptypes | varchar(250) | latin1_swedish_ci |
| pgender | varchar(250) | latin1_swedish_ci |
| plocation | varchar(250) | latin1_swedish_ci |
| pnumber | varchar(250) | latin1_swedish_ci |
| Status | varchar(250) | latin1_swedish_ci |
| hashcode | varchar(250) | latin1_swedish_ci |
| pimage | varchar(250) | latin1_swedish_ci |

### 3) Nurse Registration

**Table 7.3:** Nurse Registration

| Name | type | Collection |
|---|---|---|
| Id | int(2500 | |
| Nid | varchar(250) | latin1_swedish_ci |
| Nname | varchar(250) | latin1_swedish_ci |
| npassword | varchar(250) | latin1_swedish_ci |
| Nmailid | varchar(250) | latin1_swedish_ci |
| Ntypes | varchar(250) | latin1_swedish_ci |
| Ngender | varchar(250) | latin1_swedish_ci |
| Nlocation | varchar(250) | latin1_swedish_ci |
| Number | varchar(250) | latin1_swedish_ci |
| Status | varchar(250) | latin1_swedish_ci |
| Hashcode | varchar(250) | latin1_swedish_ci |
| Nimage | varchar(250) | latin1_swedish_ci |

### 4) Patient Test Report

**Table 7.4:** Patient test report

| Name | type | Collection |
|---|---|---|
| Id | int(11) | |
| Pid | varchar(250) | latin1_swedish_ci |
| Speclict | varchar(250) | latin1_swedish_ci |
| Bp | varchar(250) | latin1_swedish_ci |
| Sugar | varchar(250) | latin1_swedish_ci |
| Temp | varchar(250) | latin1_swedish_ci |
| Weight | varchar(250) | latin1_swedish_ci |
| bloodgroup | varchar(250) | latin1_swedish_ci |
| Hp | varchar(250) | latin1_swedish_ci |
| Status | varchar(250) | latin1_swedish_ci |
| Hashcode | varchar(250) | latin1_swedish_ci |
| Problem | varchar(250) | latin1_swedish_ci |

## 4. Conclusions

The smart and secure medical management system will help medical personnel, as well as patients, benefit from a smooth medical service. For this, the authors in this paper attempted to introduce a smart and protected hospital management system. This module helps in providing the suggestion of whether a patient should be admitted to the hospital or not. This decision-providing

strategy is not yet implemented in state-of-the-art methods. A smart and secure health management system is proposed for providing an accurate facility to the patient. For secured insurance data processing, a modified cryptographic approach of SHA-256 is utilized in this work, as it encodes 256 bits into

64 hexadecimal characters providing the highest security. From the result, it can be observed that the proposed approach can be a supportive tool for effective healthcare service. Furthermore, the diagnosis results can also be encrypted using the hashing algorithm. There are many different solutions available to help with cyber security in healthcare, including identity and access management, risk management, compliance management, antivirus, antimalware, and DDoS.

## References

[1] A.F. Rahim et al., "GN Information privacy concerns in electronic healthcare records: A systematic literature review." In Proceedings of the 2013 International Conference on Research and Innovation in Information Systems (ICRIIS), Kuala Lumpur, Malaysia, 27–28 November 2013

[2] Martti Lehto et al., "Cyber Security: Critical Infrastructure Protection". Springer International Publishing. https://doi.org/10.1007/978-3-030-91293-2_8, 2020

[3] V. Diamantopoulou et al., "Supporting the design of privacy-aware business processes via privacy". In Proceedings of the 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, UK, 10–12 May 2017.

[4] A. Rawat and S. Gochhait, "Iot Enabled Mental Health Diagnostic System Leveraging Cognitive Behavioural Science," 2022 International Conference on Decision Aid Sciences and Applications (DASA), 2022, pp. 1401-1405, doi: 10.1109/DASA54658.2022.9765032.

[5] S. Gochhait et al., "Implementation of EHR using Digital Transformation: A study on Telemedicine," 2020 International Conference for Emerging Technology (INCET), 2020, pp. 1-4, doi: 10.1109/INCET49848.2020.9154146.

[6] M. Pathapati and S. Gochhait, "Intelligent Data Management to Facilitate Decision-Making in Healthcare," 2022 International Conference on Decision Aid Sciences and Applications (DASA), 2022, pp. 1-5, doi: 10.1109/DASA54658.2022.9765260.

[7] Digital Guardian. Data Insider—Digital Guardian's Blog. 1 January 2018. Available online: https://digitalguardia n.com/blog/historydata-breaches (accessed on 9 November 2019).

[8] E. Marin, "On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them", in ACSAC'16 (Los Angeles, CA, USA, 2016) [9] Z. Wang, P. Ma, X. Zou, J. Zhang, T. Yang, "Security of medical cyber-physical systems: an empirical study on imaging devices", in IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (2020)

[9] R.Piggin, "Cybersecurity of medical devices: addressing patient safety and the security of patient health information". BSI.https://www.bsigroup.com/LocalFiles/ENAU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper Cybersecurity_of_medical_devices.pdf

[10] NIST, "Framework for improving critical infrastructure cybersecurity: version 1.1. National institute of standards and technology (NIST). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.p df. 1782 Authorized licensed use limited to: Zhejiang University. Downloaded on January 21,2024 at 05:39:14 UTC from IEEE Xplore. Restrictions apply.

[11] A. W. Khan, S. Zaib, F. Khan, I. Tarimer, J. T. Seo and J. Shin, "Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach," in IEEE Access, vol. 10, pp. 65044-65054, 2022, doi: 10.1109/ACCESS.2022.3179822.

[12] J. Peters, "How is industry 4.0 affecting Healthcare. Intetics". https://intetics.com/blog/ guest-post-how-is-industry-4-0-affectinghealthcare, 2020.

[13] M. Eichelberg, K. Kleber, M. Kämmerer, "Cybersecurity challenges for PACS and medical imaging". Acad. Radiol. 27(8), 1126–1139 (2020) [

[14] S. Tuli et al., "Next generation technologies for smart Healthcare: challenges vision, model, trends and future directions", December. Inter Technol Lett 3(2017): e145. https://doi.org/10.1002/itl2.145

[15] Pradeep Kumar Garg et al., "Geospatial Data Science in Healthcare for Society 5.0". Springer Singapore.2022. https://doi.org/10.1007/978-981-16-9476-9

[16] Rajeev Agrawal et al., "Securing Cyber-Resilience in Healthcare Sector". In Cyber Security in Intelligent Computing and Communications, 2022, (pp. 211–225). Springer Singapore. https://doi.org/10.1007/978-981-16-8012-0.

[17] M. Bahrami and M. Singhal. "A dynamic cloud computing platform for eHealth systems": 17th International Conference on E-health Networking, Application & Services (HealthCom), 2015, pp. 435–438.

[18] A. V. Vijayalakshmi and L. Arockiam, "Hybrid security techniques to protect sensitive data in E-healthcare systems," in The International Conference on Smart Systems and Inventive Technology, 2018, pp. 39–43.

[19] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute based access control," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2130–2145, 2018.

[20] A. S. Black and T. Sahama, "eHealth-as-a-Service (eHaaS): The industrialisation of health informatics, a practical approach," in 2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom), 2014, pp. 555–559.

[21] A. Alabdulatif, I. Khalil, and V. Mai, "Protection of electronic health records (EHRs) in cloud," in 2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), 2013, pp. 4191–4194.

[22] A. T. Lo'ai, R. Mehmood, E. Benkhlifa, and H. Song, "Mobile cloud computing model and big data analysis for healthcare applications," IEEE Access, vol. 4, pp. 6171–6180, 2016.

[23] L.Griebel et al., "A scoping review of cloud computing in healthcare," BMC Medical Informatics and Decision Making, vol. 15, no. 1, pp. 1–16, 2015

## Author Profile

**Pachiyappan C**. serves as an Assistant Professor at GKM College of Engineering and Technology (Anna University). He completed his M.E. in Computer Science and Engineering (Specialization in Networks) at Karpaga Vinayaga College of Engineering and Technology and earned his B.E. from S.R.I. College of Engineering and Technology. His research interests center on Network Technology.