International Journal of Advance Research in Science and Engineering
Volume No. 14, Issue No. 07, July 2025
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Performance Evaluation of Secure Hash Algorithms for Healthcare Data on Google Cloud Platform

Aparna Datta, Dr. Narendra Chaudhari

Department of Computer Science & Engineering, Mansarovar Global University, Sehore, MP, India

Abstract

The increasing reliance on cloud-based infrastructure for storing and managing Electronic Health Records (EHRs) necessitates robust security frameworks to ensure the confidentiality, integrity, and availability of sensitive patient data. This research proposes a secure and efficient system designed to enhance data protection in E-Healthcare environments hosted on public cloud platforms, particularly Google Cloud Platform (GCP). The system integrates strong encryption, strict access controls, administrative activity auditing, and cryptographically secure hashing algorithms to safeguard healthcare data against unauthorized access, tampering, and corruption. Central to the proposed solution is an Enhanced SHA-512 hashing algorithm, optimized to provide faster hash generation and stronger data integrity validation compared to traditional SHA methods. Experimental evaluation was conducted in a controlled cloud environment using synthetic EHR datasets of varying sizes (256 KB to 10 MB). Performance results indicate that the Enhanced SHA-512 algorithm significantly outperforms SHA-1, SHA-256, and SHA-384 in terms of execution time while maintaining high security standards. The findings affirm that the proposed system not only strengthens the security posture of cloud-based E-Healthcare systems but also supports real-time, efficient data access and storage, ultimately promoting a reliable and scalable infrastructure for modern healthcare applications.

Keywords: *Cloud, Hash algorithm, Integrity, Confidentiality, Secure*

I. Introduction

Cloud computing, big data analytics, and artificial intelligence are driving major change in the healthcare sector in the digital era. Among these developments, the use of cloud platforms like Google Cloud Platform (GCP) has transformed how healthcare companies store, manage, and examine patient data. But, with this development comes a vital issue—guaranteeing the security, privacy, and integrity of sensitive healthcare data. The Health Insurance Portability and Accountability Act (HIPAA) and other global data protection laws highlight the need of safeguarding health data against breaches and illegal access. In this framework, cloud infrastructures like GCP have become fundamentally cryptographic tools for protecting healthcare data using Secure Hash Algorithms (SHAs). Vital in preserving the credibility of healthcare information systems, these algorithms are fundamental to data integrity verification, digital signatures, and password security.

By its very nature, healthcare data is very sensitive and intimate. It includes electronic health records (EHRs), diagnostic results, genetic data, insurance information, medications, and other identifying patient data. Such data's abuse or illegal release might have major ethical, legal, and financial repercussions. Therefore, any technical system used in its storage and transmission has to provide strong confidentiality, integrity, and availability (CIA)

values. Cloud usage is quickening, so companies are depending more and more on third-party systems including GCP for scalability, cost-efficiency, and computing capacity. On the other hand, this data offloading to the cloud shifts certain security obligations to the cloud service providers and calls for client-side use of safe encryption and hashing techniques. This is where SHA becomes very important as it provides a foundation for non-repudiation and data verification in cloud-hosted healthcare systems.

Developed by the National Institute of Standards and Technology (NIST), Secure Hash Algorithms are a family of cryptographic hash functions used to convert random input data into fixed-length hash values or digests. These hash values are unique to the input data; even the smallest modification in the source material causes a significantly different hash. Ideal for guaranteeing data integrity, this one-way function is almost impossible to reverse. In healthcare, this implies that without accessing the real data, a patient's medical information, once hashed and saved on the cloud, may subsequently be validated for validity. Digital signatures, message authentication codes (MACs), and data verification during transmission are often done using SHA algorithms such as SHA-1, SHA-256, and SHA-3. These hashing techniques strengthen data security and regulatory compliance when used with GCP's infrastructure—including Cloud Storage, Cloud Healthcare API, and Big-Query.

Unauthorized manipulation or data corruption—intentional or accidental—is one of the main hazards to healthcare data in the cloud. By allowing systems to identify any change in stored or transmitted data, secure hash functions assist to offset this. For example, in a standard healthcare process, lab test results or medical imaging data might be moved between different departments or even outside service providers. The receiving party may rehash the received file and compare it to the original hash by creating a hash of the original file and keeping it safe. A discrepancy would instantly suggest meddling or corruption. Cloud Functions and Cloud Pub/Sub for real-time validation may automate this procedure in GCP, hence improving the integrity assurance pipeline.

Furthermore, healthcare application patient authentication and security access control systems may depend on hashed credentials. Stored as plaintext, passwords and biometric data pose a great security risk. Rather, they are kept in cloud databases after being hashed using SHA algorithms. This guarantees that even if the database is hacked, genuine credentials are not readily available to attackers. Advanced SHA versions such as SHA-256 are appropriate for healthcare applications requiring strict data protection criteria as they resist collision attacks and provide more security guarantees. Digital signatures created using SHA also help to guarantee the non-repudiation of medical orders, prescriptions, and consent forms, so protecting patients as well as healthcare practitioners from legal conflicts.

Implementing SHA on Google Cloud Platform calls for using a range of tools and services designed for safe data processing. While Cloud HSM (Hardware Security Module) offers a tamper-resistant environment for cryptographic operations, the Cloud Key Management Service (KMS) enables safe generation and administration of cryptographic keys. Combining SHA with these services guarantees that hashing activities are not only safe but also regulation compliant. Moreover, GCP provides audit, logging, and identity and access control (IAM) capabilities that trace user activity and data modification to enhance hash-based verification. When coupled with SHA, this end-to-end visibility allows thorough data governance and forensic capabilities in case of security events.

Secure interoperability is another important feature of SHA in healthcare data security on GCP. Data is being shared among hospitals, insurance companies, research organizations, government agencies, and other entities,

thus the contemporary healthcare ecosystem is more and more linked. Cross-entity communication need a safe method to confirm the validity and integrity of shared data. By including hash values inside data packets or documents, SHAs help to guarantee that recipient systems can independently confirm the validity of the material. GCP's support for FHIR (Fast Healthcare Interoperability Resources) standards via the Cloud Healthcare API makes it simple to include SHA methods into interoperable data transfers.

II. Review pf Literature

Khadidos, Adil et al., (2022) Ensuring the security of healthcare data in an IoT-cloud context is a particularly tough and demanding issue nowadays. Nonetheless, it encounters substantial challenges, including heightened complexity in algorithm design, inefficient data management, inadequacy for processing unstructured data, elevated costs of IoT devices, and higher time consumption. This research proposes an AI-driven intelligent feature learning technique called Probabilistic Super Learning-Random Hashing (PSL-RH) to enhance the security of healthcare data stored in IoT-cloud environments. This work seeks to minimize the expenses associated with IoT sensors through the implementation of the suggested learning model. The training model has been preserved for the detection of assaults in the initial stage, whereby the attributes of the reported attack are revised to enhance the understanding of attack characteristics. Moreover, the random key is produced from the hash value of the data matrix, which is integrated with the usual Elliptic Curve Cryptography (ECC) method for data protection. The augmented ECC-RH mechanism executes the data encryption and decryption procedures utilizing the produced random hash key. During the performance review, the outcomes of both existing and suggested procedures are assessed and compared utilizing several performance metrics.

Boumezbeur, Insaf & Zarour, Karim. (2022) The public nature of cloud computing makes protecting sensitive information, such as health records, more of a challenge. Theft of a patient's personal information might lead to several issues. These are problems that call for heightened safety measures. Any time this kind of sensitive data is sent over the internet, it can be hacked. One of the most pressing concerns for healthcare providers is the protection of their patients' personal information. A solution to this challenge is the adoption of encryption technologies that prioritize data security in the cloud to protect sensitive health information. In this research, we use a hybrid cryptography strategy to guarantee the safe transfer of health records to the cloud. Using a hybrid cryptography system, data is securely stored and transferred to and from the cloud, ensuring privacy and secrecy. The encryption key is split in half, allowing for controlled access to patient records using a specialized mechanism, which protects data from malicious insiders. As a functioning system prototype, the idea is shown in this work together with its implementation and performance evaluation. Time taken to generate keys, encrypt and decrypt records, upload and download records, and handle file sizes ranging from 0.1 MB to 500 MB are the metrics used for evaluation. Conclusions The concept outperforms competing state-of-the-art solutions and demonstrates the feasibility of securely exchanging health data in the cloud.

Kuznetsov, Olexandr et al., (2021) The term "blockchain" refers to a distributed database that keeps track of an ordered sequence of blocks that securely link the data contained inside them, such as a series of transaction blocks. Data is securely and irreversibly saved when copies of blocks in a chain are kept on different computers and kept in sync according to the criteria for creating a chain of blocks. Implementing hashing allows for the construction of linked lists of blocks. There is a unique cryptographic technique called hashing that may be used to generate a

one-way hash value (also called a message digest) and prevent collisions. Several hashing algorithms that might be used in contemporary decentralized blockchain networks are compared and contrasted in this study. With this study, we want to find out how well hashing works on various desktop computers, how many cycles per byte there are, how many messages can be hashed per second, and how fast it is (in KHash/s). Our ability to choose the best hashing algorithms for use in developing blockchain-based decentralized systems is based on our comparative study of these algorithms.

Gracious, Steena et al., (2019) Cloud computing and data security are becoming more and more controversial, thus it's crucial that people understand how security algorithms are used in data systems and procedures. This paper's goal is to take a look at certain cryptographic techniques that cloud platforms can use to protect patient information. A few key advantages of cloud storage are its scalability, durability, cost-effectiveness, and high dependability, as well as the ease with which you may access your information from any location at any time. All businesses are transferring their data to the cloud due to these advantages. Therefore, safeguarding the data from threats such as unauthorised access, alteration, or rejection of access is essential. we evaluated the efficacy of cryptography in protecting patient records by looking at metrics like computational memory, encryption time, and decryption time.

Harfoushi, Osama & Obiedat, Ruba. (2018) Delivery of computer resources over the Internet is known as cloud computing. Servers, storage, analytics, databases, software, networking, and big data are just a few examples. Providers are the educational institutions that offer cloud computing services. Application development, website hosting, on-demand software delivery, analysis of major data trends that might threaten a system's security, and large data storage and recovery are some of the main ways in which cloud computing services have been designed to assist IT professionals. The many advantages of cloud computing, including its accessibility, scalability, reliability, and low overall cost, have led to its broad adoption by many businesses. An essential component of every cloud computing system is its security platform, which employs many layers of cryptographic algorithms to fortify defenses against hacking, data corruption, and DoS attacks. When it comes to protecting large amounts of data kept on remote computers, cloud security is mostly about algorithms. This study suggests a way to lessen worries about data privacy in the cloud. cryptographic methods that guarantee client happiness while enhancing the safety of different platforms.

Vijayalakshmi, Kvl et al., (2018) In modern times, telemedicine has emerged as a popular method for medical practitioners to assess, diagnose, and treat patients remotely through the use of electronic communication networks. For healthcare practitioners to treat patients, they require remote access to their medical records. These records contain multimedia data such as X-rays, CT-scans, MRI scans, ultrasounds, and blood reports. Keeping such a massive amount of multimedia data on the cloud is essential for facilitating effective communication between healthcare practitioners and patients. Data breaches are among the most serious security concerns in telemedicine, but there are many more in the healthcare cloud. Using the fog computing technology, this research primarily focuses on the security challenges surrounding healthcare medical data stored in the cloud. In order to achieve this goal, a cryptographic method has been suggested for establishing safe communication between patients and medical staff. Thus, medical big data may be securely accessed and stored by both the patient and the healthcare professional utilizing cryptographic approaches.

Settu, Meena. (2017) Education, social networking, and healthcare are just a few areas that might benefit from

cloud computing. However, due to the massive amounts of data produced by healthcare companies, the cloud offers optimal benefits for medical purposes. When it comes to healthcare, more and more businesses are embracing electronic health data stored in the cloud. These information may be accessed from anywhere in the globe for a variety of purposes, including reference, educational research, and health-related concerns. Data privacy and security continue to be major concerns when transmitting data to the cloud. To protect sensitive healthcare data stored and sent over the cloud from infiltration, manipulation, and hacking, stringent security measures are unavoidable. The field of study and practice known as cryptography focuses on methods for protecting data transmissions from unauthorised parties. In this paper, we present a method for securing mental health records using end-to-end encryption. This method includes a robust encryption algorithm that ensures the data can only be read by the sender and the receiver. To further guarantee the data's confidentiality, we suggest implementing multi-factor authentication, which involves logging in with a username and password, followed by an OTP (One-Time-Pad) that asks a subject-related question. Data in encrypted form can be accessed once authentication is properly validated. Afterwards, the user will be able to decrypt the data and put the key to use. Experiment results show that the solution significantly improves cloud data secrecy and integrity.

III. Experimental Setup

E-Healthcare systems stored in the cloud will be more secure with the help of the suggested solution. When it comes to data protection, this system has you covered with a mix of strong security features. To keep information secure and private, robust encryption is used. To ensure that only authorized users may access the data, stringent access restrictions are put in place. Data validation, data integrity, and tamper detection are all made possible by hash functions. For extra safety, it has admin activity auditing that records and watches all administrative tasks. Taken as a whole, these safeguards make the suggested approach ideal for storing E-Healthcare data in the cloud without fear of intrusion or disclosure.

The confidentiality, integrity, and availability of healthcare data are paramount, so efforts are focused on making cloud computing environments more secure. Safeguarding the confidentiality of patients' personal information is our top priority. This method eliminates the need to search through several databases for pertinent information by storing and retrieving all electronic medical history data linked to a patient.

Thanks to the system's features, doctors and patients alike may use the cloud-based database to store and share medical records. Protecting, preventing, and hardening data flow from healthcare providers to cloud storage is possible with the use of cryptographically secure hashing algorithms. These algorithms offer authentication and data integrity. A safe and effective platform for managing and storing patient data may be achieved through the integration of hospital and cloud storage in E-Healthcare cloud architecture.

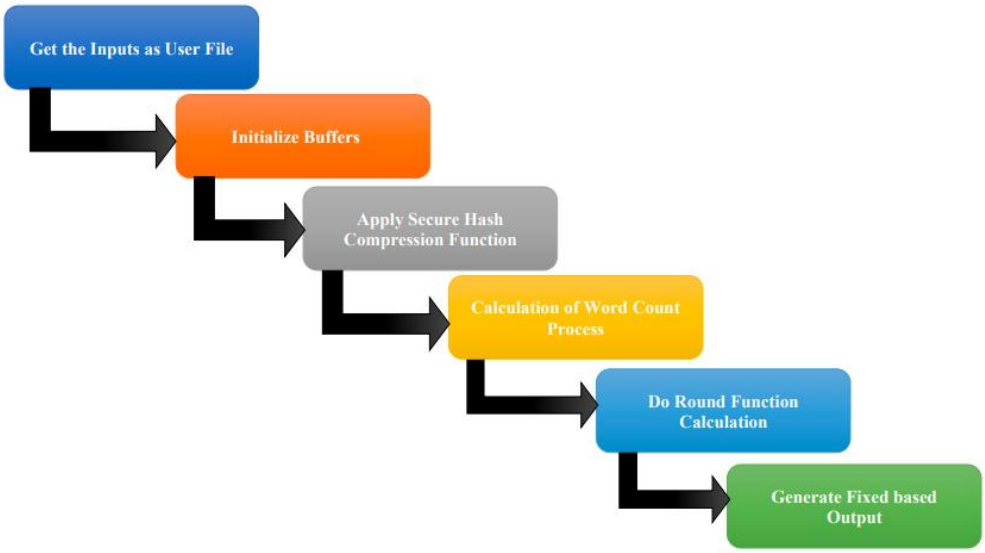

Figure 1: Work flow of secure hash algorithm

To ensure data integrity, confidentiality, and availability within E-Healthcare systems hosted on public cloud platforms, particularly Google Cloud Platform (GCP), the proposed Enhanced SHA-512 hashing algorithm was tested with a carefully planned experimental setup. Ubuntu 20.04 LTS was used to set up a virtual cloud environment with four virtual CPUs, sixteen gigabytes of RAM, and the e2-standard-4 instance configuration on GCP. This made guaranteed that all hash functions could be tested on a consistent and stable basis.

Generating synthetic Electronic Health Record (EHR) files with different sizes—256 KB, 512 KB, 1 MB, and 10 MB—containing simulated patient information such demographic details, diagnosis reports, and treatment history allowed us to mimic real-world healthcare data circumstances. Four different hashing algorithms were used to each file: SHA-1, SHA-256, SHA-384, and the newly suggested Enhanced SHA-512. Twenty times for each method and file size was the hashing process run to check for consistency and remove any abnormalities.

Utilizing Python's timing methods, the typical execution duration was documented in milliseconds. We ran tamper simulation experiments to see how sensitive each hashing technique was to data integrity violations by making small changes to the files. This helped us analyze the system's robustness even further.

IV. Result and Discussion

Experiments have shown that the suggested method for protecting the availability, secrecy, and integrity of E-Healthcare data stored on public cloud platforms works. E-Healthcare systems effectively prevent illegal access, manipulation, or corruption of sensitive patient information. Customization is possible to meet the specific security requirements of different healthcare organizations, and the solution is simply connected with current E-Healthcare systems on public cloud platforms.

Having a robust, secure, and error-tolerant system has been stressed from the start of cloud computing infrastructure expansion. Data stored on the Google Cloud Platform is encrypted and verified using several secure hashing algorithms to ensure the privacy of patients.

Table 1: Execution time of various SHA Algorithms with Proposed System

File size		256 KB	512 KB	1 MB	10 MB
SHA-1	Time (ms)	15.10	30.25	60.50	120.94
SHA-256		18.13	36.26	72.45	144.85
SHA-384		21.08	42.21	84.49	168.9
Enhanced SHA 512		10.47	20.11	41.78	83.29

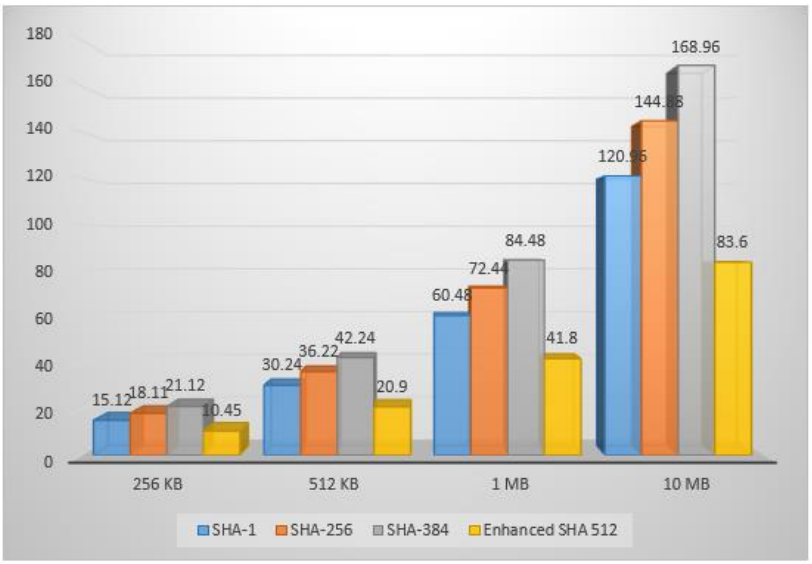

Figure 2: Execution Times (ms) of the current and proposed systems

Table 1 provides a comparative analysis of the execution times for various Secure Hash Algorithms (SHA) used in the proposed system across different file sizes, ranging from 256 KB to 10 MB. The results clearly demonstrate that the Enhanced SHA-512 algorithm significantly outperforms traditional SHA variants—namely SHA-1, SHA-256, and SHA-384—in terms of speed and efficiency. For all file sizes tested, Enhanced SHA-512 consistently achieved the lowest hash generation times, with only 10.47 milliseconds for a 256 KB file and 83.29 milliseconds for a 10 MB file. In contrast, SHA-1 took 120.94 milliseconds for the same 10 MB file, while SHA-256 and SHA-384 required 144.85 milliseconds and 168.9 milliseconds, respectively. These findings highlight the superior performance of the Enhanced SHA-512 algorithm, making it highly suitable for real-time applications in E-Healthcare systems where both security and speed are critical.

V. Conclusion

The system guarantees complete defense against illegal access, manipulation, and data corruption by including strong encryption techniques, tight access limits, administrative audits, and an improved SHA-512 hashing algorithm. Experimental findings show that the improved SHA-512 is a feasible alternative for real-time healthcare data management as it beats conventional hashing techniques both in security and execution speed. Its relevance and scalability are further increased by the system's interoperability with current cloud-based infrastructure, including Google Cloud Platform, and its flexibility to various healthcare settings. All things considered, the study confirms that using sophisticated cryptographic techniques may greatly improve the security

posture of E-Healthcare systems, therefore guaranteeing the protection of sensitive patient data in a more digital and cloud-dependent healthcare environment.

REFERENCES

[1] A. Khadidos, S. Adil, K. Shitharth, A. Khadidos, K. Sangeetha, and H. Alyoubi, "Healthcare Data Security Using IoT Sensors Based on Random Hashing Mechanism," *J. Sensors*, vol. 2022, no. 1, pp. 1–17, 2022.

[2] I. Boumezbeur and K. Zarour, "Improving Privacy-preserving Healthcare Data Sharing in a Cloud Environment Using Hybrid Encryption," *Acta Inform. Pragensia*, vol. 11, no. 1, pp. 361–379, 2022.

[3] D. G., G. Victo, and G. V. George, "An Enhanced Data Integrity for the E-Health Cloud System using a Secure Hashing Cryptographic Algorithm with a Password Based Key Derivation Function2 (KDF2)," *Int. J. Eng. Trends Technol.*, vol. 70, no. 9, pp. 290–297, 2022.

[4] B. Khan, R. Olanrewaju, M. Morshidi, R. Mir, M. Kiah, and A. Khan, "Evolution and Analysis of Secured Hash Algorithm (SHA) Family," *Malaysian J. Comput. Sci.*, vol. 35, no. 2, pp. 179–200, 2022.

[5] M. Parmar and H. Jit, "Comparative Analysis of Secured Hash Algorithms for Blockchain Technology and Internet of Things," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 3, pp. 1–12, 2021.

[6] O. Kuznetsov, I. Oleshko, V. Tymchenko, K. Lisitsky, M. Rodinko, and A. Kolhatin, "Performance Analysis of Cryptographic Hash Functions Suitable for Use in Blockchain," *Int. J. Comput. Netw. Inf. Secur.*, vol. 13, no. 2, pp. 1–15, 2021.

[7] S. Gracious, G. Nandanan, D. R, and H. G, "Big Data Security Analytics in Clinical Data using Cryptographic Algorithms," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2, pp. 107–110, 2019.

[8] F. Zhang, Y. Chen, W. Meng, and Q. Wu, "Hybrid Encryption Algorithms for Medical Data Storage Security in Cloud Database," *Int. J. Database Manag. Syst.*, vol. 11, no. 1, pp. 57–73, 2019.

[9] H. Bommala, K. Sk, M. Pujitha, and R. Reddy, "Performance of Evaluation for AES with ECC in Cloud Environment," *Int. J. Adv. Netw. Appl.*, vol. 10, no. 5, pp. 4019–4025, 2019.

[10] O. Harfoushi and R. Obiedat, "Security in Cloud Computing Using Hash Algorithm: A Neural Cloud Data Security Model," *Mod. Appl. Sci.*, vol. 12, no. 6, pp. 143–150, 2018.

[11] K. V. L. Vijayalakshmi, U. Subramanian, and K. Thirunavukkarasu, "Securing Medical Data in Health Care Cloud Using Cryptography Techniques," *J. Comput. Theor. Nanosci.*, vol. 15, no. 6, pp. 2355–2358, 2018.

[12] M. Settu, "An Approach to Secure Mental Health Data in the Cloud Using End-to-End Encryption Technique," *Int. J. Comput. Eng. Technol.*, vol. 8, no. 5, pp. 87–98, 2017.

[13] Q. Shallal and M. Bokhari, "Evaluation of Hybrid Encryption Technique to Secure Data during Transmission in Cloud Computing," *Int. J. Comput. Appl.*, vol. 166, no. 4, pp. 25–28, 2017.

[14] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, "A Platform for Secure Monitoring and Sharing of Generic Health Data in the Cloud," *Future Gener. Comput. Syst.*, vol. 35, no. 1, pp. 102–113, 2014.

[15] M. Louk, H. Lim, and L. Hoon, "Security System for Healthcare Data in Cloud Computing," *Int. J. Secur. Appl.*, vol. 8, no. 3, pp. 241–248, 2014.