Study of SHA-256 Hashing Algorithm

Prof Dr Neelam Kumar[1], Maheer Khan[2], Vrushabh Pasalkar[3,] Salman Pathan[4,] Sahil Shaikh[5]
[1](Professor, SRCOE, Department of Computer Engineering Pune)
[2],[3,4,5](Student, SRCOE, Department of Computer Engineering Pune)

Abstract: *The rapid growth of mobile healthcare platforms necessitates robust security measures to protect sensitive patient data and ensure privacy in cloud-based environments. This project, An Effective & Safe Mobile Healthcare Platform Leveraging Cloud Technology, employs the SHA-256 algorithm to establish a secure framework for data integrity and confidentiality. As a part of the cryptographic hash function family, SHA-256 is pivotal in safeguarding electronic health records (EHRs) by ensuring tamper-proof data storage and transmission. By integrating SHA-256 into the platform's security architecture, the project addresses critical challenges such as data breaches, unauthorized access, and secure patient-doctor interactions. This ensures a scalable, effective, and safe healthcare delivery system, leveraging the power of cloud technology without compromising on data security and user trust.*

Keywords: *SHA-256, Cryptographic hash function, Data integrity, Data confidentiality, Secure healthcare platform,*

I. Introduction

In the era of digital healthcare, protecting sensitive patient data is paramount, particularly when leveraging cloud technology for scalable and efficient services. An Effective & Safe Mobile Healthcare Platform Leveraging Cloud Technology aims to address these challenges by integrating robust cryptographic mechanisms, with the SHA-256 algorithm as a cornerstone for security.SHA-256, a member of the Secure Hash Algorithm (SHA-2) family, is a cryptographic hash function that generates a fixed, 256-bit (32-byte) hash value from any input data. Its deterministic nature ensures that identical inputs always produce the same output, while its collision-resistant properties make it virtually impossible for two different inputs to produce the same hash. This makes SHA-256 ideal for ensuring data integrity and security in cloud-based systems. In this project, SHA-256 is applied to protect electronic health records (EHRs), authenticate users, and secure communication between mobile devices and the cloud infrastructure. By hashing sensitive data before storage or transmission, the algorithm ensures that patient information remains confidential and tamper-proof. Furthermore, its resilience against modern cryptographic attacks, such as pre-image and collision attacks, provides a robust foundation for a secure mobile healthcare platform. The integration of SHA-256 into this project highlights its critical role in addressing key challenges such as data breaches, unauthorized access, and ensuring trust in cloud-based healthcare systems, ultimately enabling a safe and effective healthcare platform for patients and providers.

II. Literature Review

M. Satish Kumar. et al. in "Advanced SHA-256 Algorithm for Device to Device Communication".(2020) Device to device communication is the communication of two devices without involvement of base station, So, communication is possible with less delay than cellular mobile communication. Because of the faster communication, device to device communication is used for the 5g networks. Device to device communication suits for the decentralized nature of the network also. To provide communication from the device to device communication, physical layer security is required. Secure hash algorithm-256(sha-256) used to provide physical layer security, but sha-256 provides only128 bit collision resistant. So in this paper, advanced sha-256 algorithm is introduced in this paper.

Alam Rahmatulloh. et al. in "Implementation of JSON Web Token on Authentication with HMAC SHA-256 Algorithm"(2022) The rapid growth of information technology is influenced by globalization to accelerate access to information. This creates new problems, as differences must produce relevant information. Of course, system integration will be required. Web Service is a system integration solution that does not consider the platform, architecture, or programming language used in different sources. The security of web service is considered not yet implemented. The JSON Web Token (JWT) technology is an authentication mechanism for web service and will have a significant impact on data security. This implementation optimizes JWT security with the HMAC SHA-256 algorithm. Testing is conducted on two information systems by comparing the performance size when JWT technology is applied to Tim Bebersih Masjid Information System. The results show that the implementation of JWT on Windows Server 2019 (VM) is 462.8 ms with an average data size of 8.59 kb. Testing on the Windows 10 operating system obtained an average speed of 216.25 ms with an average data size of 8.59 kb. The result on Windows Server 2019 (VM) from the JWT performance test itself obtained the highest result, due to the use of virtual machine which is considered to consume a lot of RAM, resulting in performance that is 2 times higher.

B. Rahul. et al. in "Chaos-based audio encryption algorithm using biometric image and SHA-256 hash algorithm"(2023) Today, Internet users who share personal and professional data are concerned about the safety of the data. Encryption is one way to safeguard sensitive and private data on inter net sites. Encrypting audio data is more challenging than other types of data owing to the correlation between neighbouring samples. Encryption algorithms based on chaos theory are now widely used to protect digital audio and image data. Chaos theory is the idea that tiny changes in initial conditions will escalate into much more significant difference in the future. This paper proposes a robust and effective method for audio encryption based on chaos theory and user-biometric images. In addition, the SHA-256 hash technique and zig zag traversal are employed to bolster the system. First, the algorithm reads the sample values from the input audio and then separates them into byte blocks. In addition, each byte block is blended with chaotic sequences generated by the Henon map first, then by the Lorenz system. The chaotic sequences generated by the logistic map are used to create different initial values for the Henon map and Lorenz Systems. The initial values of the logistic map are constructed using the hash values of the plain audio signals and biometric images produced by the SHA-256 hash algorithm. The proposed method has a variety of desirable characteristics, such as good chaotic behaviour, low computational complexity, a huge key space, and substantial parameter space. The results of the various security and performance assessments show that the proposed algorithm is more robust and efficient than existing approaches against all forms of crypto-graphic threats.

S Shajarin. et al. in “Three Fish Algorithm: T-Mix Cipher using SHA-256”(2022) In every organization, use of online services is increasing. With this the sensitive data is carried over internet on daily basis. Hence, there is a chance of misleading the data by unauthorized parties. So, there is need to provide security for that data and cryptography is the science that helps in providing security. By using cryptography different types of security algorithms have been developed. Three fish is a symmetric-key and tweakable block cipher algorithm designed as a part of the skein hash function. The strength of three fish encryption relies on 128-bit tweak value. The proposed work focuses on strengthening Encryption Process by implementing tweak buffer along with input. Whereas key scheduling is secured by applying SHA-256 algorithm. SHA-256 is a secured hash function which belongs to SHA-2 family. Three Fish is used in providing security on software and hardware. It is also implemented in electronic media such as transactions like banking.

Dr Ali H Kashmar. et al. in “Enhancing Blockchain Security by Developing the SHA256 Algorithm”. (2024) notice that Security plays a vital role in various domains, including blockchain technology. The Blockchain serves as a secure data structure for storing transactional records. Hash functions are employed in cryptography to ensure integrity and authentication within the blockchain. The widely used SHA256 algorithm has faced recent attacks, prompting the development of stronger hash functions. This paper presents a novel modification approach to enhance the performance of SHA256 by introducing an extended mechanism for generating a 288-bit message digest and reducing the number of rounds to 44 instead of 64 while preserving the diffusion of data through its complex iterative process, which involves multiple rounds of bitwise and logical operations. The change makes sure that even small changes to the input data cause noticeable variations in the output hash, thereby maintaining cryptographic properties. The suggested hash function SHA288 achieves improved security, collision resistance, and preimage resistance, while maintaining a faster execution time compared to SHA256. The tables and tests conducted on the suggested algorithm have revealed its remarkable safety and robustness in countering attacks as well as demonstrated outstanding performance in random tests, which further enhances its security measures.

Fariha Jahan. et al. in “SHA-256 in Parallel Blockchain Technology: Storing Land Related Documents”(2020) identify that everyday many land documents are stored in an offline process. This process is challenging because it is done manually; for registration and storing, it needs many papers too. However, there is also a lack of security because anyone can see the document. Safety problems can be solved by creating a secure digitized system and the successful implementation of the system. The digitalization of the land registry system through Block-chain could be the only solution to serve a helpful, more secure, and corruption-free solution. In this paper, a new block-chain architecture called parallel block-chain by Satellite Chain Formation algorithm specially designed to store land-related documents with the SHA-256 hash algorithm has been implemented. Polynomial equations also show the numbers of generated blocks and times. And this research also indicates that the proposed system is secure, scalable, and fast.

III. Algorithm

1. **Preprocessing**

   The input message is padded so that its length is 64 bits short of being a multiple of 512. Padding includes appending a 1 bit followed by enough 0 bits.

   Then, the length of the original message (before padding) is appended to the end of the padded message.

2. **Initialize Hash Values**

   SHA-256 uses eight 32-bit words (H0 to H7), which are initialized with specific constant values.

3. **Processing Message Blocks**

   The message is processed in 512-bit blocks.

   Each block is divided into 16 words (W0 to W15), which are expanded to 64 words (W16 to W63) using bitwise operations.

4. **Main Computation (Rounds)**

   Each round involves updating eight working variables (a, b, c, d, e, f, g, h) using predefined constants and the message words. The 64 rounds involve bitwise operations and modular additions based on the constants and message words.

5. **Final Hash**
   After processing all blocks, the hash values are combined to form the final 256-bit hash.

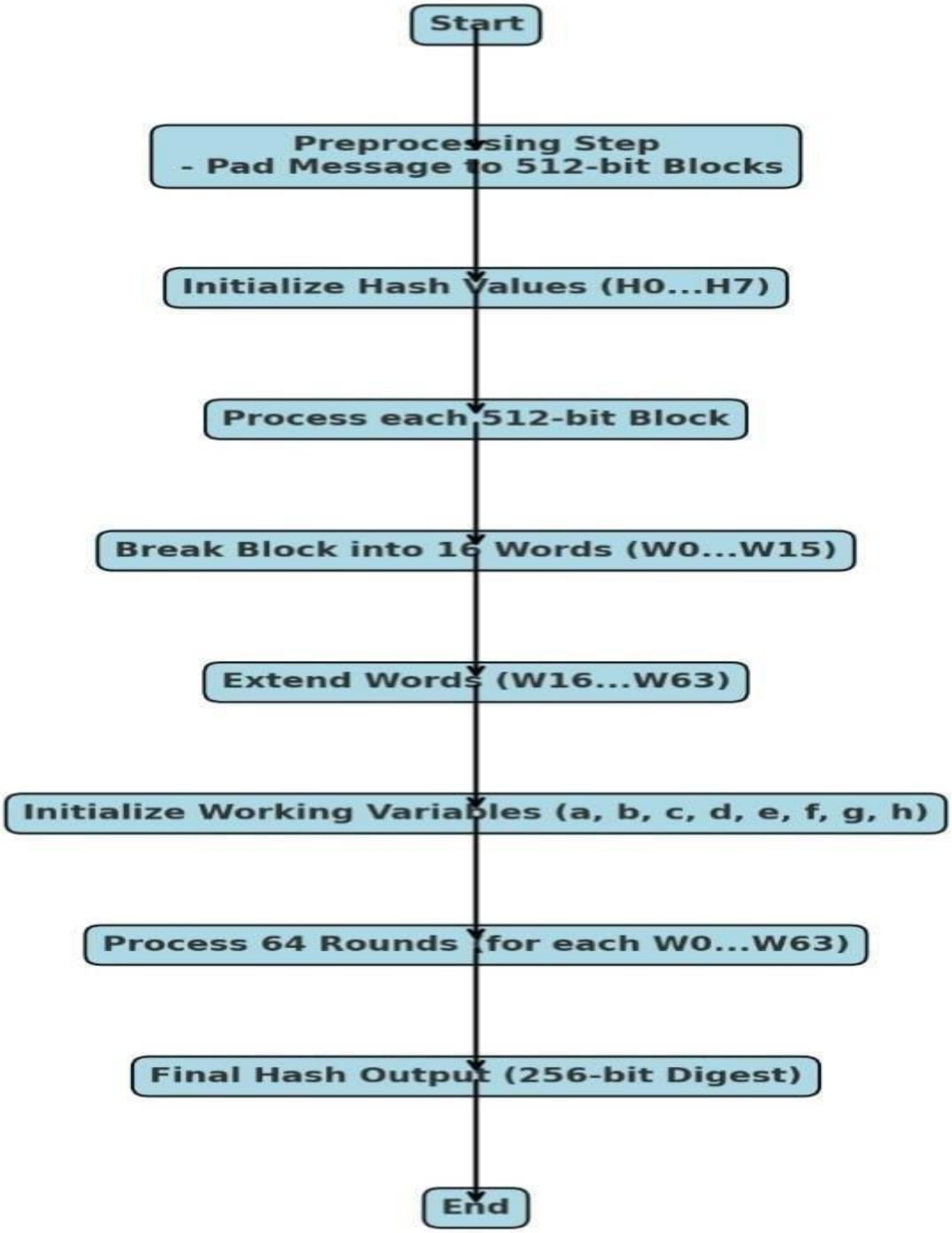
Start
Preprocessing Step
- Pad Message to 512-bit Blocks
Initialize Hash Values (H0...H7)
Process each 512-bit Block
Break Block into 16 Words (W0...W15)
Extend Words (W16...W63)
Initialize Working Variables (a, b, c, d, e, f, g, h)
Process 64 Rounds (for each W0...W63)
Final Hash Output (256-bit Digest)
End

Fig: SHA-256 flow diagram

IV. Advantages

1. **Strong Security**
   SHA-256 provides robust security through its collision-resistant and pre-image-resistant properties, making it highly suitable for protecting sensitive healthcare data.
2. **Data Integrity**
   Ensures that electronic health records (EHRs) remain untampered during storage and transmission by detecting any unauthorized modifications.
3. **Deterministic Output**
   Guarantees the same hash for identical input, enabling reliable data verification and authentication in cloud-based healthcare systems.
4. **Widely Accepted Standard**
   SHA-256 is a trusted, NIST-approved algorithm widely used in cryptographic applications, ensuring compatibility and reliability in security implementations.
5. **Scalability for Cloud Use**
   Efficiently handles large data sets, making it ideal for cloud-based environments where scalability is critical.

V. Disadvantages

1. **Computational Overhead**
   SHA-256 involves complex calculations that may increase processing time and power consumption, especially on resource-constrained mobile devices.
2. **No Encryption Capability**
   SHA-256 is a hashing algorithm and does not provide encryption, meaning it cannot be used to protect data confidentiality by itself without additional encryption layers.
3. **Irreversibility**
   While this is a security feature, the inability to reverse the hash can complicate scenarios where reversible encryption is required, such as data recovery or auditing.
4. **Potential for Misuse**
   Hashing algorithms like SHA-256 must be used with secure implementation practices (e.g., salting for password hashing). Misimplementation could lead to vulnerabilities, such as dictionary attacks.
5. **Resource-Intensive for Large-Scale Systems**
   In high-volume healthcare systems with frequent data synchronization, SHA-256 may contribute to increased resource demands, requiring optimized hardware or cloud processing capabilities.

VI. Application

1. **Data Integrity Verification**
   SHA-256 ensures the integrity of electronic health records (EHRs) by generating hash values before storing or transmitting them.
   On retrieval or receipt, the hash can be recalculated and compared to detect unauthorized changes.
2. **User Authentication**
   Patient and provider credentials are hashed using SHA-256 during authentication processes.
   This prevents plain-text storage of sensitive information, protecting user accounts from breaches.
3. **Secure Data Transmission**
   SHA-256 is used to create message digests for healthcare data transmitted between mobile devices and cloud servers.
   This ensures secure communication channels by detecting tampering during transmission.
4. **Digital Signatures for Authorization**
   SHA-256 is utilized in generating digital signatures for documents such as medical prescriptions, patient consent forms, and billing information.
   This provides authenticity and non-repudiation of critical healthcare records.
5. **Blockchain Integration for Healthcare**
   In blockchain-based implementations of the healthcare platform, SHA-256 secures transaction blocks, ensuring tamper-proof and immutable records.
   This is particularly useful for maintaining transparency and trust in patient data sharing among healthcare providers.

VII. Conclusion

The implementation of the SHA-256 algorithm in An Effective & Safe Mobile Healthcare Platform Leveraging Cloud Technology ensures a robust framework for data security and integrity. By leveraging the deterministic and collision-resistant properties of SHA-256, the platform safeguards sensitive patient data against unauthorized access, tampering, and breaches during storage and transmission..

VIII. References

[1]. A paper on 'SHA-512/256' by Shay Gueron, Simon Johnson and Jesse Walker published in 2011 Eighth International Conference on Information Technology.

[2]. A paper on 'Hardware Acceleration of SHA-256 Algorithm using NIOS-II Processor' by Argirios Sideris, Theodora Sanida and Minas Dasygenis published in 2019 8th International Conference on Modern Circuits and Systems Technologies (MOCAST)

[3].Adhikari S, Karforma S (2021) A novel audio encryption method using Henon-Tent chaotic pseudo ran dom number sequence.

[4]. Al-kateeb ZN, Mohammed SJ (2020) A novel approach for audio file encryption using hand geometry. [5]. Babu NR, Kalpana M, Balasubramaniam P (2021) A novel audio encryption approach via finite-time synchronization of fractional order hyperchaotic system.

[6]. Ahmed S. Nori, Ansam Osamah Abdulmajeed, “Design and implementation of Threefish cipher algorithm in PNG file”, Sustainable Engineering and Innovation, Vol.3, N0.2, July 2021, pp,72-91. [CrossRef]

[7]. Theda Flare G. Quilala, Ariel M. Sison, Ruji P. Medina, “Modified Blowfish Algorithm”, Indonesian Journal of Electrical Engineering and Computer Science Vol. 12, No. 1, October 2018, pp. 38~45 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v12.i1.pp38-45. [CrossRef]

[8]. Anil G. Sawant, 2 Dr. Vilas N. Nitnaware, Pranali Dengale, Sayali Garud, Akshay Gandewar, “TWOFISH ALGORITHM FOR ENCRYPTION AND DECRYPTION”, © 2019 JETIR January 2019, Volume 6, Issue 1.

[9] Federal information processing standard (fips), " Sucre Hash Standard,"180-2. National Institute of Science and Technology, 2002.

[10]Prof. Dr. Neelam Kumar, A STUDY OF ALGORITHMS USED IN MOBILEAPPLICATION DEVELOPMENT FOR SUGAR FACTORY, ALOCHANA JOURNAL VOLUME: 13, ISSUE: 13, ISSN NO11:2231-6329, PP-218-226, November 2024

[11]Neelam LabhadeKumar, Mangala S Biradar, Ashvini Narayan Pawale,"Reinforcement Learning-Based Deep FEFM for Blockchain Consensus Mechanism Optimization with Non-Linear Analysis"Journal of Computational Analysis and Applications, Vol. 33 No. 05 (2024)

[12]Neelam Labhade-Kumar “Shot Boundary Detection Using Artificial Neural Network”, Advances in Signal and Data Processing. Lecture Notes in Electrical Engineering, Springer, Vol 703. PP-44-55 Jan-2021

[13]Dr.Neelam Labhade-Kumar “Novel Management Trends Using IOT in Indian Automotive Spares Manufacturing Industries”, Journal of Pharmaceutical Negative Results , Vol. 13 ISSUE 09,PP 4887-4899, Nov-2022

[14]Dr.Neelam Labhade-Kumar “Adaptive Hybrid Bird Swarm Optimization Based Efficient Transmission In WSN”, Journal of Pharmaceutical Negative Results, Vol. 14 ISSUE 02,PP-480-484, Jan-2023,

[15]Neelam Labhade-Kumar “Combining Hand-crafted Features and Deep Learning for Automatic Classification of Lung Cancer on CT Scans”, Journal of Artificial Intelligence and Technology, 2023

[16]Neelam Labhade-Kumar “Enhancing Crop Yield Prediction in Precision Agriculture through Sustainable Big Data Analytics and Deep Learning Techniques”, Carpathian Journal of Food Science and Technology,2023, Special Issue, 1-18

[17]Neelam Labhade-Kumar “Accident prevention and management system in urban VANET for improving slippery roads ride after rain” Journal of environmental protection and ecology, ISSN:1311-5065 Issue 2 volume 25,PP 586–599,2024