International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I9P229

Volume 70 Issue 9, 290-297, September 2022

Original Article

An Enhanced Data Integrity for the E-Health Cloud System using a Secure Hashing Cryptographic Algorithm with a Password Based Key Derivation Function2 (KDF2)

G. Dhanalakshmii[1], G. Victo Sudha George[2]

[1,2]*Department of Computer Science and Engineering, Dr.M.G.R Educational And Research Institute, Maduravoyal, Chennai, Tamil Nadu.*

[1]*Corresponding Author : dhanalakshmi4481@gmail.com*

Received: 15 June 2022 Revised: 06 September 2022 Accepted: 16 September 2022 Published: 30 September 2022

Abstract - *Cloud computing has become an integral part of everyone's life since it allows us to share our data with anyone at any time and from any location over the internet through a service provider. Cloud computing provides virtualized platforms that enable users to manage and analyze data without having to do it manually. The term "E-Health" is used by hospital executives to describe the electronic monitoring of health-related data. Various e-Health applications have been developed to use e-Health data to monitor patients' health successfully remotely. Patient-sensitive data must be safeguarded at all costs to prevent data manipulation. In the cloud, protecting E-Health data is a serious problem. They have used numerous security algorithms in the existing system and still have much work to do to enhance security levels. This proposed method to secure data for E-Health applications in cloud environments by securing improved versions of secure hash fixed-based output cryptographic algorithms (SHA-512) with a Password-Based Key Derivation Function (PBKDF2), which helps to secure patient data in e-health cloud environments. These methods identify the most common aggressions faced by end users, such as Man in the Middle, Brute Force and Rainbow attacks. Finally, all the cryptographic hash methods were compared in terms of CPU time, Memory space, and Execution time.*

Keywords - *Cloud Storage, Security Issue, Cryptography algorithms, Secure Hash Functions, Attacks.*

1. Introduction

Cloud computing is a web-based system that allows us to access software, data, and services from any location on any web-enabled device via the internet. Performance, availability, and security are the three key study areas in cloud computing. The security of cloud computing is among the most important fields of study. Cloud computing constantly installs resources and monitors their utilization. Cloud computing collects data and resources and provides services to millions of users. In cloud computing, data security is a big issue.

The various attribute-based encryption methods are implemented for security before transmitting data to the cloud server. The Electronic Health Record service is a novel approach for exchanging health-relevant data. Patients can use it to generate, update, and manage their personal and medical data. They can also manage and share their medical information with other users and healthcare providers. Because of the critical and sensitive information kept in the cloud for consumers, security and privacy are considered critical issues in a computing cloud. The following aspects of cloud security are outlined: Availability, Confidentiality, Integrity, Authentication, and Accountability [1].

Availability ensures that data and services are always available to users. Confidentiality is used to secure a user's data and prevent unauthorized access. When data is exchanged across the network, integrity ensures it has not been tampered with. Authentication is used to ensure that the message contains only original authors. Accountability ensures that no one can deny they were present in data transmission. Maintaining data confidentiality and integrity is one of the most challenging aspects of cloud computing as it relates to data security. Encryption is the first line of defense against these issues. However, data encryption introduces new challenges, such as Integrity, legal issues, and Confidentiality's Families:

This algorithm was published in 1993 with the name Secure Hash Standard (version-0) by the US agency NIST (National Institute of Standards and Technology). Lateral, the revised version was published as an SHA-1. SHA-1 is a cryptographic hash function that takes an input and produces a 160-bit hash value as a Message Digest. The SHA-1 message size is 64 bits, the block size is 512bit, and the word size is 32 bits.SHA-1 produces a Message Digest based on similar principles in MD2, MD4 and MD5 Message Digest algorithm design. So, it provides greater protection than MD5, and a brute force attack would be far more difficult to execute.

Also, no known collisions have been found. But the problem here is that hackers can exploit SHA-1 to generate and install a fake certificate. Since 2005, it has not been found safe against well-funded opponents. SHA-2 was introduced, including significant changes compared to its predecessor SHA-1. It consists of six hashing features with hash values of 224, 256, 384 or 512 bits. SHA256 is a type of SHA2 which outputs a 256-bit hash value. The inner state and the output size are 256 bits. It is safer than SHA1. This is a hash function commonly used in the blockchain. It has improved safety compared to SHA-1. But it needs a lot more rounds to become as secure as SHA512, so while it's not insecure, a brute-force attack would be possible.

Secure Hash Algorithm 512 is a hash algorithm that converts the text of any length to a fixed-size chain. Each output provides a 512-bit (64-byte) SHA-512 length. This algorithm is widely used for hashing email addresses, hashing passwords and verifying digital records. Each data element results in a unique hash which is completely non-duplicable by any other data element. It is safe, possibly not for much longer than the predictable future. But PBKDF2 is considered usable. As a result, we provide improved data integrity by employing SHA 512 with a password-based key derivative function that includes inputs such as salt and iteration count, which are used to increase the workload of such attacks significantly and are used to reduce the vulnerabilities of brute-force attacks.

2. Related Works

The authors [1] offered, Evidence based on the Square-CDH (Computational Diffie Hellman) hypothesis, which is used to demonstrate the safety of auditing public shared data. [2] They discovered a revocable identity-based encryption storage system for cloud computing that allows for secure and reliable data exchange. This approach is primarily utilized to update cipher text and key update components.

[3] The authors presented the stable dynamic skyline query technique, which combines an enhanced B+ tree structure with symmetrical encryption to create a safe storage structure for tackling the secure skyline query problem in cloud services. This method also generated efficient skyline queries and dynamic updates with faster response times. The authors [4] offer a new technique for releasing an attribute-based storage structure that permits safe DE duplication and in which a private cloud and storage manage the computational process is maintained by a public cloud.

[5] The authors recently developed secure cloud storage and a proven data transfer system in which fresh verifiable data is shared with safe cloud storage based on proven data ownership and destruction. Because of the delicate nature of this privacy notion, they observed that many advanced algorithms for protecting privacy included defects that caused them to violate their stated privacy. The authors proposed [6] a novel semi-black-box approach for testing and giving counter-instances for erroneous algorithms that are designed to be fast and user-friendly, allowing a developer to easily explore iterations of an algorithm and identify where they fail.

[7] They discovered millions of images are uploaded to social media platforms daily, many of which include sensitive information. As a result, social care providers must not only provide retrieval and distribution services, but they must also protect the privacy of the images. The scientists published a content-based picture extraction and sharing approach that retains anonymity and may be used to promote friends in social multimedia apps.[8] They've developed a text-image retrieval cypher based on the bag-of-words notion and random mapping skills. Random models are aggregated and retrieved using the k-means approach.

[9] They revealed that electronic medical records, which are utilized to prevent diseases, enhance cure rates, and provide a solid platform for medical institutions and pharmaceutical corporations, have unresolved security and trustworthiness issues. [28] They looked at the widely held idea that data should be transferred through perhaps untrustworthy middleboxes that act as a channel between data writing. Based on Intel SGX technology, they have created a key management mechanism that can protect both symmetrical and asymmetric keys, making key exchange secure.

3. Proposed Work

This electronic healthcare management system is a web-based concept that aids in administering employees, physicians, and patients in a simple, pleasant, and effective manner. The proposed system provides a pleasant working environment for any healthcare facility and addresses the current healthcare management system's faults [26].

This system's design is built on smart devices such as mobile phones, laptop computers, desktop computers, and wireless sensor networks, enabling real-time analysis of numerous patient characteristics [20-21]. It aims to create a series of modules that will aid doctors in their diagnosis by monitoring patients' data over the internet. It also allows for continual examination of the patient for crises by attendants and caregivers. The data collected from the server allows physicians and caregivers to monitor the patient in real time. Each patient's medical history, including prescriptions and medical reports, is maintained on the cloud for simple access and processing for logistical and potential difficulties.

Table 1. Literature Survey Comparison

Ref. No& Year of Publication	Algorithms / Methods	Merits	Demerits
[11] &2021	Data Mining and the Decision Tree Algorithm	High scalability and reliabilit y at affordable prices.	Overheads of computational and memory and discussed virtualization attacks only.
[12] & 2020	Cloud-Edge Collaborative Storage and Secure Network Coding Methods	Solves the problem of data leaking by public-private key pair and managing private keys.	Dynamic cloud storage is not supported.
[13] & 2020	Random Oracle Model (ROM)	The system is more practical in terms of resource use	The usage of resources is not optimal, and also issues with latency.
[14] & 2020	Policy Attribute Based on Encryption	Provide excellent data sharing Security with reduced overhead costs for cloud computing.	In terms of IoT Devices, the cost factor is high.
[15] & 2020	Web Cloud Encryption Algorithm	Offers data confidentiality, flexible file sharing, and revoking user keys, usability and efficiency.	Required own Internet Cloud.
[16] & 2020	Cryptographic threshold techniques and intelligent linguistic threshold schemes.	Cryptographic threshold techniques of secret data protection	Different layers are needed in the management structure
[17] & 2020	Secure Sockets layer, hash functions, message signing and message authentication code.	Provide Security policies, user-focused security, application security and data storage.	Time consumption is more
[18] & 2020	Less searchable public key authentication system.	Ensures the confidentiality and security of externalized sensitive data.	Usage of resources more

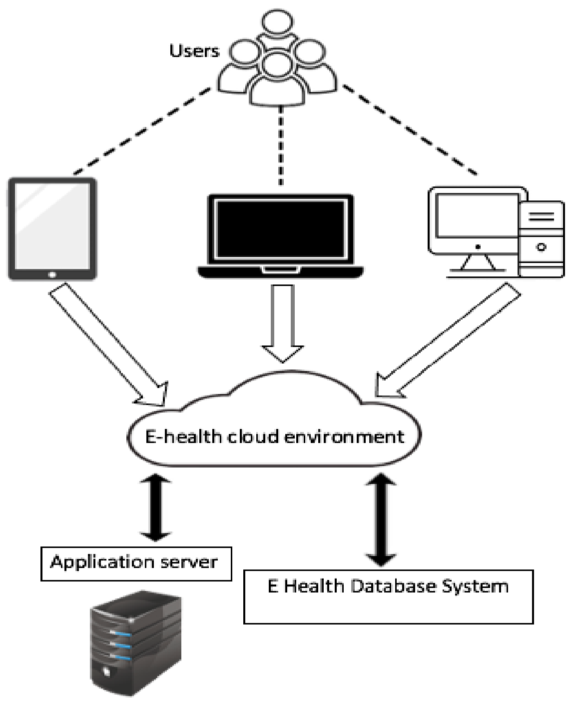

Fig 1. Architecture of E-Health Management System [22]

It is intended to monitor a single patient at home and several patients in hospitals and public health care facilities. Using cell phones to transmit data via the internet lowers the overall cost of the system. We proposed that the secure hash algorithm SHA-512 with Password-based-KDF2 offer the privacy and security features of the system for patients and their families to access the cloud storage as well as the system's probable dangers.

3.1. Evolution Steps

In this research, we use the secure hash technique SHA-512 with apassword-based-KDF2 to give more data integrity and authentication [22-23] for patients' sensitive data in healthcare administration.

The following Six procedures are followed:

*3.1.1. Procedure for Converting an Input Message to Message Padding (N*1024 bits)*

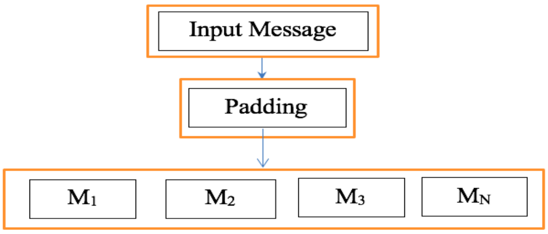

Fig. 2 Converting an Input message into Message Padding (N*1024 Bits)

Step 1: Get and Read an Input Message ←M
Step 2: if M as character
Do
{
Convert it into ASCII value and
Then get it in the binary form ←M_b
{
Else
Convert it into Binary Form ←M_b.
Step 3 Determine the length of M_b ←M_L
Step 4: do the Padding Process
{
Check
(M_L congruent 896) mod 1024 // Rule in the SHA 512
If M_L mod 1024=896
Then add 1 at the end of the M_b and make it as 896 bits ← Mp
Else
set: Padding bits ←896-M_L
M_L + (Padding bits) mod 1024=896, to verify after that add 1 at the end of Mb & make it as 896 bits ←Mp
}
Step 5: Convert M_b into Hexadecimal,

M_B ←Mp + [Hex (M_b) as 128 bits]

As a result, the block's length becomes length (=896+128).
Therefore, M_B as 1024 bits of message block size

3.1.2. Procedure for Generating 80 Words Wo-W79

Step 1: *Take an input as 1024 bits of Message Block from Step5 of Procedure 1(Go to Step5 of Procedure 3.1.1).*
Step 2: *Make 64 bits of 16 words (W_0-W_{15}) from 1024 bits.*

Step 3: *To generate the remaining Words W_{16} to W_{79} using the below equations.*
Set,

$\boxed{W_i \leftarrow W_i-16 +64\ \sigma0\ (W_i-15) +64\ W_i-7 +64\ \sigma1\ (W_i-2)}$

Where

- $\sigma_0(x)$ ← Assign (ROTR1(x)XOR(ROTR8(x)) (SHR7x))
- $\sigma_1(x)$ ← Assign (ROTR19(x)XOR(ROTR61(x)) (SHR6x))
- $ROTR^n(x)$ ← perform an n-bit circular right shift on the 64-bit
- $SHR^n(x)$ ← right shift the 64-bit by n bits, the padding on the left with zeros
- $+_{64}$ ←addition module 2^{64}

Step 4: After performing Step 3, we have obtained totally 80 rounds of 64 bits from W_0 to W_{79}

3.1.3. Procedure for Initializing 8 Hash Vectors and 80 Constant Hexadecimal Values

Procedure for Initialize 8 Hash Buffer Vectors
Step1: Initialize registers as Hash buffer, which is represented
by 8x64-bit registers are labelled as a, b, c, d, e, f, g, h,
Step 2: The registers are initialized with the first 64 bits of the fractional parts of the square roots of the first
eight primes.
Step 3: The data reported below are in hexadecimal format.

- Assign, a ←6a09e667f3bcc908,
- Assign, b ←bb67ae8584caa73b,
- Assign, c ←3c6ef372fe94f82b,
- Assign, d ←a54ff53a5f1d36f1
- Assign, e ←510e527fade682d1,
- Assign, f ←9b05688c2b3e6c1f,
- Assign, g ←1f83d9abfb41bd6b,
- Assign, h ←5be0cd19137e2179

Step 4: Go to Procedure 3.1.6.

Procedure for assigning 80 constant hexadecimal values (k_0 to k_{79})
Step 1: Initialize variables from K_0 to K_{79}
Step 2: Assign 64 bits of Hexadecimal values to each K_o to K_{79}
Step 3: Go to Procedure 3.1.6.

3.1.4. Procedure for Calculating 80 Round Functions

Step 1: Set the variables a, b, c, d, e, f, g, h, T1, T2 to their default values.
Step 2: Initialize K_i where i=0 to 79
Step 3:

- Assign g ← h
- Assign f ← g
- Assign e ← f
- Assign d+$_{64}$T2 ←e
- Assign c ← d
- Assign b ← c
- Assign a ← b
- Assign T1+64T2 ←a

Step 4: Do the calculations,

- Assign,
T1 ← h+64Ch (e, f, g) +64e+64W_i+64K_i

- Assign,
  T2 ←a+64 Maj (a, b, c)
- Assign,
  Ch (e,f,g) ← (e AND f) XOR (NOT e AND g)
- Assign,
  Maj (a,b,c) ← (a AND b) XOR (a AND c) XOR (b AND c)
- ∑(a) ← ROTR(a,28) XOR ROTR(a,34) XOR ROTR(a,39)
- ∑(e) ←ROTR(e,14) XOR ROTR(e,18) XOR ROTR(e,41)
- += addition modulo 2^64
  Where,
- K_t ←a 64-bit additive constant
- W_t ← a 64-bit word formed from the 512-bit input block currently in use

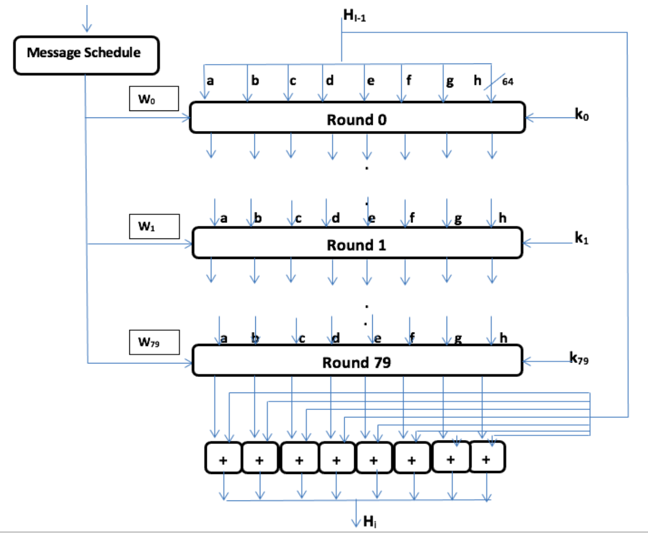

Fig. 3 Message Schedule

Step 5: Go to procedure 3.1.6

3.1.5. The procedure for Getting the Message Digests through Message Scheduling

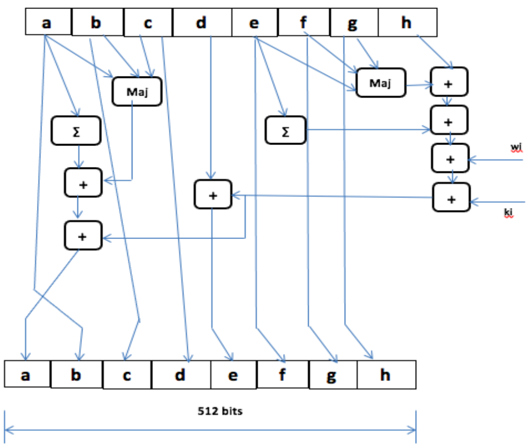

Fig. 4 8 * 80 Round Functions

Step 1: Procedure 1 should be used. To get Message Block (M_B) as 1024 bits

Step 2: Procedure 2 should be used. To get 64 bits of 80 Words as W_0 to W_{79}

Step 3: Use Procedure 3 for obtaining 8 Initialization vectors from a to h and 80 Hexadecimal constant values.

Step 4: Use Procedure 4 to study and discuss round function calculations.

Step 5: Using Step 1 to Step 4 of Procedure 3.1.5 to get the Message Digest value in the form of 512 bits. (Note: This value is never to be modified to the actual input message because it is one-way property)

3.1.6. Procedure for Combined Secure Hash Function with a Password-Based-KDF2

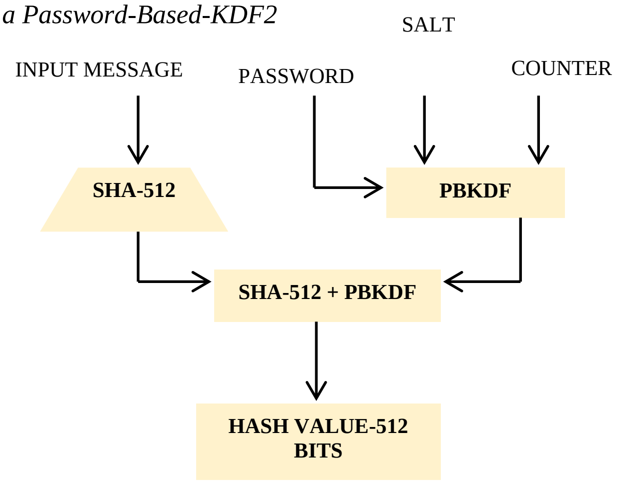

Fig. 5 Block diagram of SHA-512 with PBKDF2

The block diagram depicts the combination of SHA-512 and PBKDF2, which accepts as input parameters the SHA-512 input message, password, salt, and counter (number of iterations). The salt and iteration values are either saved with the hashed password as a 512-bit hash value or delivered as clear text with an encrypted message.

4. Results and Discussion

Since the beginning of its development agenda, cloud computing infrastructure has been filled with conflict. It concludes that having a more robust, secure, and fault-prone system is more essential than systems that assign security texture only after the design has been sent. The secure hashing techniques 256, 384, and 512 bits are supported by SHA 1 and SHA 2. The table below displays the execution results of the input applied to various SHA algorithms with PBKDF2 and the associated output.

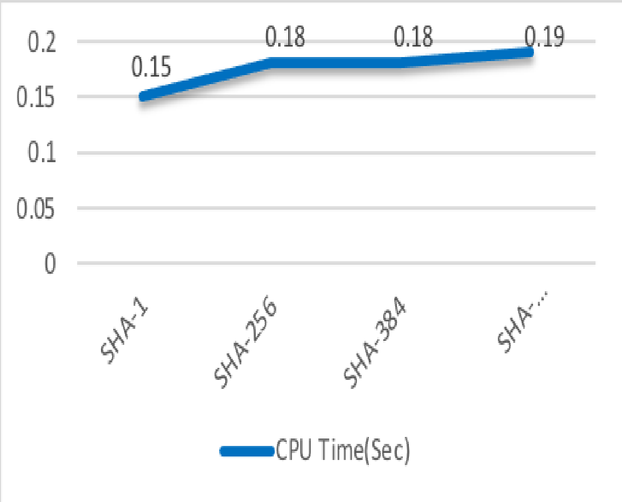

Fig. 6 The output of CPU time for various SHA Algorithms with input "abc."

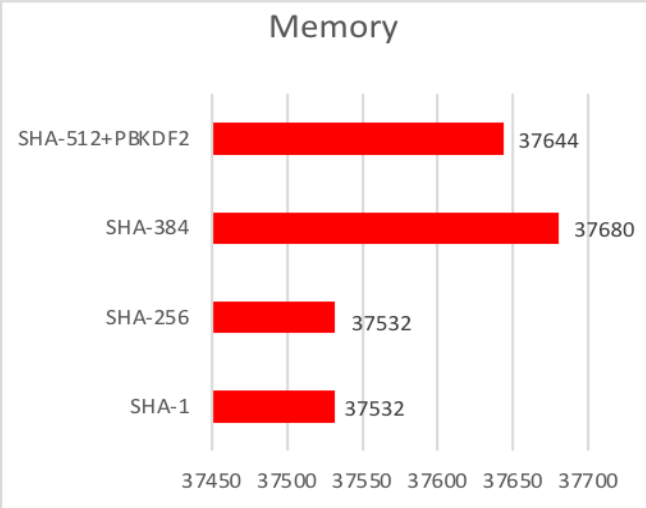

Fig. 7 The output of memory occupied by various SHA Algorithms with input "abc."

Table 2. Shows that CPU Time, Memory occupied, Execution time (ns & ms) of various SHA Algorithms with input "abc."

Message / Password : abc	SHA-1	SHA-256	SHA-384	SHA-512+PBKDF2
CPU Time(Sec)	0.15	0.18	0.18	0.19
Memory	37532	37532	37680	37644
Execution Time (ms)	76.606201	67.148167	1.529447	76.428328

Table 3. The output of various SHA Algorithms with input "abc."

Inputs	SHA-1 (Fixed length output:160 bits)	SHA-256 (Fixed length output:256 bits)	SHA-384(Fixed length output:384 bits)	SHA-512(Fixed Length output:512 bits) +PBKDF2
lion	dd220ebf8686edacb886be2691900f8561186c8a	a16202c75ee5cf8b000e54b5c5cd890de15a44463ba030d41f9847862710394b	96596bf844065992c4a3566900998e3eed796806e7fde2eea5d3bd10cc08a2bf108fabdc2bc9208bca9d1abd7f28055f	b0ade6600b25acbc830630e449550ef049b2ae61afc578000f71723a5115f4ed4d990f06de41d21bbbc2b1789f76c977dfa5088150f180a8d91bf395cc5fae45
scott	80d54452b301af25c681923e94dc7634a1a0d82e	21f7247d4d2d7838fed366e2aba1bed69582f8cc52a265ae3ac3279b7a49e409	a1c8509d6481318dd665359f2b64df6abb990eaf98546ebe4836ed4261748486a6693935e7bd5b03f2603fd12a1036c8	0081461c7863e4b8a2ec0ee9eec9811264e6ec1204192abc6ec75cea41d608026bef844b93724092f983fb96b2f39807cf38fcd6e124ad66b1996a0f2d847690
help	ba19a8b0e407cde1f0a6f3eca4a4c97b97b272c5	ac4583b21c9a0c07669942dbe6bca0e3a5d6aeaaa41e509c8a965e6eeeff1f61	30115d6b59d13891c101955e8e0aab4c70cbb4f82d17b6c2c0351401d3be4c603f7cef2d2d060a6431dc10b5b86a8e02	bacf79525bc66944be318ec28dc2b038727e6b463601249fdc3d51b4e9afc81ca4d90a8cdbb8719e0bcf7c0fecbb13a53a20a90e369d693067c04b4f47c5e3c4
abc	f24255597351d0579e6dc9d0234f80ab3e3a8ec9	dbbfe5b87ef78683600d074f4c7b1bc7241a0d7b0f78fc1c873687225e2a0f78	aafaeacb6e6856d59ac41126cca37126b35be1c3ce33d0704e34c922f3371e6747236b53566ea9d0b97fa9730cbcbd2b	30f443544cb095f3591ccdea04c2e69c538376177957726d3356bdfd4af0836572a5625d6861ac7e6664ffe16a7aba1cab5cd1aa43ae18c55017b0bed15c009e

4. Conclusion

In this research article, we have proposed that the combined secure hash algorithm Version-512 with Password Based Key Derivative Function, which provides more security for patient's data in the E-Health Management System at every assault during a Brute Force Attack, Man in the Middle Attack, and a Rainbow Attack on an exceedingly cloud server. The computer's hash value (Hv) is compared to the hash value preserved in the archive, which is frequently capable and sufficient to assess the reliability and security of patient data in an E-health system. The various SHA algorithms are discussed, compared, and implemented. Our proposed system provides more security, and Improved results are obtained as CPU Utilization is 0.19 seconds, Memory Usage is 37644 KB, and Execution Time is 76.42 milliseconds by the JAVA tool.

Future Work

This research can be improved in the future to take and analyze an original dataset of patient information in a hospital management system using an analytic tool.

Abbreviations

In this manuscript, the following abbreviations are used:

PBKDF	-	Password Based Key Derivation Function
SHA	-	Secure Hash Algorithm
MD	-	Message Digest
CDH	-	Computational Diffie Hellman
IPFS	-	Inter Planetary File System
ROM	-	Random Oracle Model
CP-ABE	-	Cipher text-Policy Attribute-Based Encryption
SSL	-	Secure sockets layer

References

[1] Chang, B. Shao, Y. Ji, and G. Bian, "Comment on A Lightweight Auditing Service for Shared Data with Secure User Revocation in Cloud Storage," *IEEE Trans. Serv. Comput.*, pp. 1–1, 2020. Doi: 10.1109/TSC.2021.3056660.

[2] K. Lee, "Comments on 'Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption," *IEEE Trans. Cloud Comput.*, vol. 8, no. 4, pp. 1299–1300, 2020. Doi: 10.1109/TCC.2020.2973623.

[3] J. Zhao, Y. Ma, J. Cui, Y. Peng, K. Li, and T. Wang, "SecSky: A Secure Dynamic Skyline Query Scheme with Data Privacy," *IEEE Access*, vol. 9, pp. 1–1, 2020. Doi: 10.1109/access.2020.3047950.

[4] H. Cui, R. H. Deng, Y. Li, and G. Wu, "Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud," *IEEE Trans. Big Data*, vol. 5, no. 3, pp. 648–660, 2019. Doi: 10.1109/TBDATA.2017.2656120.

[5] Y. Liu, S. Xiao, H. Wang, and X. Wang, "New Provable Data Transfer from Provable Data Possession and Deletion for Secure Cloud Storage," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 4, 2020. Doi: 10.1177/1550147719842493.

[6] Z. Ding, Y. Wang, G. Wang, D. Zhang, and D. Kifer, "Detecting Violations of Differential Privacy," *Proc. ACM Conf. Comput. Commun. Secur.*, 2020. Doi: 10.1145/3243734.3243818.

[7] Z. Zhang, F. Zhou, S. Qin, Q. Jia, and Z. Xu, "Privacy-Preserving Image Retrieval and Sharing in Social Multimedia Applications," *IEEE Access*, vol. 8, pp. 66828–66838, 2020. Doi: 10.1109/ACCESS.2020.2984916.

[8] H. Wang, Z. Xia, J. Fei, and F. Xiao, "An AES-Based Secure Image Retrieval Scheme using Random Mapping and BOW in Cloud Computing," *IEEE Access*, vol. 8, pp. 61138–61147, 2020. Doi: 10.1109/ACCESS.2020.2983194.

[9] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS," *IEEE Access*, vol. 8, pp. 59389–59401, 2020. Doi: 10.1109/ACCESS.2020.2982964.

[10] Vincent Manuceau, "About a Fast Cryptographic Hash Function Using Cellular Automata Ruled by Far-Off Neighbours," *SSRG International Journal of Engineering Trends and Technology*, vol. 69, no. 2, pp. 39-41, 2021. *Crossref*, https://doi.org/10.14445/22315381/IJETT-V69I2P206

[11] Q. He and H. He, "A Novel Method to Enhance Sustainable Systems Security in Cloud Computing Based on the Combination of Encryption and Data Mining," *Sustain.*, vol. 13, no. 1, pp. 1–17, 2021. Doi: 10.3390/su13010101.

[12] B. Sengupta, A. Dixit, and S. Ruj, "Secure Cloud Storage with Data Dynamics Using Secure Network Coding Techniques," *IEEE Trans. Cloud Comput.*, pp. 1–1, 2020. Doi: 10.1109/tcc.2020.3000342.

[13] Z. Ghaffar, S. Ahmed, K. Mahmood, S. H. Islam, M. M. Hassan, and G. Fortino, "An Improved Authentication Scheme for Remote Data Access and Sharing Over Cloud Storage in Cyber-Physical-Social-Systems," *IEEE Access*, vol. 8, pp. 47144–47160, 2020. Doi: 10.1109/ACCESS.2020.2977264.

[14] S. Xiong, Q. Ni, L. Wang, and Q. Wang, "SEM-ACSIT: Secure and Efficient Multi Authority Access Control for IoT Cloud Storage," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2914–2927, 2020. Doi: 10.1109/JIOT.2020.2963899.

[15] S. Sun, H. Ma, Z. Song, and R. Zhang, "WebCloud: Web-Based Cloud Storage for Secure Data Sharing across Platforms," *IEEE Trans. Dependable Secur. Comput.*, 2020. Doi: 10.1109/TDSC.2020.3040784.

[16] Ogiela L, Ogiela MR, Ko H, "Intelligent Data Management and Security in Cloud Computing," *Sensors*, Basel, Switzerland, vol. 20, no. 12, 2020.

[17] Tabrizchi H, Rafsanjani MK, "A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions," *The Journal of Supercomputing*, pp. 1-40, 2020.

[18] Wu B, Wang C, Yao H, "Security Analysis and Secure Channel-Free Certificate Less Searchable Public Key Authenticated Encryption for a Cloud-Based Internet of Things," *PloS one*, vol. 15, no. 4, pp. e0230722, 2020.

[19] Arun Pratap Singh, Himanshu Pundir, "Secure File Storage on Cloud Using Cryptography," *SSRG International Journal of Computer Science and Engineering,* vol. 7, no. 5, pp. 12-15, 2020. *Crossref,* https://doi.org/10.14445/23488387/IJCSE-V7I5P104

[20] Dr.G.Victo Sudha George G, "A Review of Classifying and Securing Sensitive Customer Data on Cloud Environments using Cryptographic Algorithms," *Design Engineering*, pp. 12424-12444, 2021. [Online]. Available: http://www.thedesignengineering.com/index.php/DE/article/view/4402

[21] V.Rajeswari, M.Gobinath, G. S. R. A. R., "Securing an E-Health Care Information Systems on Cloud Environments with Big Data Approach," *Design Engineering*, pp. 6986-6994, 2021. [Online]. Available: http://www.thedesignengineering.com/index.php/DE/article/view/3215.

[22] G. Dhanalakshmi, Victo Sudha George, "Security Threats and Approaches in E-Health Cloud Architecture System with Big Data Strategy Using Cryptographic Algorithms," *Materials Today: Proceedings*, 2022. https://doi.org/10.1016/j.matpr.2022.03.254. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214785322015978).

[23] Saritha Gattoju, and Vadlamani Naga Lakshmi, "An Adaptive Wolf Based Dansing System for Securing Hadoop at the Data Cleaning Stage," *SSRG International Journal of Engineering Trends and Technology*, vol. 70, no. 4, pp. 31-43, 2022. *Crossref,* https://doi.org/10.14445/22315381/IJETT-V70I4P204

[24] Kalaichelvi.T. Jabasheela, L,Ramapraba, P S,Shobana, M, "MAC-Based Secure Data Transmission in Vehicular Ad hoc Networks," In: Pandian, A.P., Fernando, X., Haoxiang, W. eds., Computer Networks, Big Data and IoT, Lecture Notes on *Data Engineering and Communications Technologies*, Springer, Singapore. vol 117, 2022. https://doi.org/10.1007/978-981-19-0898-9_4.

[25] Parvathaneni Rajendra Kumar, et al., "Heart Disease Prediction based on Ensemble Classification Model with Tuned Training Weights," *SSRG International Journal of Engineering Trends and Technology,* vol. 70, no. 4, pp. 59-81, 2022. *Crossref,* https://doi.org/10.14445/22315381/IJETT-V70I4P206

[26] Shakil KA, Zareen FJ, Alam M, Jabin S, "BAM Health Cloud: A Biometric Authentication and Data Management System for Healthcare Data in the Cloud," *Journal of King Saud University-Computer and Information Sciences*.

[27] Naseema Shaik, Noha Abdullah ayedalshahrani, Afnan saadalali, Amjad mohammedsaad Alqahtani, Salhasaeedhedan, "Making Digital Artifacts on the Web Verifiable and Reliable by using Cryptographic Hash Key," *SSRG International Journal of Computer Trends and Technology*, vol. 67, no. 11, pp. 38-41, 2019. *Crossref,* https://doi.org/10.14445/22312803/IJCTT-V67I11P106

[28] M. Park, "An SGX-Based Key Management Framework for Data-Centric Networking," *IEEE Access*, vol. 8, pp. 45198–45210, 2020. Doi: 10.1109/ACCESS.2020.2978346.