IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10621

STORAGE AND VALIDATION OF CERTIFICATES USING CRYPTOGRAPHY

Mrs. B. Haritha Lakshmi[1], S. Dhana Lakshmi[2], T. Lalitha[3], P. Sivani[4], M. Sai Kavya Sri[5], M. Padmavati[6]

[1-6]Department of Computer Science and Engineering, Vignan's Institute Of Engineering For Women, Visakhapatnam, A.P, India.

Abstract: In today's modern world, generation of fake certificates is not a big deal. In educational institutions and Recruitment Organizations, the problem of submission of forged certificates is increasing. It is difficult for the Authorities to identify a certificate as original or modified. Storing the original certificates with Digital Signatures and Hash codes, helps us identify a certificate distinctly, later we can able to validate any copy of the certificates we stored and prove it as original one based on generation of hash code for the certificate we want to validate. Today, cryptography is used to protect digital data. It is a division of computer science that focuses on transforming data into formats that cannot be recognized by unauthorized users. A digital signature is a mathematical technique used to validate the authenticity and integrity of any data.SHA-256 is used to produce Hash codes for the certificates, it generates an almost-unique 256-bit signature for any data. SHA-256 is one of the successor hash functions to SHA-1, and is one of the strongest hash functions available.

Keywords: Cryptography, Digital signature, Hash code, SHA256.

I. INTRODUCTION

Cryptography is the science of hiding information in order to conceal it from unauthorized access. It is a technique of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it and other stop others from accessing the data. Cryptography deals with a set of methods which enable us to store and transmit information while safeguarding it from intruders. That is, we can use cryptography methods to keep information private.

SHA-256 is one of the successor hash functions to SHA-1, and is one of the strongest hash functions available. SHA256 algorithm can be still used for making sure you acquired the same data as the original one. For example if you download something you can easily check if data has not changed due to network errors or malware injection. You can compare hashes of your file and original one which is usually provided in the website you are getting data or the file from.

Hashing is an algorithm that calculates a fixed-size bit string value from a file. A file basically contains blocks of data. Hashing transforms this data into a far shorter fixed-length value or key which represents the original string. The hash value can be considered the distilled summary of everything within that file. A good hashing algorithm would exhibit a property called the avalanche effect, where the resulting hash output would change significantly or entirely even when a single bit or byte of data within a file is changed. A hash function that does not do this is considered to have poor randomization, which would be easy to break by hackers.

II. OBJECTIVE

Hashing is a fixed-length string of numbers and letters generated from a mathematical algorithm and an arbitrarily sized file such as an email, document, picture, or other type of data. This generated string is unique to the file being hashed and is a one-way function , a computed hash cannot be reversed to find other files that may generate the same hash value. In simple terms, a hash value is a unique number string that's created through an algorithm, and that is associated with a particular file. If the file is altered in any way, and you recalculate the value, the resulting hash will be different. In other words, it's impossible to change the file without changing the associated hash value as well. So if you have two copies of a file, and they both have the same hash value, you can be certain that they are identical. Some of the more popular hashing algorithms in use today are Secure Hash Algorithm-1 (SHA-1), the Secure Hashing Algorithm-2

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10621

family (SHA-2 and SHA-256), and Message Digest 5 (MD5).The main reason technology of using SHA-256 is that it doesn't have any known vulnerabilities that make it insecure.

III. LITERATURE SURVEY

The certificate are stored in centralized manner and verified manually, so it takes too much time to verify, there is no platform to store the certificates safely and verify them when required. Therefore fake graduation degree certificates are created to get backdoor jobs. In industries, once an employee is hired, they require a background check of the educational details of the employee, and this verification is done just manually by their HR team or by some third party. There may be a delay in the process and a chance to manage the concerned section personnelof the university or college who receive the verification calls. It is even difficult to distinguish the fake and original degrees if the master register has already been tampered. Some universities store certificates in digital form but are also in a centralized network where there is a chance of tampering the certificate. Therefore, this may increase the cases of fraud since there is no means of security and integrity of the data both in manual and in digital form.

IV. PROPOSED SYSTEM

A cryptographic certificate system was developed based on relevant technology. Details of particular student will be entered and all the certificates to be stored will be saved. Hash codes of each certificate are generated using SHA256.The hash code contains 64 hexadecimal characters which are of 4 bits each. (64*4=256).The generated unique ID is used to verify the certificates. This system can be used by all the universities and colleges, in order to provide security to the certificates and the students' data. The problem of fake certificates can be identified by validation.

V. ARCHITECTURE

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001. They are built using the Merkle – Damgård construction, from a one-way compression function itself built using the Davies–Meyer structure from a specialized block cipher.

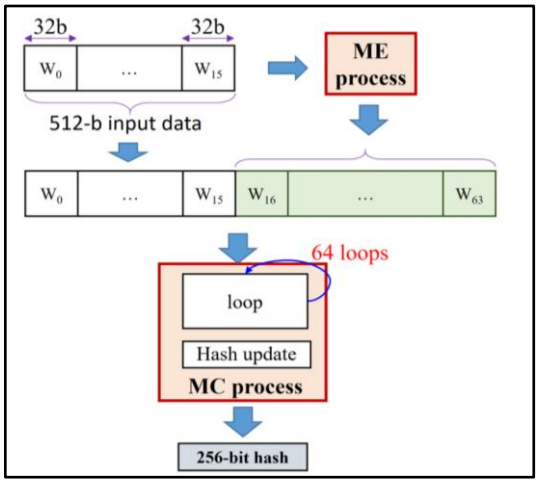

Fig. 1 SHA256 functioning

SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256. SHA-256 and SHA-512 are novel hash functions computed with eight 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are truncated versions of SHA-256 and SHA-512 respectively, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512, but the initial values are generated using the method described in Federal Information Processing Standards (FIPS) PUB 180-4.

Hash functions transform arbitrary large bit strings called messages, into small, fixed-length bit strings called message digests, such that digests identify the messages that produced them with a very high probability. Digests

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10621

are in that sense fingerprints: a function of the message, simple, yet complex enough that they allow identification of their message, with a very low probability that different messages will share the same digests.

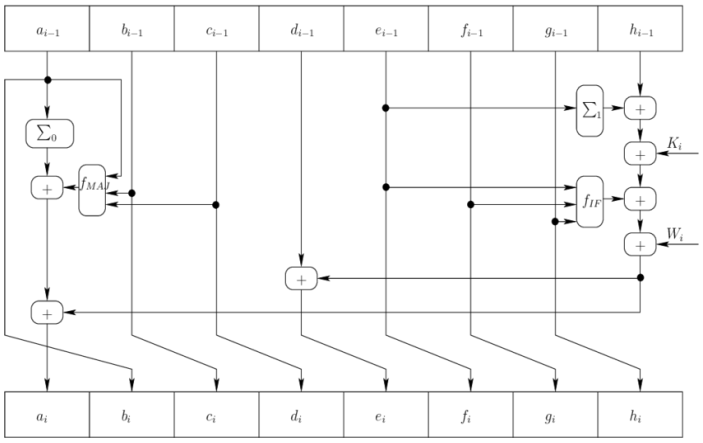

Fig. 2 Secure Hash Algorithm

The input blocks of message schedule W are fed, one after the other, to a function represented below as a graph. The graph takes as inputs a hash $\omega^i(t)$ and a message schedule input block $W^i(t)$, and outputs a hash $\omega^i(t+1)$. The initial hash $\omega^i(0)$ fed to the graph is the intermediate hash H^{i-1}: in the case of W^1, it's H^0 defined in the pre-processing step.

For t=0 to 63:

{

$$T_1 = h + \sum_1^{\{256\}}(e) + Ch(e,f,g) + K_t^{\{256\}} + W_t$$

$$T_2 = \sum_0^{\{256\}}(a) + Maj(a,b,c)$$

$$h = g$$

$$g = f$$

$$f = e$$

$$e = d + T_1$$

$$d = c$$

$$c = b$$

$$b = a$$

$$a = T_1 + T_2$$

}

VI. IMPLEMENTATION

We implemented user Interface for uploading the certificates to store them and uploading the certificates to verify them and validate as Original or fake Certificates. The certificates that we want to save need to be selected from the computer, original copies of the certificates are stored, for which hash codes will be generated. The hash codes are generated for the saved certificates using Secure Hashing Algorithm. The Certificate that we upload will be validated, the hash code of the uploaded certificate is compared with that of stored certificates, if it is the original copy of the certificate which is not modified , then the hash codes matches and the result is displayed as "Certificate Validation is Successful". All the details that are entered while storing the original certificates displayed after validation. If the certificate that we uploaded is modified copy, then the hash code of it doesn't match with the hash code of any certificates that we stored previously and it doesn't get validated. The result is displayed as "Validation failed or certificate modified".

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10621

Fig. 3 User Interface Screen

VII. RESULTS

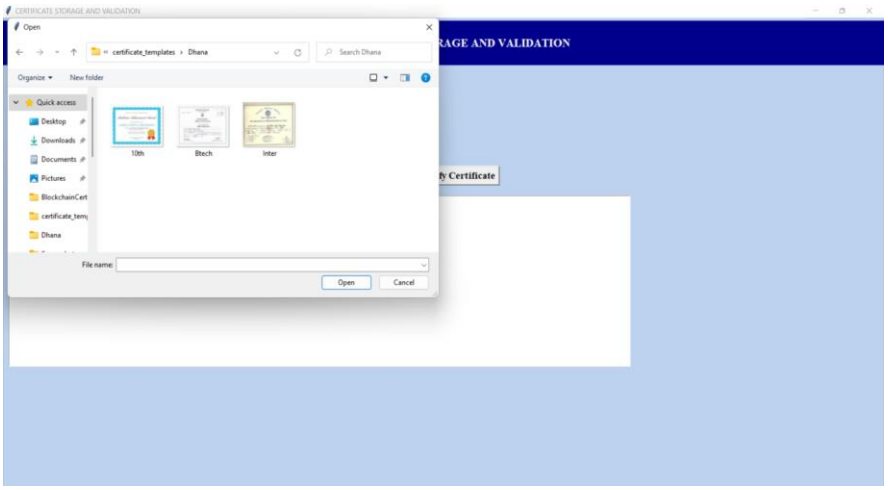

Fig. 4 Browsing certificates

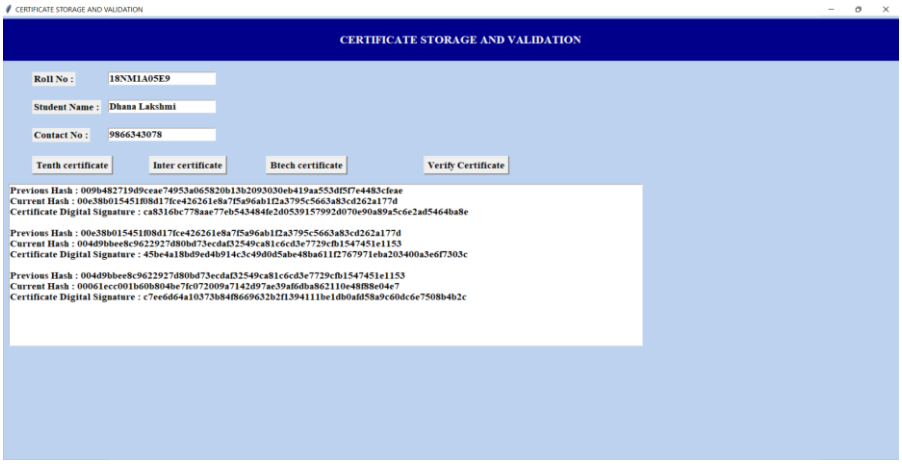

Fig. 5 Hash code generation of saved Certificates

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.047 ⁜ Vol. 10, Issue 6, June 2022

DOI: 10.17148/IJIREEICE.2022.10621

Fig. 6 Validation of original certificate

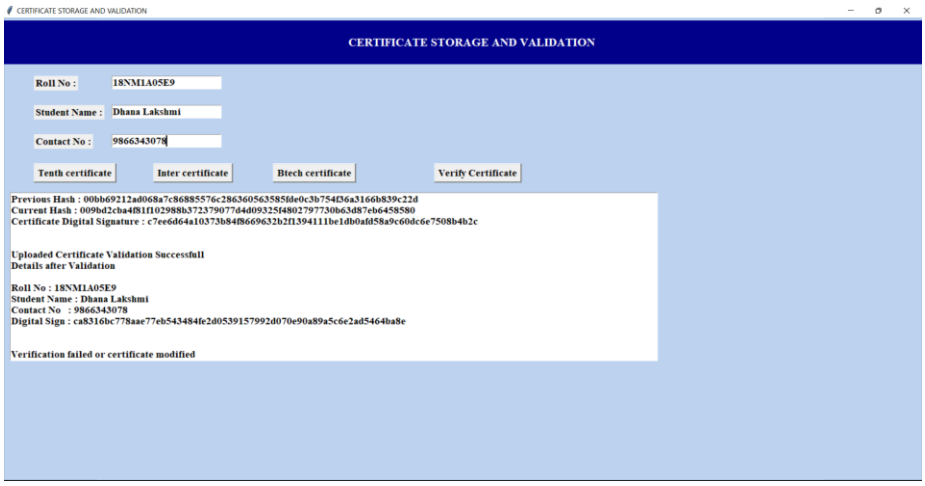

Fig. 7 Validation of modified certificate

VIII. CONCLUSION

The proposed model uses Cryptography techniques. The main goal of this technique is to know the originality of the certificate that is uploaded. Hashing Algorithm is used to create the hash code for each certificate uniquely, which is used to identify the original certificate distinctly. This model is useful in Academic Institutions, Recruiting Organizations, both Government and Private sectors can use this model as third party system. The Certificates are validated as Original or forged and helps the authorities find if a provided Certificate is an original one. The system is mandotory for all the Organizations that provide Employment to students.

IX. REFERENCES

[1] H. Abdulzahra, R. AHMAD, and N. M. NOOR, "Security enhancement; Combining cryptograhy and steganography for data hiding in images," ACACOS, Applied Computational Science, pp.978-960, 2014.
[2] P. R. Ekatpure and R. N. Benkar, "A comparative study of steganography & cryptography," 2013.
[3] M. H. Rajyaguru, "Cryptography-combination of cryptography and steganography with rapidly changing keys " Interntional Journal of Emerging Technology and Advanced Engineering, ISSN , pp.2250-2459, 2012.
[4] D. Seth. L. Ramanathan, and A. Pandey, "Security enhancement; Combining cryptography and steganography," International Journal of Computer Applications(0975-8887) Volume, 2010.
[5] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image steganography," International Journal of Computer Science and Network Security(IJCSNS), vol. 14, no. 6. P. 58. 2014.