International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 10th Mar 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 03

10.48047/IJIEMR/V12/ISSUE 03/06

Title **A New hashing Technique for Transmitting Data Securely**

Volume 12, ISSUE 03, Pages: 46-51

Paper Authors

P Vyshnavi, M JayaMadhuri, P SriVasavi, K Keerthi, N Gayathri,

Prof. R Ramesh

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A New hashing Technique for Transmitting Data Securely

P Vyshnavi[1], M JayaMadhuri[2], P SriVasavi[3], K Keerthi[4], N Gayathri[5], Prof. R Ramesh[6]
[1,2,3,4,5]Students, Department of Computer Science and Engineering, KKR & KSR Institute of Technology and Sciences, Guntur, Andhra Pradesh, India
6: Professor, Head of The Department, Department of Computer Science and Engineering, KKR & KSR Institute of Technology and Sciences, Guntur, Andhra Pradesh, India
[1]vyshnavipentyala@gmail.com
,[2]mannavamadhu81@gmail.com,[3]srivasaviperavarapu@gmail.com
[4]keerthirkc@gmail.com, [5]nallamothugayathri8@gmail.com, [6]repudiramesh@gmail.com

Abstract
Every aspect of human life revolves around security[1]. The most frequent and crucial query that emerges whenever a new technology is introduced is Security. When data is transmitted from one location to another, it must do so securely and without losing any information. On the other hand, it can be harder to provide security and secure data because hackers are constantly coming up with new ways to do so. By authenticating the data at both ends, we offer security in this paper. A hashing algorithm SHA-512 is used to compare hash values and authenticate the data. Where the data is transmitted and stored securely[2], users can follow the data and check its status.

Keywords: Encryption, SHA512, Hashing, Authorization, Hash Keys, Security.

Introduction

Data transmission is the act of moving data from one location to another. Data is typically transmitted end to end, without the use of a middleman. The information may be in written or verbal formats, as well as[10| images, videos, and other types of media[22]. The major challenge is to securely[3] transport data from one location to another and to store it while allowing users to handle it with confidence. Every business needs high-speed data transmission infrastructure to cope with the daily volume of content sent from one location to another[16].

There has been a significant change in technology in the now popular technological world. The amount of data being transferred between locations has also been rising quickly[7]. The internet has become an integral aspect of our lives, which has indirectly caused everyone to consider their data privacy[5]. There will be numerous data transfers from one individual to another. Security is the first concern that comes to mind when someone wants to move data from one location to another. It increases the person's challenges with regard to the security of their data when it is being transmitted[4].Many companies will have sensitive information that needs to be protected and should not be viewed by anybody else, including political, military, and other data. Data must be protected from hackers and several other hardware[9] and software assaults.

The most used phrase in cryptography is "encryption"[6].The process of converting a human-readable message into an unintelligible message is known as encryption. The original message is changed to a cypher text during encryption. To accomplish this, a Key is used. [19]Using a key, ordinary text is transformed into cypher text. Cipher text is a plain text that has been encrypted, and it is sometimes referred to as the encryption technique's[11] output, whilst plain text and the key are its inputs.

Plain text + Key = Cipher Text
CT = E (PT + K).
Here,
K is Key; PT is plain text; CT is cipher text; E is encryption.

At the sender's end, encryption is performed.

Numerous encryption algorithms exist. Block cypher, stream cypher, AES, RSA, XCHACHA20, SHA-256, SHA-512, and other encryption algorithms [8] are a few of these.

The hash tables are implemented via hashing. Hashing and encryption are not the same. It is a method of condensing fixed-length information into a shorter fixed-key or string of characters[26]. It is utilized for indexing and database retrieval. Using a hash function, the process of hashing turns plain text into a hash key. Despite the fact that all data are identical, hashing only seldom produces duplicate hash keys.

Plain text + Hash function = Hash Key

Hash keys are kept in a database and used to check if plain text or messages are identical or not.

The original communication cannot be recovered from the hash key by the intrusive party. The hashed data's length is independent of the message's length.

Literature Survey

The research papers help us to find the existing models and guide us to develop a new thesis by overcoming the problems which have been found out[1] Secure data transmission in cloud environment using visual cryptography and genetic algorithm [1] linked publications on visual cryptography and genetic algorithms that aid in understanding all applications for these methods. Visual cryptography is employed to hide important data, whereas genetic algorithms are utilized for encryption and decoding.

[2]Secure Cloud Storage of Data [2] distinguishes between the services of encryption and decryption and data storage. One cloud service provider offers a storage service, while another offers an encryption/decryption service.

[3]Inter Cloud Data Transfer Security [3] an inter-cloud communication security framework in a cloud computing context. Attacks such as Dos, fingerprinting, and unauthorised user attacks are identified and mitigated utilising techniques used with the Windows Azure Framework. These methods protect users and servers from intruders.

[4]A New Approach for Secure Data Transmission [4]Just text encryption and decryption were performed using the RSA technique.

[5]Novel Approach to Secure Data Transmission [5] a reliable message encryption system that can communicate and encrypt data without being connected to the internet[5]. To protect the data in this, numerous encryption levels are used. IEA Algo, DES, and Vignere.

[6]An Approach to Secure Data Transmission Through the Use of Cryptography and Steganography [6] A URL will be sent when the sender sends the data to the receiver in the event that the data is obtained by a third party or an intruder. After that, he will open the URL, open a webpage, and he will not discover any hidden data.

[7]Research on The secure Transmission Method of Cloud Computing Data [7] An internal cloud communication-friendly Simple Secure Communication Model (SSCM) is proposed in this paper. A USB Key-based method that combines software and hardware is suggested for data transmission outside of the cloud system.

[8]Secure Data Storage in Cloud Using Cryptographic Algorithms [8] For cloud data storage, this paper proposes combining

RSA, ONE TIME PAD, and AES and compares the algorithms.

Backgroud

A. Existing System:

Data transportation from one location to another has significantly risen `in the modern era[21]. It is crucial that people communicate with one another. Thus, there are a lot of data transmissions. Security for the data should be offered and stored securely throughout transmission. Through our investigation, we discovered that encryption and decryption procedures [20]are used to offer protection for the data. DES, RSA, and AES are the most widely used encryption and decoding methods[12].

The majority of users are concerned about the data's security, accessibility[15], and privacy. Public key and private key algorithms are now used to provide security. AES and RSA are the two most used encryption and decryption methods used to secure data. where issues with data privacy[14] exist. These methods create keys[18] that can be used to retrieve data if the intrusive party is well-versed in them. There are opportunities to hack the data.

B. Proposed System

In order to secure the data, we suggested a hashing algorithm in this paper. The hashing method is mostly used for hash key comparison and authentication. In the course of our investigation, we discovered that one of the finest hashing methods for the system we had in mind was the SHA-512 method. It uses a one-way encryption method. Hash values are used in the SHA-512 hashing algorithm to create hash keys.

For every piece of information, a unique set of hash keys is generated. Any attacker will have a very tough time recovering the original message from the hash key. This method uses message digestion to produce hash keys. Sender uploads data together with generated hash keys. Data and hash keys can both be viewed by the receiver. Receiver also decodes[24] the message and obtains the hash key; he then compares the two keys to determine if the data has changed or not.

Methodology:

SHA-512 Algorithm:

A hashing algorithm is SHA-512, or Secure Hash Algorithm. [29]The National Institute of Standards and Technology created the SHA algorithm. [17]It is a member of the SHA-2 family. The most recent version of the Secure Hash Algorithm is SHA-512. The message is encrypted using this SHA-512 algorithm. It's used to figure out data's cryptographic hash values. The variable-length text data is transformed into a fixed-length string using the hashing algorithm SHA. The SHA-512 algorithm has few working principles. The SHA-512 algorithm has a maximum message size of 2128 bits. A message's block size is 1024 bits. The message is digested by SHA-512, and its size is 512 bits. The SHA-512 algorithm's word size is 64 bits, and the process of digesting the message takes 80 rounds. There are permutations and s-boxes in these 80 rounds. Based on the operations carried out, the message will be compressed and expanded during these rounds. The SHA-512 operations are and, or, xor, shr, and rotr.

Working of SHA-512 Algorithm:

Step1: Append Padding Bits

The original message will be lengthened and padded (by adding bits). Even though the message is the right length, padding is always added. A single 1 bit is followed by the necessary number of 0 bits in padding.

Step2: Append Length

A 128-bit block that specifies the length of the original message (previous to padding in step 1) is used to extend the message. After appending, the message will be divided into N blocks of 1024 bits each, totaling N*1024 bits.

Step3: Initialize buffer

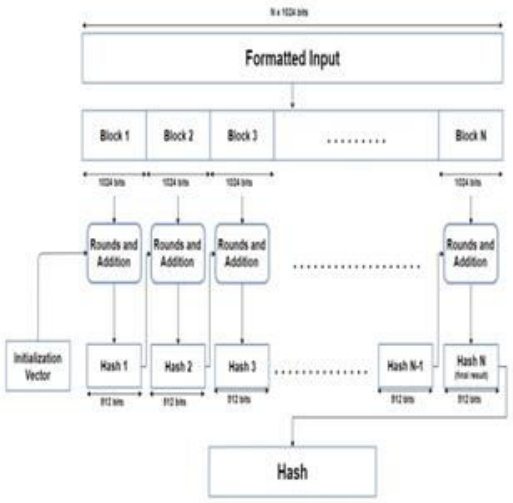
This 160-bit buffer (32*5) is used to store the Compression function's intermediate and final results. It has five 32-bit registers labeled A, B, C, D, and E. The 32-bit hexadecimal number is stored in five registers.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Step 4: Process message into 1024-bit blocks
The formatted input is taken one block at a time for message processing. Two things are used in the actual processing: the block with 1024 bits and the outcome of the previous processing.

A number of "Rounds" and an addition operation make up this section of the SHA-512 algorithm. Each round function takes three values: a Word, the result of the previous round, and a SHA-512 constant. After processing these three values, the round function produces a 512-bit output. This is done eighty times. To get the final result for this iteration of message processing, its output is simply added to the result of the previous message processing phase after the 80th Round.[27]

Step 5: Output
The final 512-bit Hash value of our original message can be obtained after each block of 1024 bits has completed step 4. As a result, each block's intermediate results are all used to process the next block. Additionally, after the final 1024-bit block has been processed, the SHA-512 algorithm's final output for our original message is available to us.[27]

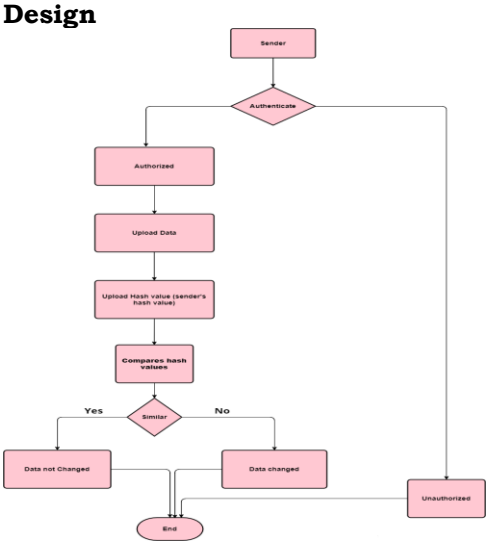


In this project, Initially we check the authentication of the user(sender and receiver). If the user is authorized then the user can upload data or can retrieve the data. There are two methods in this project. They are:

Sender:
Sender logs into their individual account and uploads the material following the authentication. Along with the data, the sender also uploads the data's hash value. The database stores the uploaded data. The database's hash value and the data can both be viewed by the sender and the recipient. Data is hashed to obtain the hash value. At both users' ends, the SHA-512 algorithm is used for hashing or message digests.

Receiver:
Receiver needs to be approved and have an account in order to access the info here. The recipient can examine the necessary data as well as its hash value by logging into their account. Hashing occurs even at the receiver's end. Hashing is done by the receiver to determine whether the data transmitted by the sender and the data received by the receiver are identical or not. Receiver compares the hash values after hashing. The data is not changed and the actual data is obtained if both hash values are the same. If not, Data is lost or violated by outsiders.

Design



Results

Conclusion

This project is unique in that it secures data using hashing rather than encryption techniques[25]. Most of the time, data may be secured using hashing, making it incredibly difficult for hackers to steal data[4]. To safeguard the data in this project, we employed the SHA-512 hashing algorithm. Since the hash keys generated by the information differ even for similar material, it is impossible to recover the original text using the hash keys.By comparing the hash keys, the user can inspect the hash values of the data provided and received and determine if the data has been altered or not.

Future Work

In the future, we intend to apply this to cloud systems[13], which rely on other partners for data privacy and security. By adopting this, cloud service providers themselves guarantee security for data and data transmission rather than relying on third parties.

References

[1] Mamta, M. D. Khare and C. S. Yadav, "Secure data transmission in cloud environment using visual cryptography and genetic algorithm: A review," *2017 International Conference on Innovations in Control, Communication and Information Systems (ICICCI)*, Greater Noida, India, 2017, pp. 1-4, doi: 10.1109/ICICCIS.2017.8660941.

[2] K. A. Dongre, R. S. Thakur and A. Abraham, "Secure cloud storage of data," *2014 International Conference on Computer Communication and Informatics*, Coimbatore, India, 2014, pp. 1-5, doi: 10.1109/ICCCI.2014.6921741.

[3] R. R. Chalse, A. Katara, A. Selokar and R. Talmale, "Inter-cloud Data Transfer Security," *2014 Fourth International Conference on Communication Systems and Network Technologies*, Bhopal, India, 2014, pp. 654-657, doi: 10.1109/CSNT.2014.137.

[4] R. Pranesh, M. Vigneshwaran, V. Harish and G. Manikandan, "A new approach for secure data transmission," *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Nagercoil, India, 2016, pp. 1-4, doi: 10.1109/ICCPCT.2016.7530163.

[5] N. Lemos, S. Khanvilkar and S. Patil, "Novel Approach to Secure Data Transmission," *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, 2018, pp. 1-3, doi: 10.1109/ICCUBEA.2018.8697369.

[6] K. Manjula Shenoy and S. G. Shaikh, "An Approach to Secure Data Transmission Through the Use of Cryptography and Steganography," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 1039-1043, doi: 10.1109/ICCES45898.2019.9002029.

[7] Z. ZONG, "Research on The secure Transmission Method of Cloud Computing Data," 2021 16th International Conference on Computer Science & Education (ICCSE), Lancaster, United Kingdom, 2021, pp. 329-332, doi: 10.1109/ICCSE51940.2021.9569731.

[8] N. L. Kodumru and M. Supriya, "Secure Data Storage in Cloud Using Cryptographic Algorithms," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-6, doi: 10.1109/ICCUBEA.2018.8697550.

[9] T. keophilavong, Widyawan and M. N. Rizal, "Data Transmission in Machine to Machine Communication Protocols for Internet of Things Application: A Review,"

2019 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 2019, pp. 899-904, doi: 10.1109/ICOIACT46704.2019.8938420.
[10] K. A. Kumar, M. J. C. M. Belinda, A. Lydia and R. S, "Secure Data Transmission through Steganography with ECC," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2022, pp. 1-7,
doi: 10.1109/ACCAI53970.2022.9752513.
[11] A. Majumder, A. Majumdar, T. Podder, N. Kar and M. Sharma, "Secure data communication and cryptography based on DNA based message encoding," 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, Ramanatha puram, India, 2014, pp. 360-363, doi: 10.1109/ICACCCT.2014.7019464.
[12] R. Jabi, P. Patel and D. Dubey, "An efficient secure data transmission based on visual cryptography," 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), Bangalore, India, 2016, pp. 1-6, doi: 10.1109/RAINS.2016.7764397.
[13] A. Sharma, D. Bhuriya and U. Singh, "Secure data transmission on MANET by hybrid cryptography technique," 2015 International Conference on Computer, Communication and Control (IC4), Indore, India, 2015, pp. 1-6, doi: 10.1109/IC4.2015.7375688.
[14] L. Tomy and Namitha T N, "Secure data transmission through reversible data hiding," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, 2016, pp. 1-4, doi: 10.1109/GET.2016.7916759.
[15] Kavitha C, Vishnu Kumar.M, Ramji.D, Rishi Rathnavel.K, 2018, Secure Data Transmission in Cloud Computing, International Journal Of Engineering Research & Technology (Ijert) Etedm – 2018 (Volume 6 – Issue 04)
[16] https://www.cdnetworks.com/enterprise-applications-blog/everything-you-need-to-know-about-data-transmission/
[17] https://medium.com/@zaid960928/cryptography-explaining-sha-512-ad896365a0c1
[18] https://www.academia.edu/24004685/Assured_Data_Communication_Using_Cryptography_and_Steganography
[19] V, Vetri & S, Gayathri. (2017). Hop-to-Hop Secure Data Transmission using Cryptography and Audio Steganography Algorithm. IJARCCE. 6. 522-525. 10.17148/IJARCCE.2017.6693.
[20] Malik, Medhavi. (2018). Secure Data Transmission using RC6 Algorithm in Multimedia Format.
[21] Antoniades, Ioannis & Miliou, Amalia & Hatalis, Miltiadis. (2008). Quantum Cryptography: The Ultimate Solution to Secure Data Transmission?.
[22] Goudar, R & Patil, Prashant & Meshram, Aniket & Yewale, Sanyog & Fegade, Abhay. (2023). Secure Data Transmission by using Steganography.
[23] Zhang, Aiqing & Zhou, Liang. (2016). Secure Data Transmission Protocol. 10.1007/978-3-319-32458-6_2.
[24] Lakshmi, Ch.Sri & Roshini, Y. & Sukanya, M. & sree, M.Hema & Jyothika, S.. (2020). Secure Data Communication using Cryptography. International Journal of Engineering and Advanced Technology. 9. 987-989. 10.35940/ijeat.D6735.049420.
[25] Okpalla, Chidimma & Madumere, & Benson-Emenike, U & Onwuama, M & Onukwugha, T. (2022). Secured and Encrypted Data Transmission over the Web Using Cryptography of the Creative Commons Attribution License (CC BY 4.0). International Journal of Sustainable Development. Volume 6. 1013-1017.
[26] Lakshmanan, Selvam & Manimozhi, Braveen & Ramachandran, Venkatesan. (2022). An efficient and secure data sharing scheme for cloud data using hash based quadraplet wavelet permuted cryptography approach. Concurrency and Computation: Practice and Experience. 34. 10.1002/cpe.7324.
[27] https://medium.com/
[28] www.sweetstudy.com