IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 7 ISSUE : 03 Print / Issue Publication Date: 29-Aug-2022

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2022.v07i03.014

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 95-99
Published Online July 2022 in IJEAST (http://www.ijeast.com)

HASHING & DOUBLE ENCRYPTION TECHNIQUE FOR INFORMATION STORAGE IN CLOUD

Soorya Kumar S, Meenakshi P
Department of Computer Science
SRC-sastra deemed university

A. Subramanyan
Software Engineer
Incedo Tech solutions

***Abstract*—Information storage in the cloud is very popular in recent days. The Cloud platform provides various services to its users and one of the important zones of service is the security of the information stored. This project proposes an enhanced approach of a complex Hybrid encryption system involving a Symmetric and an Asymmetric key encryption technique to secure the information on the cloud platform from potential attacks like encryption failure, man-in-middle attack and Insider attack etc along with a hashing technique for the key.**
The proposed hybrid encryption system involves a newly designed Symmetric key technique "Dehex Algorithm" which encrypts the information with a random key generated from the input size. The Dehex algorithm is followed by the ECC algorithm which is an Asymmetric encryption method. The output formed will be double encrypted information, which then reaches the cloud storage. The keys used for encryption need to be securely stored and so the keys are subjected to the SHA hashing algorithm. Hence this new approach can be one of the ways which can be used for securing information stored in the cloud.

***KeyWords* - Dehex algorithm, Elliptical Curve Cryptography (ECC), SHA, SMTP Protocol, Cloud, data transfer, security.**

I. INTRODUCTION

Communication has been a lot in today's world and yet it grows more and more in the future. There exists a lot of information in this world which has some purpose to do. As the information grows more and more, the task of saving them securely is also very high. They need to be maintained with special care so as to satisfy the needs in the future. Till then, the information must be stored in local (or) online directory such as cloud until the information is taken by the user. Storing the information safely is the utmost concern. The most important condition in communication of data and messages in security. Needing security is a tedious task. There exist many false people called Hackers (or) attackers whose job is to seek (or) take information without their knowledge. There may be a possibility of information getting leaked. Since the path cannot be secured as it is huge, the message is encrypted and stored which has been done by the users for the past few years. As information and technology grows higher and higher, the risk also grows higher.

Then the intruders (or) Hackers also develop themselves to some sort of new ways to get the information from the other's user. So new algorithms must be developed to ensure that avoiding the same algorithms which would be easy for the intruders to peek through. Even though some algorithms that are existing are strong, adding new algorithms and using them may develop some new type of encryption which would create some toughness of breaking it. At present days, using double encryption is more popular as it creates more security than using a single algorithm.

Thus, protecting the information would be fair enough to make sure that it is safe. It is very difficult to secure the path as it is huge. As we create, it is difficult to maintain the security as updating them requires a lot of work. To maintain privacy over the unsecured network, the messages are encrypted and sent to the receiver. Messages are modified first, then sent to the receiver and remodified later to see the original message.

II.WORKING MODULE

A. Working of Encryption module–

The algorithm requires an input to be started. The input is given as a text file format (.txt file). The first algorithm is called the "Dehex Algorithm". This algorithm is considered the first level of encryption. The output of the dehex algorithm is given to the second level of encryption called "ECC" (Elliptical Curve Cryptography. The output from ECC will be doubly encrypted.

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 95-99
Published Online July 2022 in IJEAST (http://www.ijeast.com)

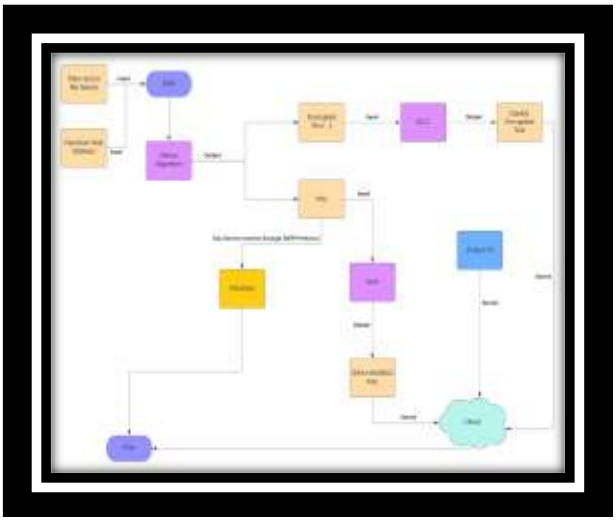

Fig. 1. Work flow diagram of encryption module

The key which is generated from Dehex algorithm is subjected to SHA algorithm so that key won't be visible to others. The main advantage of using SHA is that it cannot be decrypted. The cloud connection is established from the python shell. An unique id is created at random to identify the contents that are stored in the cloud.

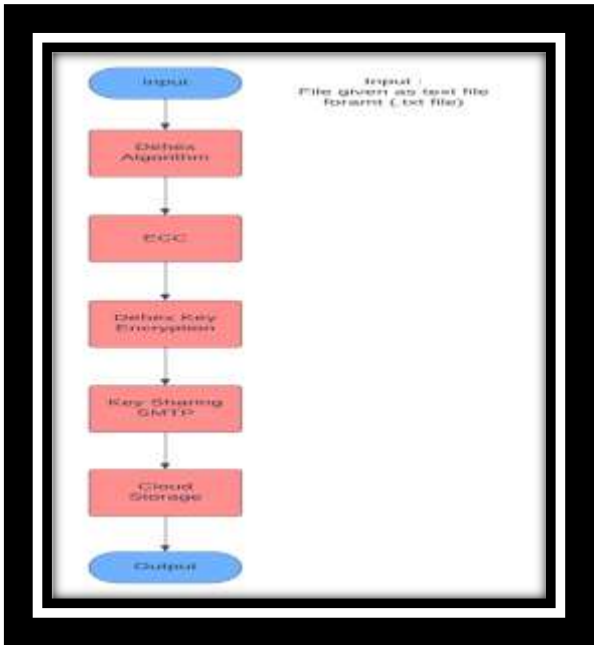

Fig. 2. Architecture diagram of encryption module

Then the doubly encrypted text along with the hashed key is stored in the cloud. Then the key file along with the unique id is sent to the receiver through SMTP (Simple Mail Transfer Protocol). This mail is sent for the decryption.

B. Working of Decryption module –

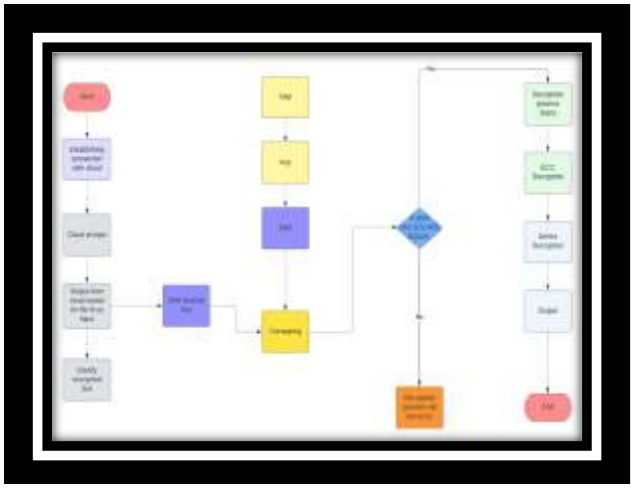

Fig. 3. Work flow diagram of decryption module

First, Cloud connection is established between the python terminal. Then the doubly encrypted information along with key hashed value are taken. The contents from the cloud is taken through the unique id. Then the key file which is sent through SMTP protocol (mail) is taken and subjected to SHA again.

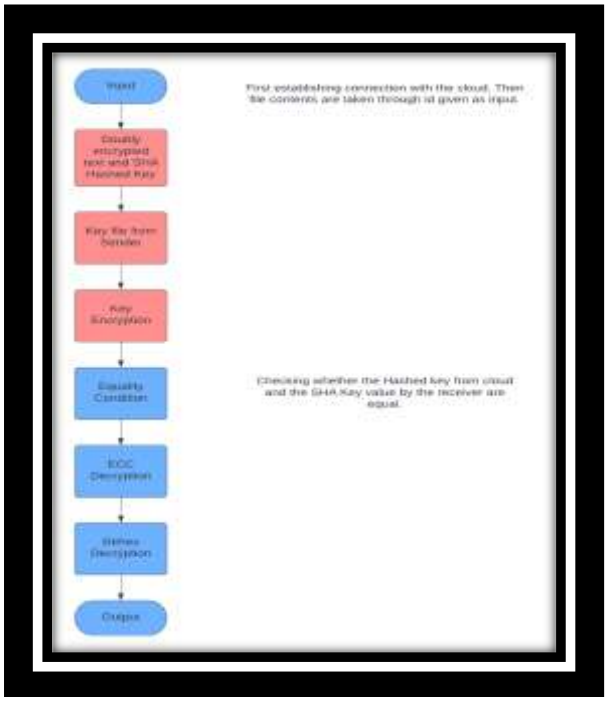

Fig. 4. Work flow diagram of decryption module

If the SHA Value taken from the cloud is equal to SHA value which is obtained from the SMTP protocol, then the decryption starts. Else the decryption process would not occur since key mismatch. This is done so that only authorized users must have access to the message sent.

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 95-99
Published Online July 2022 in IJEAST (http://www.ijeast.com)

The first stage of decryption is called ECC (Elliptical Curve Cryptography), where the double encrypted text is given as input. The Output from ECC is sent as input to the Dehex algorithm which is called the second round of decryption. The output will be the plain text (or) original message that users want to see.

C. Working of Cloud module –
It is defined as Highly flexible non-relational database which handles structured, unstructured, semi-structured data. It has a capacity to handle and store large amounts of data.
It uses a different form storage format called BSON, which is called the Binary form of JSON format. It is used so that it can handle various data types.
MongoDB stores in the form of collections and documents. Collections are nothing but a set of documents. Documents consist of Key-value pairs, which are used for identification. The structure of the documents is not constant, as it changes when new data are added and deleted.

D. Working of Mail Protocol -
It allows for the transfer of information between the sender and the receiver. It helps to transfer messages between different devices (or) on the same device. It is also considered as one of the best and emerging activities that are carried out through the internet.
It first establishes connection with the receiver through TCP protocol. The connection is established through port 25. After establishing the connection, the mail is sent to the receiver successfully

III.PROPOSED ALGORITHMS

A. Dehex algorithm –
It is a newly created Symmetric Key Cryptosystem (or) Secret Key Cryptography, which is easy and straightforward to use. it's used for faster encryption. This algorithm is employed to encrypt input files of text format only.

This algorithm encompasses a key which is to be used for both encryption and decryption. it's also ready to transfer large amounts of information with minimal time and value.

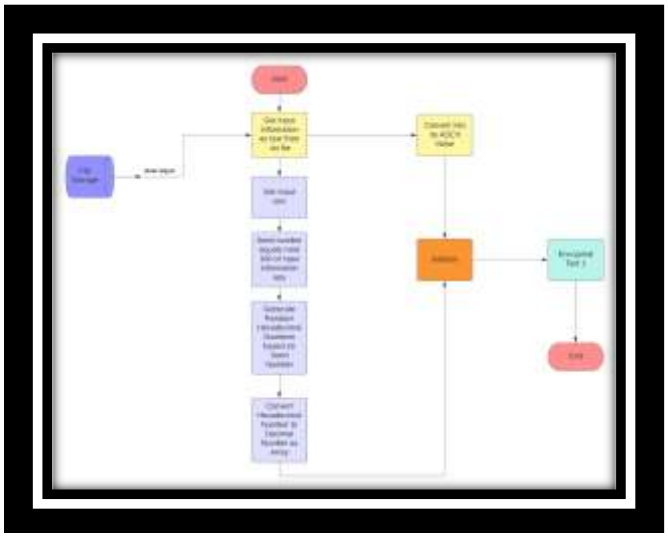

Fig. 5. Working of dehex algorithm

It comes under Substitution Technique. It works under the Stream Cipher Model. It creates a key supported the computer file given by the user at run time.
Since the secret's generated dynamically, its key size and key contents are unpredictable by the user. The generated secret is then added with the text input successively giving another text, which forms the primary level of encryption.

B. Elliptical Curve Cryptography (ECC)–
It is an Asymmetric Key (or) public key cryptosystem which is taken into account as a robust cryptographic approach.
ECC maintains a high level of performance and security. In recent years, since industry has grown, this has been adopted by hundreds of companies as an innovative tool for security technology.
It generates security between key pairs for public key encryption by using the mathematics of elliptic curves. This algorithm is popular due to smaller key size than the other algorithms. They are very difficult to crack mathematically. They are widely utilized in many web applications since key length is small and effective for usage.

C. Simple Hash Algorithm (SHA) –
SHA Stands for Secure Hash Algorithm which is employed for hashing data. It shortens the input file into smaller forms which can't be understood.SHA isn't considered as an encryption algorithm, rather is taken into account as "One Way Hash Function".
Data is transformed into a secured format that's unreadable. But it will be readable providing the receiver encompasses a key that matches it.SHA Provides a feature of "One-Way-Encryption", which suggests that there's no possibility of decryption.

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 3, ISSN No. 2455-2143, Pages 95-99
Published Online July 2022 in IJEAST (http://www.ijeast.com)

Even if one character is modified from the entire document, the SHA value is going to be different than obtained before. Since using it, whether or not the database is stolen (or) hacked then he would know only the hashed passwords and not the initial passwords.

IV. MERITS-

In Dehex Algorithm, the key generated is of randomness whose length cannot be predicted. The key used is stored and hence used in both encryption and decryption process. Even though Dehex algorithm can protect the text in secure way, to add more security it is then made to pass through the Second encryption Algorithm called as "ECC" which also protects the text in secure way. Thus, the input text is double encrypted.

Instead of taking the local databases which could be a threat to attack, the encrypted information and SHA-Hashed Key is stored in large databases called as "Cloud". Since Cloud is huge, the probability of finding the information is decreased.

The key generated in Dehex is subjected to SHA where it is converted into alternative form. It is then used in the decryption process for key authentication and validation. The key stored in file format is then sent to receiver through Mail Transfer protocol for the decryption purpose. If encryption is done and stored in cloud, the user can decrypt them at their required time. There is no time bound that decryption must occur once encryption is done.

Confidentiality: It ensures the documents are seen by the receiver only.
Authentication: It checks whether if the receiver is the known and valid for the sender.
Integrity: It ensures that only the sender and receiver have access to change the information.
Availability: Sender and receiver have access to the information all the time.
Access Control: Prevent the use of unauthorized access. It provides the feature that the resources are available for access at the target computers.
Privacy: User has rights to taken control of the information.
Authorization: Ability to access the resources by the receiver through mail sharing and cloud.

V. RESULTS-

The chances of unauthorized access are decreased by using the concept of double encryption and decryption. Using Symmetric and Asymmetric cryptosystem, the complexity of encryption will be higher and chances of stealing them would be minimal.
The encrypted text along with key is stored in cloud, since the local storage might be under the threat of attack. The message which is sent as input during encryption process is same as message after decryption process is done. As cloud is vast and huge, the files are identified by the authorized user through the id which is generated at random.During each encryption process, different keys are generated which ensures that humans cannot predict.

Fig. 6. Encryption module

Fig. 7. Decryption module

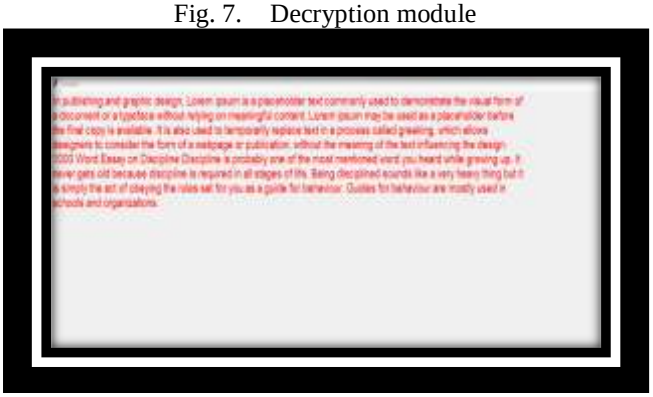

Fig. 8. Output module

VI. REFERENCES-

[1]. Aamir Nadeem, Muhammad. (2016): Cloud Computing: Security Issues and Challenges
[2]. Yan, Zheng; Deng, Robert H.; Varadharajan, Vijay. (2017): Cryptography and data security in cloud computing
[3]. Selvanayagam, Joseph; Singh, Akash; Joans, Michael; Jeswani, Jaya. (2018): Secure File Storage on Cloud Using Cryptography

[4]. Imran Tariq, Muhammad. (2019): Agent Based Information Security Framework for Hybrid Cloud Computing.
[5]. Yang, Pan; Xiong, Naixue; Ren, Jingli. (2020): Data Security and Privacy Protection for Cloud Storage: A Survey
[6]. Du, Leilei; Li, Kenli; Liu, Qin; Wu, Zhiqiang; Zhang, Shaobo. (2020): Dynamic multi-client searchable symmetric encryption with support for Boolean queries
[7]. Feng, Jun; T. Yang, Laurence; Zhu, Qing; Choo, Raymond, Kim-Kwang. (2020): Privacy-Preserving Tensor Decomposition Over Encrypted Data in a Federated Cloud Environment
[8]. Lee, Kwangsu. (2020): Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption
[9]. Sharma, Surbhi; Kaushik, Baijnath; Khalid Iman Rahmani, Mohammad; Ezaz Ahmed, Mohammad. (2021): Cryptographic Solution-Based Secure Elliptic Curve Cryptography Enabled Radio Frequency Identification Mutual Authentication Protocol for Internet of Vehicles
[10]. Nagarajan, G; Sampath Kumar, K. (2021): Security Threats and Challenges in Public Cloud Storage
[11]. Patel, Aditi; Shah, Nisarg;Ramoliya, Dipak; Nayak, Amit. (2020): A detailed review of Cloud Security: Issues, Threats & Attacks
[12]. Nooh, Sameer A. (2020): Cloud Cryptography: User End Encryption

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143