International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

DYNAMIC SYMMETRIC ENCRYPTION IN GMAIL OVER CLOUD

Venkateshwaran. B[1], Siddharth. H, Varun Sharma[3]

[1-3]*Department of Computer Science and Engineering, SRM Institute of Science and Technology Chennai, India*

***Abstract*—**From the history of email data leakage, for instance, Hillary Clinton's Email Data Leakage and the Marriot Data Breach and the other various massive data breaches, the assur- ance and the trust of security of the email data have become into the user's main concern. Cloud Security is now becoming more and more important now, however, the security for the information stored is still not secure. In the existing system, it is incredibly hard for anyone to get the data while its en-route however that doesn't guarantee the security of the data once the user receives the email. In this paper, we propose a more secure plan in which the user receives the encrypted message so the data will be safe and secure. And it can only be decrypted using a key by the user. This paper provides an intermediary function that can secure authentication for the user and encrypts the email messages sent to the Cloud Storage. The middleware used, encrypts the message with a proposed cryptographic algorithm and then uploads the message to the Cloud Security. In this where the user receives the encrypted message provides data security.

***Index Terms*—Cloud Security, Cryptography, Cloud Storage.**

1. INTRODUCTION

Information Security is not just about securing information from hackers or from any unauthorized access. Information Security is basically like preventing unauthorized access, mod- ification, inspection, tampering of information. Information can be physical or electrical. Information can be anything like personal details or profile on social media, your data on mobile phone or email, your biometrics signatures. Infor- mation Security creates so many research and development areas like Cryptography, Mobile Computing, Cyber Forensics, and Social Media. In the course of the First World War, a Multi- tier Classification System was prepared and created for the sensitivity of the information. And at the beginning of the Second World War, a Classification System was done. To secure the information and war strategy Alan Turing was the person who successfully decrypted the Enigma Machine which was the one used by the Germans to encrypt all the warfare data.

Information Security Programs are all built using 3 common objectives which are also known as CIA- Confidentiality, Integrity, and Availability.

Confidentiality - Confidentiality means protecting the infor-mation from being accessed by unauthorized individuals and entities. Only the people who have the authorization to do so can gain access to all the sensitive information and data.

Integrity - Integrity refers to ensure the authenticity of information and the data — that information is not tampered or modified, and the source of the information is authentic.

Availability - Availability means that information can be accessed by authorized users. If the attackers are not able to compromise or alter the first two elements of information security they may try some other executable attacks like denial of service that would shut down the entire server which would result in making the website unavailable to legitimate users.

2. DYNAMIC SYMMETRIC ENCRYPTION

Cryptography is a way of securing the information derived from mathematical principles and some calculations called algorithms to transform messages in ways that are tough to understand or decipher. These algorithms are all used for key generation and authentication to protect web browsing on the internet and confidential communications like email. Encryption is the main concept in cryptography. Encryption is the process where a message or data is encoded in a format that cannot be understood by any hacker or unauthorized user. A plain text can be encrypted into ciphertext and then sent through a network channel where no one can eavesdrop and no one can access the plain text and when it reaches the receiver, the ciphertext is decrypted into the original plain text.

Symmetric Encryption is the simplest kind of encryption that involves only one secret key to encrypt and decrypt information. Symmetrical encryption is an old and widely used technique. It uses a secret key that can be anything like a number, a word or a string of random letters. It is a combined or put together with the plain text of a message to modify the content in a particular way. The receiver should know the secret key to decrypt the encrypted message by the sender.

There are two different types of symmetric encryption algorithms:

A. Block algorithms

The block cipher algorithm converts the plain text into encrypted text by taking the plain text's one block at a time. The set of bits is encrypted in blocks of data using a specific secret key. As the data is encrypted, the system possesses the data in its memory as it awaits the complete blocks. The complexity is simple.

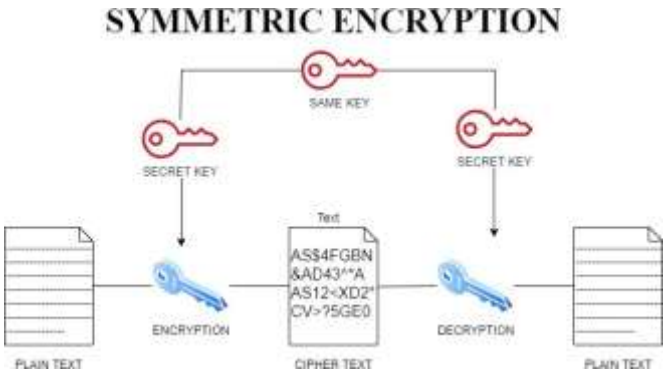

Fig. 1. Symmetric Encryption.

B. Stream algorithms

The stream cipher algorithm converts the plain text into encrypted text by taking 1 byte of plain text one at a time. The information gets encrypted as it streams instead of being retained in the system's memory. The complexity is more complex.

3. Literature Survey

In 2018, Gianluca Fimiani proposed privacy in cloud health information system using Fuzzy Conditional Identity-Based Proxy Re-encryption .Healthcare was traditionally a data-intensive domain, where physicians needed a complete and updated medical history of their patients to take the best medical analysis and choice. Dematerialization of the medical documents and the health information systems to share the patient's health records among healthcare providers were building the way to an effective solution to this issue. But, they were also flooring the way of unimportant privacy problems that were restricting the application of these technologies. Encryption was a valuable means to resolve such issues, however the schemes were not able to cope with all the needs and challenges that the cloud-based sharing of electronic health records imposed. In that work they investigated the use of the scheme where the encryption was combined with the biometric authentication which also defined a preliminary solution.

In 2018 Shuo Qiu, Jiqiang Liu, Yanfeng Shi, Ming Li and Wei Wang proposed a Identity-Based Private Matching in Subcontracted Encrypted Datasets. In 2018 the cloud computing and the storage services were globally used, which led to the sensitive information to be centralized into the cloud to reduce all the management costs, which raised a lot concerns about the data privacy. Encryption was a promising method to maintain the confidentiality of an outsourced sensitive data, but it also made effective data utilization to be a challenging task. They also focussed on the issues of private matching over the outsourced encrypted datasets in an identity-based crypto system that just simplified the certificate management. To solve that issue, they proposed the Identity- Based Private Matching scheme (IBPM), which made them realize the fine-grained authorization that enabled an entitled cloud server to perform the matching operations without leaking any private data. They presented the strict and severe security proof beneath the Decisional Linear Assumption and Decisional Bilinear Diffie-Hellman Assumption. Furthermore, through the analysis of the asymptotic complexity and the experimental evaluation, they were able to verify that the cost of the IBPM scheme was linear to the size of the dataset and it is more competent than the existing work of Zheng and Xu. Finally, they also used their IBPM scheme to build two competent schemes, including the identity-based fuzzy private matching as well as the identity-based multi-keyword fuzzy search.

In 2011 Yanjiang Yang proposed a Multi-User Private Keyword Search for Cloud Computing. Storages for a business service is a vital element of the cloud computing foundation. Database subcontracting was a regular and common use of the cloud storage services, wherein the data encryption was a right approach which enabled the data owner to keep all of its control over to the subcontracted data. Searchable encryption was the first one allowing the private keyword search over the encrypted database. Within the framework of all the enterprises subcontracting the databases to the cloud required a multi-user searchable encryption, whereas virtually all the existing schemes considered only a single-user setting. To keep head above water, they proposed a practical multi-user searchable encryption scheme, which had a number of advantages over all of the known approaches.

In 2017 Muhammad Saqib Niaz and Gunter Saake proposed a Forward Secure Searchable Symmetric Encryption. Data subcontracting to third party clouds posed numerous data security threats. Access by unauthorized users is one of the main security threat to the outsourced data. Unauthorized access was avoided by encrypting the data before outsourcing. However, encrypting the data before subcontracting rendered it unsearchable to the data owner. Searchable encryption schemes were developed to particularly solve this problem. The dynamic symmetric

encryption was the one that permitted the data owner to add or delete a file after data subcontracting. Dynamic searchable encryption schemes were fragile and unprotected to two specific security threats that were not applicable to the static searchable encryption schemes namely forward privacy and backward privacy. Forward privacy required that the addition of a file should not reveal the presence of a previously searched keyword. Backward privacy required that a search should not return the file identifier of a previously deleted file. In this project, they proposed a dynamic searchable scheme that guaranteed forward privacy. It only used the symmetric key algorithms which reduced the needs and conditions for storage and the processing power on the client side. Furthermore, their proposed scheme was space reclaiming. After the deletion of a file, the redundant data nodes were also deleted from the secure index in the subsequent searches. Because of this space reclaiming capability of the scheme, the scheme was also partially backward private.

In 2019 Yang Lu and Jiguo Li proposed the Construction of Certificate-Less Encryption against Outside and Inside Keyword Guessing Attacks. Searchable public key encryption was a beneficial cryptographic paradigm that enabled an unreliable and undependable server to recover the encrypted data without disclosing the contents of the data. It provided a encouraging solution to the encrypted data retrieval in the cryptographic cloud storage. Certificate-less public key cryptography (CLPKC) was a cryptographic primitive that had a lot of benefits. It overcame the key escrow problem in identity-based cryptography (IBC) and the cumbersome certificate problem in conventional public key cryptography (PKC). Encouraged by the fascinating features of CLPKC, several certificate-less encryption with keyword search (CLEKS) schemes has been presented in the literature. However, their cryptanalysis demonstrated that the previously proposed CLEKS frameworks suffered from the security vulnerability caused by the keyword guessing attack. To solve the security weakness in the previous frameworks and provide resistance against both the inside and the outside keyword guessing attacks, they proposed a new CLEKS framework. Under the new framework, they also created a solid and tangible CLEKS scheme and officially demonstrated its security in the random oracle model. Compared with previous CLEKS schemes, the proposed scheme had overall better performance while offering stronger security guarantee as it would withstand the existing known types of keyword guessing attacks.

4. PROPOSED SYSTEM

The proposed system is a middleware which authenticates the user. To use the encryption initially, the users have to register using a valid G-mail ID and Password. Then they have to sign in using their credentials. After the authentication of the user, the user will be allowed to send an encrypted E-Mail. When the user sends a message, each letter will be converted to binary values and value 1 is added to the end to mark the end of the phrase. The phrase size is converted into binary and added. The binary value of the phrase is kept at first and the binary value of the size is kept at last and the middle is padded with 0's to get the block size. However, the message needs 64 words, which need to be created from the block. But with each word will need 32 bits long and we only have enough for 16 words. To get the rest of the words we use the equations in SHA-256 with RSA Algorithm to encrypt it with a key. And the encrypted message is sent and they key is also sent. The key is generated using a random function to produce a 5 letter alpha-numeric value. To decrypt, the receiver should register in the middleware and sign in using their credentials and after its authenticated, the decryption option will be available where the encrypted message has to be entered along with the key. After submitting the encrypted message will be decrypted. This system is proposed to strengthen and reinforce security since G-mail is being widely used today for communication.

5. SYSTEM ARCHITECTURE

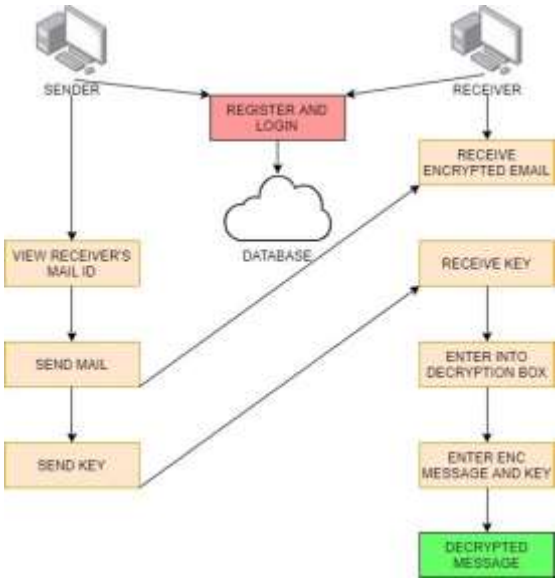

Fig. 2. *System* Architecture.

The proposed system consists of sublayers. It involves User, Middleware System, and the Cloud Storage System. The mode of communication takes place with HTTPS.

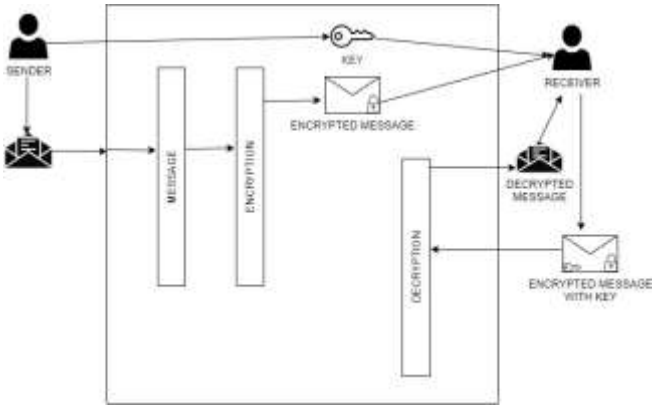

Fig. 3. System Model.

a) User

The user is an actor who registers an account in the middleware and stores the details in the storage cloud system respectively. He/she can access the system by entering the credentials in the middleware that opens the connection to the functions and enable them to perform actions in it.

b) Middleware

The middleware is the hub that can send an encrypted message and key and which also provides decryption of the encrypted message.

1) Send Encrypted Message and Key: The middleware is the hub that can send an encrypted message and key and which also provides decryption of the encrypted message. This is the module to get executed when the user wants to send messages or to send key. After the user accesses the system by entering their credentials, they can send messages and keys. On sending the message, the message is taken straight to the encryption module. After that, the message gets split and turned into binary values. And the message is encrypted using the encryption algorithm used in the middleware. When the user sign-in, it also goes to the key generation module. So every time when the user sign-in a new random key will be generated. After the user sends the message, they can send the key.

2) Key Generation: On signing in the middleware also calls the Key Generation module. The key is generated using a random function that creates a 5 letter key. The key consists of all the alphabets and all the numbers. The key generation module generates a random 5 letter alpha-numeric key.

3) Encryption/Decryption: On Encryption, each part of the file is encrypted by the conversion of the alphabets into a binary value and using the equations used in SHA-256 with RSA Algorithm and are directly sent to the other person's account. When the message is sent the algorithm that was used to encrypt the message and the respective key used is logged by the middleware system and it's stored in a separate file.

On Decryption, when the user wants to decrypt the message, it goes to the decryption module. The middleware system asks for the user's private key and the encrypted message to decrypt the message. Once the encrypted message and the key are entered, the algorithm is used to decrypt the message.

C. Cloud Storage

Cloud storage is the place where the credentials and the key technically get stored. Cloud storage is the place where anyone can save all the files and folders or any kind of data and use the storage anywhere, anytime. It is preserved, operated and administered by a cloud storage service provider on a server that is built on virtualization techniques.

CONCLUSION

In this work focusing on providing encrypted email, the concept of PMSEHS was proposed in this paper. The utilization of E-Technology is growing day by day. Most of them are using E-mail as a primary mode of communication. So, it's crucial that the information is secured. SHA-256 with RSA Encryption is a mode of encryption which is a union of RSA encryption and a hash function. This makes the encryption very much secure and at the same time, it's respectively quick in encryption and decryption.

ACKNOWLEDGMENT

We are grateful to our guide Dr.S.Prasanna Devi from faculty of SRM Institute Of Science And Technology, for their continuous guidance and invaluable support that helped to improve the paper greatly.

REFERENCES

[1] Xiaoyun Wang and Hongbo Yu, How to Break MD5 and Other Hash Functions. EUROCRYPT 2005, LNCS 3494, pp.19-35, 2005.
[2] Hang Chen, Jianfeng Zhou and Shan Feng, Practical and Effective Two-Way Authentication System based on SHA and RSA Algorithm,
COMPUTER SECURITY, pp.6-8, 2006

[3] Zhimin Li, Hongan Jiang and Cunhua Li, Collision Attack on NaSHA- 384/512, 2010 International Conference on Networking and Information Technology, pp243-246, 2010.

[4] H. Ren-Junn, S. Feng-Fu, Y. Yi-Shiung and C. Chia-Yao "An effi- cient decryption method for RSA cryptosystem" Advanced Information Networking and Applications, 2005 (AINA 2005). 19th International Conference on, 2005, pp. 585-590 vol.1.