Preserving Data Privacy Using Self Destructing Data System

Vasant Diwane[1], Prasad Doke[2], Shabbir Essaji[3], Vinayak Gadekar[4]

Department of computer Engineering

Vishwakarma Institute Of Information Technology Pune-411048

Abstract- Today, in the world of Internet, preserving the privacy of confidential data plays crucial role. When confidential data such as bank account numbers, passwords and other important information shared through internet, it can be misused by miscreants. These data are cached, copied on the cloud service providers. Self-destructing data provides a mechanism in which the data is destructed or deleted after particular amount of time specified by sender or client. Here, in this paper, we present a system which follows the same concept. The encryption and decryption algorithms are used at the time of uploading and downloading the files respectively.

INTRODUCTION

The use of Internet has been increased from last few years in greater extent. There are multiple sectors which are directly dependent on internet service to share their confidential data, Such as banking sector, finance company. These institutions or organizations make use of cloud technology to store data. This storage is provided by CSP's (Cloud Service Providers). They subjectively hope that service providers will provide security policy to protect their data from leaking.

As now people rely more on internet and cloud technology, there are many possibilities that the private data such as passwords, account numbers may be misused by attackers. The copies of data is stored or cached in the network while the sender or client has no control over this. In vanish[2] system, the keys are generated for every file, the data is stored along with its secret key in P2P system with distributed hash tables(DHT). Key is generated by using Shamir secret sharing algorithm [3]. The Shamir algorithm divides the key into several parts before storing, further it says that if one cannot get the enough parts of the key, will unable to get the data or to encrypt the data. So, the key corresponding to file is deleted, while encrypted files still remain at the storage node.

- Our system focuses on deletion of files that are stored on the storage node, along with its corresponding encryption key. This deletion process is executed after specified amount of time provided by user or client. This user specified time is said to be TTL (Time to Live).

- Our system provides the Interactive User Interface to carry out these operations.

1. PRIVATE DATA IN THE NETWORK

When the private information is shared from the client, it is stored on the main server. While sharing the information from client to server, the data might pass through multiple intermediate servers. Sometimes, such intermediate servers are larger in number. The data which is being shared is archived in each and every intermediate server. This archived data will remain as it is even if it is deleted from main storage server. For the sectors which need great privacy and confidentiality such as banking and finance sector, this scenario tend to increase the problems. The local destruction of private data will not work in cloud storage or cloud technology. The data must be deleted permanently form all the intermediate servers through which it has passed before.

Another factor is that, while passing through the intermediate servers the data must not be read by third-party or the person who is not authorized to do so. That means the information should be in format, such that only user and the person who is authorized to read it can get access to it.So the information is shared in the encrypted format. And this encrypted data can only be decrypted with the help of key which is associated with that particular file.

2. PRIVACY IN VANISH

Somehow, Vanish system also provided the mechanism to preserve the privacy of information. Vanish is a system that creates the messages and destructs them after some period of time. The Distributed Hash Tables (DHT's) discard the data for which the time is expired. The key is lost permanently and the encrypted data becomes unreadable for infinite time after data expiration. Vanish works by encrypting the data with a random key and storing it in shares in DHT. However, Sybil attacks may compromise the system by continuously crawling the DHT and can get the key references.

Vanish had proposed two schemes as follows:

3.1) *Fire Vanish*

Fire Vanish had provided a plug-in for Firefox browser. This plug-in particularly developed for G-mail service. By using this plug-in, when any user uses G-mail service for communication or for sharing information, user asked to put a time limit or Time to Live (TTL) before sending. The file may be of format .txt, doc file etc. When time expires with corresponding file, the file is discarded.

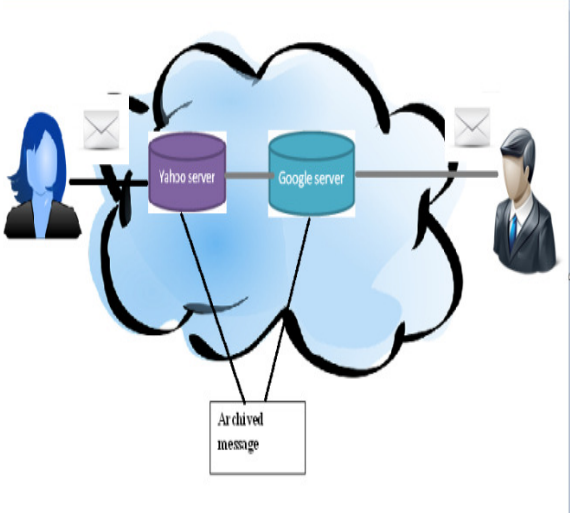
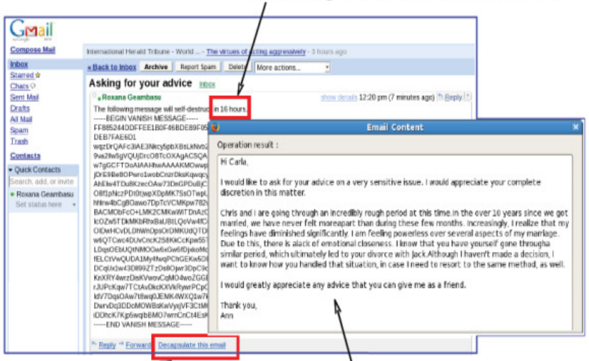


Fig. 1(a) Archived Messages on servers

"This message will self-destruct in 16 hours"



Asking for your advice

Roxana Geambasu 12:20 pm (7 minutes ago)

The following message will self-destruc in 16 hours.

```
-----BEGIN VANISH MESSAGE-----
FF885244DDFFEE1B0F46BDE89F05
DEB7FAE6D1
-----END VANISH MESSAGE-----
```

Operation result :

Hi Carla,

I would like to ask for your advice on a very sensitive issue. I would appreciate your complete discretion in this matter.

Chris and I are going through an incredibly rough period at this time.in the over 10 years since we got married, we have never felt moreapart than during these few months. Increasingly, I realize that my feelings have diminished significantly. I am feeling powerless over several aspects of my marriage. Due to this, there is alack of emotional closeness. I know that you have yourself gone througha similar period, which ultimately led to your divorce with Jack.Although I haven't made a decision, I want to know how you handled that situation, in case I need to resort to the same method, as well.

I would greatly appreciate any advice that you can give me as a friend.

Thank you,
Ann

"Decapsulate this email"

Decapsulated email content popup window

Fig. 1(b) Firefox plug-in for Gmail.

3.2) *Vanishing Files*

Vanishing file is the application which can be used directly or by with other applications such as trash bins. The users can wrap the sensitive data or private information into VDO i.e. vanishing data object, which is discarded after timeout.

4. ENCRYPTION AND KEY GENERATION

RSA:

RSA (Ron Rivest, Adi Shamir, and Leonard Adelman) algorithm is used for Secured data transmission. In RSA the asymmetry is based on the practical difficulty of factoring the product of two large prime numbers. The client will have the RSA algorithm for encryption at the time of uploading and for decryption at the time of downloading.

RSA algorithm requires 3 steps:

4.1) Key Generation:-Client generates two keys out of which one is private and one is public. Public key is broadcast over the network to all, while the private key is kept secret. Public key is derived or created on the basis of two large prime numbers along with an auxiliary value. The prime numbers are kept secret. P and Q are selected at random which are prime numbers.

4.2) Encryption:-Client transmits public key and keeps private key secret. And encryption is done with the help of public key.

4.3) Decryption:- The file is decrypted at the client side with the help of private key.

RSA Algorithm:

1. Choose P=prime number
   Q= another prime number
2. Compute n=P*Q
3. Compute φ(n) = (P - 1) * (Q - 1)
4. Choose e such that 1<e<φ(n) and e and n are coprime.
5. Compute a value for d such that (d*e)% φ(n)-1.
6. Public Key is (e, n).
7. Private Key is (d, n).

5. PROCESS

5.1) *Connection of Client to the Server*

When user wants to send file, file first uploaded on server. For uploading or sending file to server, a connection between client and server must be established. Server gets the details about client after establishing connection, such as IP address, name of the client PC etc. Client will remain connected to the server throughout the process. Client will be disconnected only after closing the desktop application.

5.2) *Log In/ Sign Up*

User logs in, if user has already registered to the server. The code on the server side checks if the login credentials of user present on database. If no user data present in server database, then user has to sign up to the server by providing all necessary information.

5.3) *File Uploading*

When user uploads a file to the server, user must enter file name along with ttl. The data in the file encrypted with encryption algorithm and the file is sent to server. After sending successfully to server, the file is removed from client machine.

Algorithm:

```
1. Start
2. Select file from local disk of any type.
3. Set TTL to file .
4. Set Password for encryption.
5. Encrypt file .
6. Upload encrypted file on Server & delete temporary file.
7. End.
```

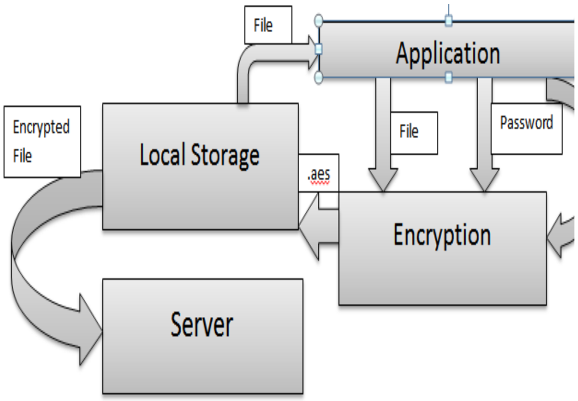


Fig. 2. File Uploading.

5.4) *File Downloading*

Any authorized user can download the file from server with his respective account after logging in. The file is downloaded is in the encrypted form. The file is decrypted after downloading. This decryption is done with the help of the public key which is shared publicly by the sender and the private key on the receiver side.
Algorithm:

```
1. Start
2. Display the List files present

3. Select file.
4. Check TTL of file.
    4.1 If TTL>0 then goto 4.
    4.2 If TTL<=0 then follow deletion algorithm.
5. Download file.
6. Decrypt file using password(Public and private key)
7. Show original file contents.
8. End.
```

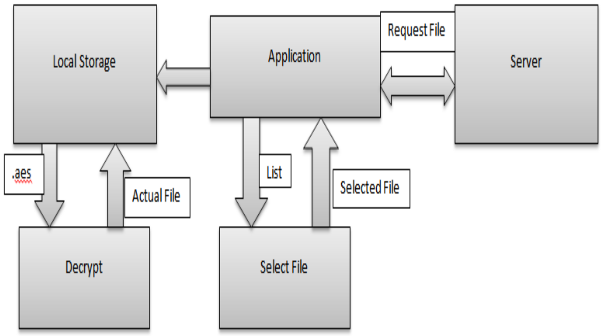


Fig 3. File Downloading.

6. DATABASE ON SERVER AND DELETION OF FILES

When user signs up, the file is created. All files shared by user are stored in the same file only. The name of the file is the username of the user itself.

The information of files is stored in the database such as filename, TTL, upload time and date, downloads. Threads are created for each file, thread will remain alive for the time specified with that file.

CONCLUSION

After the thorough analysis of the current situation of the extent of security standards enforced in the standard public or private networks, we come to know that, self deletion of private/confidential data along with the encryption mechanisms is the necessity for the communication networks. Our research mainly focuses on encryption of data along with the self-deletion for the most secure communication method. In short, we are assigning the specific amount of time for the data to delete by itself along with the standard encryption mechanism.

REFERENCES

[1] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructing data," in *Proc. USENIX Security Symp.*, Montreal, Canada, Aug. 2009, pp. 299–315.

[2] Lingfang Zeng , Shibin Chen , Qingsong Wei , and Dan Feng, "SeDas: A Self Destructing Data System Based on Active

Storage Framework", Wuhan National Laboratory for Optoelectronics, School of Computers, Huazhong University of Science and Technology, 430074 China.
Data Storage Institute, A*STAR, 138632 Singapore