Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 9, Issue. 4, April 2020, pg.44 – 48

INFORMATION SHARING ACROSS ORGANIZATION USING SYMMETRIC KEY ENCRYPTION

Sowmiya M[1]; Subeksha S[2]; Vanmathi T[3]; Vidhupriya P[4]
[1]UG Student, CSE & Rajalakshmi Engineering College, Tamilnadu, India
[2]UG Student, CSE & Rajalakshmi Engineering College, Tamilnadu, India
[3]UG Student, CSE & Rajalakshmi Engineering College, Tamilnadu, India
[4]Assistant Professor, Dept. of CSE & Rajalakshmi Engineering College, Tamilnadu, India
sowmiyaa0520@gmail.com; subee3010@gmail.com; vanmathitamil3368@gmail.com; vidhupriya.p@rajalakshmi.edu.in

Abstract: ***Many Organizations share data through the network which provides numerous security vulnerabilities. In the existing systems, when a person wants to transfer details, they may send data over the network where data breaches may occur. So, we create a system that allows all the members of an organization to upload and retrieve data using Key based data access. Initially, they must register themselves and then login to the system. They can upload a file and for each file, system will generate a unique key using random class. After data is uploaded in the database, it is encrypted using symmetric key encryption technique called Advanced Encryption Standard (AES). This algorithm is more secure and supports larger key sizes than triple data encryption standard and other algorithms. AES is faster in both hardware and software. To download a file of other branch, they should send request and the request will be processed by the admin and key will be sent to their email id. Here, we use Simple mail transfer protocol as mail transfer agent and use port number 587 for transport layer security to send e-mail. With this key, file can be decrypted and then provided to the user. Unbreakable security, effective storage and transmission, quicker processing and overall improved efficiency of this system makes it ideal for the enormous data handling in present day.***

Keywords-- Confidentiality, Advanced Encryption Standard (AES), Symmetric Key, Authorized Access.

I. INTRODUCTION

Online administrations use a secret phrase confirmation which is the most broadly utilized verification technique, for it is accessible requiring little to no effort and is simple to send. Consequently, secret phrase security consistently draws in incredible interest from the scholarly community also, industry. Despite extraordinary research accomplishments on secret key security, passwords are yet broken since client's imprudent practices. For example, numerous clients frequently select frail passwords; they will in general reuse same passwords in various frameworks. They normally set their passwords utilizing recognizable jargon for its benefit to recall. In this way, Internet plays an important role in transferring large amounts of data in various fields. Some of the data might be hacked and misused as they are transmitted through insecure channels [6]. So, data security is an important task while sharing information across organizations. Private and public sectors use different techniques to protect the data from intruders. One such technique is the use of cryptographic algorithms for encryption and decryption process. In this system we use Advanced encryption Standard to secure the data. AES is a symmetric encryption format where we use the same key for encryption and decryption. The main aim of this algorithm is to replace

DES for its various vulnerabilities. It is extremely difficult for the intruders to get the real data when encryption is done using AES. AES can deal with three different key sizes 128,192 and 256 bits. This will help us use keys of various sizes since the block size is 128 bits.

II. RELATED WORK

1. In this system, they have used a blowfish algorithm. The algorithm encrypts information to unreadable format and then sends over the internet which increases the level of security dimensions. Main disadvantage in using the blowfish algorithm is that the new key requires pre-processing. Each pair of users needs a unique key, so as the number of the user's increase, key management becomes complicated. Blowfish algorithm can't provide authentication as well as non-repudiation as two people have the same key. It also has weakness in decryption [3].

2. In this study, a quantitative model was developed, which incorporates four dimensions: openness towards advanced technology as an individual personality dimension, website usability, including ease of use, perceived security concern, and Green concern for conserving nature resources as the social influence dimension[1].

3. This article proposes and analyzes a general cloud-based security overlay network that can be used as a transparent overlay network to provide services such as intrusion detection systems, antivirus and anti-spam software, and distributed denial-of-service prevention[8].The authors analyze each of these in-cloud security services in terms of resilience, effectiveness, performance, flexibility, control, and cost.

4. To achieve the forward security for public key searchable encryption, our intuition is to bind a search token and its generation time together. We use, the 0-Encoding and 1-Encoding approach for this. The study provided an overview of block cipher, stream cipher and hash function which are used for encrypting the data in the cloud whether it is at rest or in transit.

5. According to the survey conducted in Saudi Arabia and India, there were many security vulnerabilities. Multifactor Authentication, Inbound / Outbound access rules, Server based alarms are common solutions. To make the internet banking infrastructure access more secure, private keys with passwords need to be used. Group policies are being applied to make sure that specific users have minimum required access of the internet banking system resources [2].

III. PROBLEM IDENTIFICATION

In existing systems, Data transfer happens through the network which may leads to attacks inside the network, there may be chances of intrusion and sometimes data loss may occur. Nowadays, employees rely on information to make decisions and requires faster data retrieval to provide customer support. Existing systems are quite time consuming when it comes to data transfer and some of the security measures were not strictly imposed like password and encryption strategies. Also, when data is being generated continuously, there is a risk of the investigators not having enough time to update the details immediately.

IV. PROPOSED SYSTEM

We create a system that mainly allows all the members of an organization to upload and retrieve data using Key based data access. This allows us to handle data without sharing them through the network. To overcome the security problems, we deploy two-way authentication and we use symmetric key encryption technique called Advanced Encryption Standard (AES) for data encryption. AES is an iterative rather than Feistel cipher. Since AES can support keys up to 256 bits, the size of the key can be increased according to data. To access the data stored in any other branch we generate a key to retrieve it. Thus, our system provides on-site data analysis when data cannot be moved. It is like remote access of data without affecting the integrity of data.

V. SYSTEM ARCHITECTURE

A. MODULES

- REGISTRATION AND LOGIN
- FILE UPLOAD
- SEND REQUEST
- KEY TRANSMISSION
- RETRIEVE THE FILE

1. REGISTRATION AND LOGIN

This module has created for the security purpose. In this module the branch manager and other employees must register themselves by providing basic details such as username, password, e-mail id and mobile number. Once registered, they can login using user id and password. It will check whether the username and password match with the registration table. We used bean class for registration in order to achieve encapsulation and interface for total abstraction and it also provides a reference variable to refer current instance of registration data. It well improves the security and preventing from unauthorized user enters to the system. In our project we are using Java Server Pages for creating design.

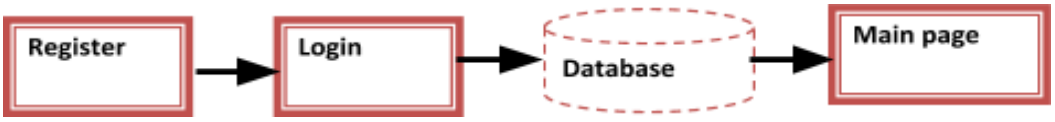

Figure 1. Registration and login

2. FILE UPLOAD

In this module, after login they can upload the file containing confidential data. File format should be in Text(.txt), portable document format(.pdf) and Word document(.docx) related to that branch and it will be stored in the database. For each file using keygenerator class, symmetric key will be generated. The file will be uploaded and then the data present in the file will be encrypted using Advanced Encryption Standard.

Figure 2. File Upload

3. FILE REQUEST

In this module, after uploading the file from branch1, branch 2 will send a request to gain file access of branch 1. To send request, we used doPost method that sends client data and request.getparameter method to retrieve the values such as branch name, username, filename. The admin will then process the request and will be forwarded to the next phase.

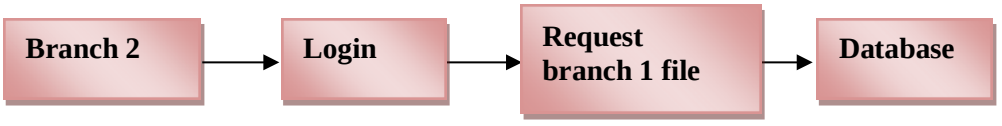

Figure 3. File request

4. KEY TRANSMISSION

In this module, admin will process and validates the request and then transmit key through mail. Here it uses Simple mail transfer protocol host smtp.gmail.com and port number 587 for Transport layer security. It transfers the key to the requested person's mail id using Transport class.

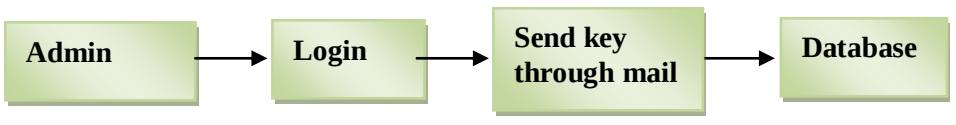

Figure 4. Key Transmission

5. DOWNLOAD THE FILE

In this module, after getting the key from the mail, download the file using the key provided by the branch1.Here we used Joptionpane class to provide dialog box and printwriter class to provide output stream.

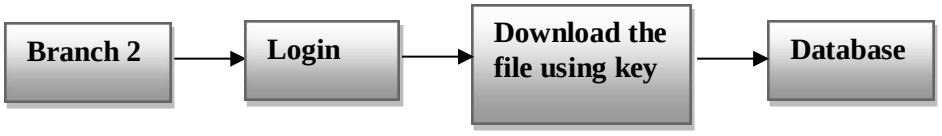

Figure 5. File download

6. WORKING OF THE SYSTEM

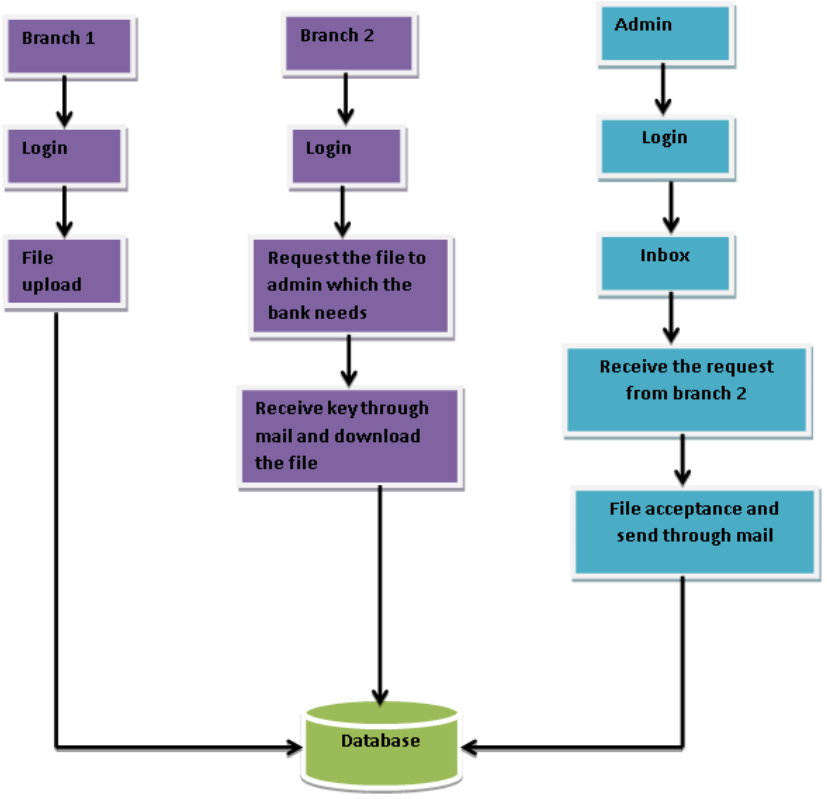

Figure 6. Process flow of the system

V. CONCLUSION

In modern communication system, Information security plays an important role. All confidential and important information are sent over the internet, so it is very important to keep records secure. To protect our information, we should concentrate in privacy, integrity, confidentiality and non-repudiation. In that way, this system maintains high security and helps people to share data by storing and encrypting all their information for future retrieval. Our system uses a key which prevents unauthorized people from accessing the data. This provides security to the user data and keeps them in a more secure way. With increasing dependency on data, this system forms a pillar of improvement for upcoming times.

FUTURE SCOPE

Inter Organizational information sharing is one of the most important deal. Our system allows the organizations to share large volume of data using key access. To enhance this and have effective knowledge about the shared

data we can incorporate open door policy into this. This can be done by developing a questionnaire section for any users who find it difficult to understand the data. The questionnaire field will be visible only between the seeker and the admin who shared the data. This helps in building stronger foundation about the shared data. Impacts associated with the participants of the system can be recorded and respective solutions can be taken.

REFERENCES

[1]. Bo Han, Vijay Gopalakrishnan, Lusheng Ji, and Seungjoon Lee (2017). Network function virtualization: Challenges and opportunities for innovations. Communications Magazine, IEEE, 53(2):90–97.

[2]. Mrs. V. Bhargavi, Dr. M. Lokanadha Reddy (2018). Security attacks and problems in banking and Security challenges and major threats. AIJRHASS 18-118.

[3]. Anupam Baruah, Prof. (Dr.)Lakshmi Prasad (2017). Information Security Using Blowfish Algorithm in E-Banking. Saikia Vol.6 Issue.3.

[4]. Chan, H.K. & Chan, F.T.S. (2017). Effect of information sharing in supply chains with flexibility. International Journal of Production Research, 47(1), 213-232.

[5]. Fulton, C. (2017). Quid pro quo: information sharing in leisure activities. Library Trends, 57(4).

[6]. Zboralski, K. (2016). Antecedents of knowledge sharing in communities of practice. Journal of Knowledge Management, 13(3), 90-101.

[7]. Millen, D. R., & Dray, S. M. (2014). Information sharing in an online community of journalists. Aslib Proceedings, 52(5), 166-173.

[8]. Chang Lan, Justine Sherry, Raluca Ada Popa, Sylvia Ratnasamy, and Zhi Liu (2018). Embark: Securely outsourcing middleboxes to the cloud. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16).

[9]. Lin, F. R., Huang, S. H. & Lin, S. C. (2012). Effects of information sharing on supply chain performance in electronic commerce. IEEE Transactions on Engineering Management, 49(3), 258-268.

[10]. Widén-Wulff, G. & Ginman, M. (2010). Explaining knowledge sharing in organizations through the dimensions of social capital. Journal of Information Science, 30(5), 448-458.

