Multi file security through hybrid mobile application

M.SRIDHARAN

Computer science engineering

***Abstract*— Security and privacy are hot topics now. Today there are many systems that store our files but you are definitely not sure whether your files are 100% safe. The reason is you are storing the files directly into their servers, which is clearly not the one you want. On thinking about the way we can store data securely, we found a model that encrypts the file in client side without even referring the server. Therefore, the file that you will get is simply an encrypted file that is going to be stored in client machine. The application that we built is a responsive web and a hybrid mobile application, which means that it will work the same in all screens and in all platforms, whether it is IOS, Android or Windows, the application is same. We found issues with the system that we built but we also found the solution for the same. When it comes to encrypting data and securing information, people naturally expect the page to be loaded through HTTPS. In this case, I believe it is not necessary, as apart from the initial download of the HTML and assets, no data is been transferred between you and the server – everything is done client-side with JavaScript.**

***Index Terms*—Encrypt, Decrypt, Recovery**

I. INTRODUCTION

It is hybrid mobile application which uses AES algorithm (8 bit) to encrypt files. User who encrypt the file does not need to remember the password all the time. They can provide some questions which gives the password as the answer. No worries we are not encrypting the file simply from the answer for those questions. We are generating a random number for each user and doing a simple calculation based on the random number. Thus, every time when the user does an encryption operation a random number is been added with the passphrase and the encrypted file will be available for them. Thus even if they remember the answer for those questions, they cannot see your file unless they login. We can share the encrypted files only with few group of people thus providing access only to them and creating a secured workgroup. Thus, we do not need to worry about the file that they are storing in different servers because they anyway need to use the above model to decrypt it thereby creating the most secured file system.

II. LITERATURE SURVEY

1. **Suchita Tayde** describes about smart gadgets including smart phones and tablets are gaining huge popularity. Comparing with conventional computer, smart phone is easily carried out and provides much computer functionality, such as processing, communication, data storage as well as many computers services such as web browser, video or audio player, video call, GPS, wireless network. However, smart phone have to come long way in terms of security. Encryption is used for security of information in data storage and transmission process. Various encryption algorithms like DES, 3DES, Blowfish, RSA and others are available to secure the data. In DES, key size is too small. In 3DES, key size is increase but the process is slower than other methods. We have used Advanced Encryption Standard algorithm to overcome above problems. AES algorithm is not only for security but also for great speed.
2. **Wenhui peng** presents detailed study on the features and problems of traditional web learning resources, introduces key technologies in the process of responsive web design with supporting mobile learning resources, analyzes some relevant examples, and concludes with the idea that the responsive web design will play an important role in the future of web design.
3. **Vikas Agrawal** presents detailed study on the process of Encryption and Decryption is perform in case of Symmetric key and public key cryptography using AES and DES algorithms and modified RSA algorithm.
4. **Mordechai Guri** describes about personal information leakage during password recovery on internet services such as Gmail, Facebook, and Twitter. Although most of these services try to maintain user privacy, with regard to registration information and other personal information provided by the user, we demonstrate that personal information can still be obtained by unauthorized individuals or

attackers. This information includes the full (or partial) email address, phone number, friends list, address, etc. We examine different scenarios and demonstrate how the details revealed in the password recovery process can be used to deduct more focused information about users.

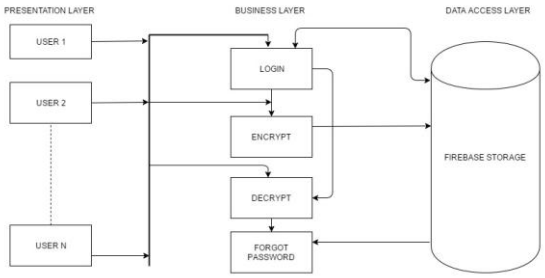
III. PROPOSED WORK

The main aim of our proposed system is not to store the password in database. We also taken into consideration that human can easily remember words that are related to incidents. For example: 24 is my lucky number, If I store password as 24 then there is a chance that I may forgot it. But if I put a security question like "My Favourite number" on top of it then he/she can easily get the password. Thus making it more simple to remember. Thus for every encrypted file there will be a filename and a security question. Thus even if the person forgot the passphrase he can easily decrypt it by flashing the security question to him. If the passphrase is leaked and the encrypted file is also with a wrong person, even then that person cannot decrypt the file. As we are creating a random number with the file and that is stored in our database for that particular person, only, when that person knows the victim's gmail credentials that person can login to the system. Getting to know the gmail credentials of a particular person is highly impossible.

Advantages:

1. The file is highly secured as the passphrase is not stored anywhere
2. Single code base for website, mobile website and mobile application. Thus making the life of developer easier.
3. The recovery is much easier with a simple security question feature.

IV. ARCHITECTURE DIAGRAM



[a]Architecture Diagram

V. MODULE DESCRIPTION

1. SIGNUP

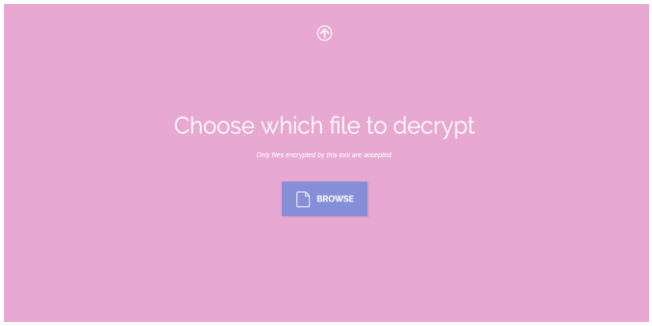
Users will be get logged into the application using google signup their mail id will get stored into database along with that a 4 digit number per user will be generated and stored in database against the respective user's mail id.

2. ENCRYPT

Users will browse the file they need to encrypt and then they will be prompted for a security question and an answer for that question. This question should have 4 digit number as an answer this answer will be used as a passphrase to encrypt a file. The security question will be stored in the database. The encrypted file will be provided to the user to download it in their machine.

3. DECRYPT

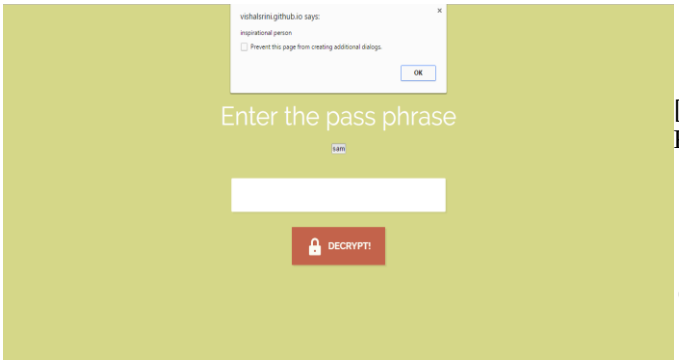
Users will browse for the encrypted file and then they will provide the passphrase to decrypt a file. If they provided the passphrase to decrypt a file. If they provided the passphrase incorrectly, file will get decrypted and downloaded with inappropriate content. To recover passphrase, recovery module will be used.



4. RECOVERY

Only the users who signed up to the application will have recovery of their passphrase. While encrypting a file the users will be asked for a security question which will have 4 digit number as an answer. So when users forget their passphrase to decrypt a file this security question will be flashed to them. They will have the answer for that

combining the 4 digit number that was already generated while signing up will be used as a passphrase to decrypt the file.



VI. Conclusion

Thus this hybrid mobile application secures files using an encryption algorithm called AES algorithm (8 bit) and also by having first 4 bit of 8 bit in client machine itself, we achieve even better security. User who encrypt the file does not need to remember the password all the time. They can provide some questions which gives the password as the answer. No worries we are not encrypting the file simply from the answer for those questions. We are generating a random number for each user and doing a simple calculation based on the random number. Thus, every time when the user does an encryption operation a random number is been added with the passphrase and the encrypted file will be available for them.

References

[1] Suchita Tayde proposed "File Encryption, Decryption Using AES Algorithm in Android Phone", International Journal of Advanced Research in Computer Science and Software Engineering , 2015.

[2] Wenhui peng proposed "The Design and Research of Responsive Web Supporting Mobile Learning Devices", Educational Technology (ISET), 2015.

[3] Vikas Agrawal proposed "Analysis and Review of Encryption and Decryption for Secure Communication", International Journal of Scientific Engineering and Research (IJSER),2014.

[4] Mordechai Guri proposed "Personal Information Leakage During Password Recovery of Internet Services", Intelligence and Security Informatics Conference (EISIC), 2016 European.