International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

ShareSafe - SECURE AND EFFICIENT DATA SHARING APPLICATION

Prof. Renuka Deshpande[1], Ninad Pevekar[2], Aakanksha Patil[3], Ashwini Palasamkar[4]

[1]*Professor, Dept of Computer Engineering, SSJCOE, Maharashtra, India*
[2,3,4] *Students, Dept of Computer Engineering, SSJCOE, Maharashtra, India*

Abstract - *Putting basic information in the hands of a cloud supplier should accompany the assurance of security and accessibility for information very still, in movement, and being used. A few options exist for capacity administrations, while information privacy answers for the database as an administration worldview are as yet youthful. Loads of web accounts are being hacked ordinary despite the fact that the general population web servers like Gmail, Yahoo and Hotmail convey the best known security systems. Nonetheless, assaults generally occur because of individual flaws. It is excessively troublesome, making it impossible to hack the Gmail or Yahoo servers, however more often than not aggressors endeavor to access client's framework itself to get some data about his secret key.*

Key Words: **Smartphone, Security, Privacy, Accounts, Web servers**

1. INTRODUCTION

Cell phones are turning into a noteworthy part in everyone's day by day life. A wide range of exercises, including keeping money or monetary exchanges (e.g. web based shopping), are these days performed online through Smartphone applications while moving. Above all else Smartphone proprietors utilize their Smartphone for exchanges. Notwithstanding, the majority of the procedures used to validate the customer towards the remote authenticator in applications still base upon exemplary (and static) confirmation factors like passwords or biometrics. The way that the customer is moving, while utilizing these applications isn't considered or used to upgrade the confirmation security.

Dependable customer confirmation and information security are as yet real worries for application suppliers on the grounds that the traditional validation factors are open for programmers. Therefore, these application suppliers confine access, by and large, to 30% of conceivable administrations to their customers by means of Smartphone applications.

1.1 LITERATURE SURVEY

P. Gilbert et al.., "Secure mobile apps via automated validation"[1]. They used commodity cloud infrastructure to emulate smartphones to dynamically track information flows and actions. Then automatically detect malicious behavior and misuse of sensitive data via further analysis of dependency graphs based on the tracked information flows and actions.

Weber and Frank Proposed "Multi-factor authentication"[2], by using PIN sent to email as the knowledge factor of the two factor authentication.

W. Jansen and T. Grance proposed "Guidelines on Security and Privacy in Public Cloud Computing"[3].This publication provides an overview of the security and privacy challenges pertinent to public cloud computing and points out considerations organizations should take when outsourcing data.

M. Egele et al. presented "PiOS to detect privacy leaks in iOS applications" [4]. They used static analysis to detect sensitive data flow to achieve the aim of detecting privacy leaks in applications in iOS.

1.2 EXISTING SYSTEM

Cryptographic record frameworks and secure stockpiling arrangements speak to the most punctual works in this field. Some DBMS motors offer the likelihood of scrambling information at the record framework level through the alleged Transparent Data Encryption highlight. This element makes it conceivable to manufacture a trusted DBMS over untrusted storage. However, the DBMS is trusted and unscrambles information before their utilization. Subsequently, this approach isn't pertinent to the DBaaS setting considered by SecureDBaas, in light of the fact that we expect that the cloud supplier is untrusted. Original plain information must be open just by trusted gatherings that do exclude cloud suppliers, mediators, and Internet; in any untrusted setting, information must be encoded.

2. PROPOSED SYSTEM

We propose a novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are intrinsic in cloud-based solutions.

This project also presents a new mobile-based multi-factor authentication scheme based on a pre-shared number, GPS location and Time stamp (PGT).

Unlike SMS-based multifactor authentication, PGT does not have any additional cost for SMSs. Compared to SecurID, PGT is considered to be more secure as SecurID is based on a fixed seed while PGT is based on a modifiab International

Conference on. IEEE, 2009le pre-shared number. Moreover, PGT uses GPS location as an extra security parameter; PGT is also cost-free as it does not require a specific security device like SecurID.

3. METHODOLOGY

3.1 USER AUTHENTICATION

This section discusses the steps involved in PGT multifactor authentication scheme. PGT requires a GPS server to synchronize the current GPS location of the user with the authentication server. It also requires a pre-shared number between the authentication server and the user's mobile device to be set during registration and can be reset whenever it is necessary. Three stages are involved in PGT multi-factor authentication.

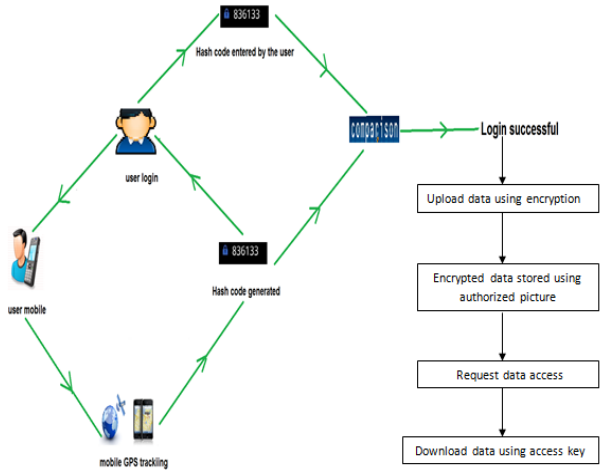

Fig 1: Implementation flow

Stage1: Traditional Log in

In this stage, the user requests his personal web page URL through any internet-enabled device D1. The web portal server S1 has to respond back to D1 with the authentication page asking the user to provide his traditional credentials (username/password). The user provides his credentials to D1 which sends them to S1 for verification. If the user is verified, S1 asks for the security token.

Stage2: Token Generation T1

The PGT phone app is installed on the user mobile device D2 (GPS enabled), this app is responsible for generating the security token T1 according to the following equation where TS1 is the current time stamp:

T1=hash (Pre-Shared Number + GPS + TS1);

At the same time D2 updates the GPS server (S2) with the user's GPS location and time stamp (TS1) through a secured channel (based on a pre-shared key negotiated during the first registration).

Stage3: Token Verification

S1 receives the security token *T1* and gets the GPS updates and time stamp of the corresponding user from S2. Following that, it generates a security token T2 using equation (1). Then it compares *T1* with *T2*, if they match, the user is authenticated and his personal web page is sent back to D1.

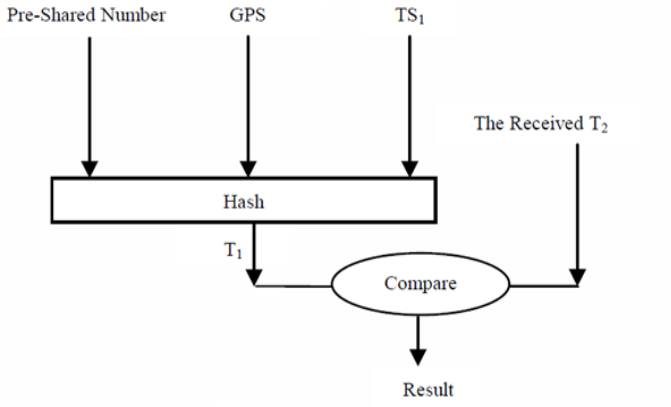

Fig 2: Token Verification

4. DATA SECURITY

4.1 DATA ENCRYPTION

Data is encrypted and stored in the database. While registration user has provided his/her photograph to the CSP. While data uploading the application will click a photograph the user who is uploading the file. This photograph and the requested file is sent to the access point provider who would authenticate the user and will upload the data encrypted.

4.2 ACCESS KEY GENERATION

As the data is uploaded, an access key is generated which is used for other users to download the file.

4.3 DOWNLOAD FILE

Other users have to request the file to the owner to be downloaded. The owner will generate the permission for the requester to download the data. This key is provided to the requester to download the data through which the data is automatically decrypted and downloaded.

5. RESULTS

Client should enlist to "ShareSafe " application in which photo is required . In the wake of enlisting client can login to his record and he will have 4 alternatives which are "Upload File", "Download File", "File List", "Request File". according to his need he can pick one of them. Following are the screen captures of application developed by us.

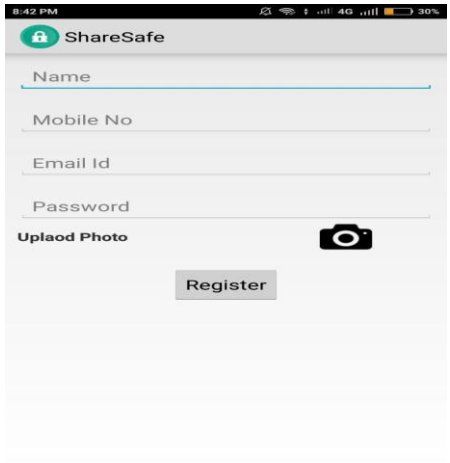

Fig 3: User register

User will register to the app through this window.

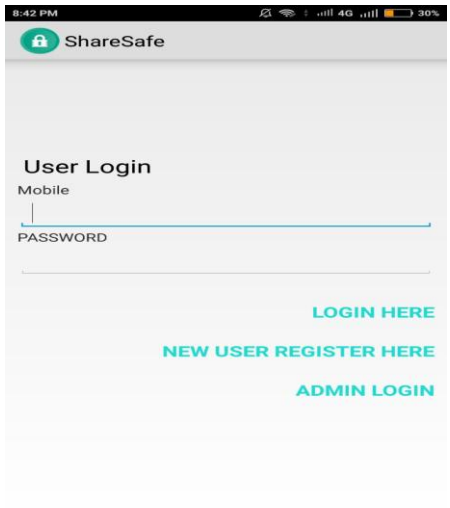

Fig 4: User Login

After successful registration user can login using his mobile number and password.

Fig 5: Admin window

Admin can monitor number of user, uploaded files and file request.

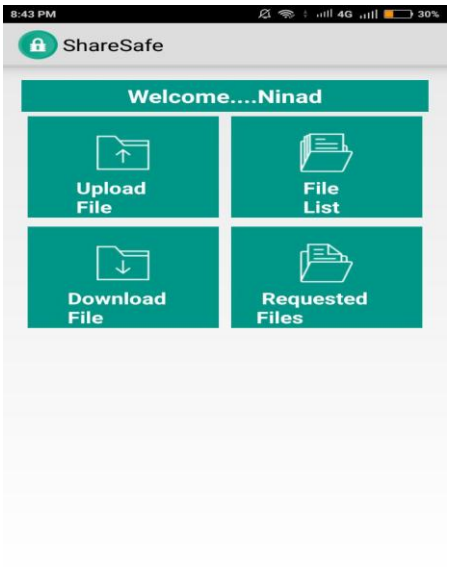

Fig 6: In-app Layout

After successful login user will have multiple options like upload file, file list, download file, requested file.

6. CONCLUSION

We propose an innovative architecture that guarantees confidentiality of data stored in public cloud databases. Unlike state-of-the-art approaches, our solution does not rely on an intermediate proxy that we consider a single point of failure and a bottleneck limiting availability and scalability of typical cloud database services. A new multi-factor authentication method was presented. It utilizes the user's mobile device to generate an OTP which can be used as an authentication second factor. Unlike other methods of multi-factor authentication that employ the use of special devices like a security token which adds more cost to the authentication system, PGT uses a mobile device which is a common device for all users. PGT uses a pre-shared number to generate the OTP. This pre-shared number is not transmitted through any channel which makes it very difficult for the intruder to guess. These and other stated features make our method very cost effective and more secure.

REFERENCES

[1] P. Gilbert et al..,"Secure Mobile apps via Automated Validation", (2000)

[2] Weber, Frank. "Multi-factor authentication" U.S. Patent No. 7,770,002. 3 Aug. 2010.

[3] W. Jansen and T. Grance. "Guidelines on Security and Privacy in Public Cloud Computing"(2013)

[4] M. Egele et al. presented "PiOS to Detect Privacy Leaks in iOS Applications", (2012)

[5] Bauckman, Dena Terry, Nigel Paul Johnson, and David Joseph Robertson. "Multi-Factor Authentication" U.S. Patent No. 20,130,055,368. 28 Feb. 2013.

[6] Aloul, Fadi, Syed Zahidi, and Wassim El-Hajj. "Two factor authentication using mobile phones." Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on. IEEE, 2009.

[7] Ross, Blake, et al. "SPORC: Group Collaboration Using Untrusted Cloud Resources"(2010)

[8] J. Li, M. Krohn, D. Mazieres, and D. Shasha. "Secure Untrusted Data Repository", (2004)