ENHANCED SECURITY FRAMEWORK TO ENSURE DATA SECURITY IN CLOUD USING SECURITY BLANKET ALGORITHM

Sanjeev Kumar Mandal[1], Farzeen Basith[2]

[1]Post Graduate student, [2]Assistant Professor, Department of MCA, Acharya Institute of Technology, Karnataka, India,
sanjeev.mandal93@gmail.com, farzeen107@gmail.com

Abstract

Data security and Access control is a challenging research work in Cloud Computing. Cloud service users upload there private and confidential data over the cloud. As the data is transferred among the server and client, the data is to be protected from unauthorized entries into the server, by authenticating the user's and provide high secure priority to the data. So the Experts always recommend using different passwords for different logins. Any normal person cannot possibly follow that advice and memorize all their usernames and passwords. That is where password managers come in. The purpose of this paper is to secure data from unauthorized person using Security blanket algorithm.

----------***----------

1. INTRODUCTION

Cloud computing is a paradigm of computing, a new way of thinking about IT industry but not any specific technology. It is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure "in the cloud" that supports them.

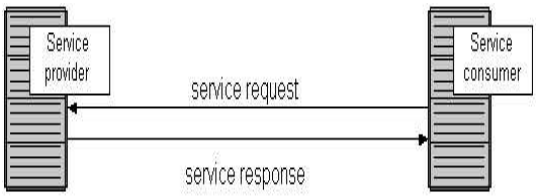
The main concept of cloud computing services is that these services are carried out on behalf of users with hardware that the customers do not own or operate. The user inputs data to the cloud, the data are processed by the cloud service provider according to the instructions of the user, and the output is delivered back to the user.

1.1 Service Models

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications.

1.2 Cloud Services

Cloud services are typically made available via a private cloud, community cloud, public cloud or hybrid cloud. Generally speaking, services provided by a public cloud are offered over the Internet and are owned and operated by a cloud provider. Some examples include services aimed at the general public, such as online photo storage services, e-mail services, or social networking sites. However, services for enterprises can also be offered in a public cloud.In a private cloud, the cloud infrastructure is operated solely for a specific organization, and is managed by the organization or a third party. In a community cloud, the service is shared by several organizations and made available only to those groups. The infrastructure may be owned and operated by the organizations or by a cloud service provider. A hybrid cloud is a combination of different methods of resource pooling (for example, combining public and community clouds).



1.3 Security

Security refers to confidentiality, integrity and availability, which pose major issues for cloud vendors. Confidentiality refers to who stores the encryption keys - data from company A, stored in an encrypted format at company B must be kept secure from employees of B; thus, the client company should own the encryption keys. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. Traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore,

verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data.

Recently, the importance of ensuring the remote data integrity has been highlighted by the following research works [1]–[2]. These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations.

2. LITERATURE REVIEW

While coming with this paper we had visited many small scale industries and companies those are recently using cloud services for outsourcing there confidential data over the cloud and are suffering with some problems while exchanging keys and accessing the services. They are also worried about the recent security techniques, which are currently available. For this paper we have refer the technical paper on Secure Data Access over Cloud Computing and Secure Data Access in Cloud Computing.

Data outsourcing in Cloud Computing is fast becoming economically viable for large enterprises. In fact,this data outsourcing is ultimately retrieving user's control over its own data and does not provide any assurance on data integrity and availability. On behalf of cloud user, a third party auditor (TPA) who has resources and experience that a user does not have can be emplaced to audit the integrity of large data storage. But user data privacy is still exposed to a TPA, which is required to be secured against unauthorized leakage.

Wang and Sherman et al. [3] have proposed a public auditing system of data storage security by developing a privacy preserving auditing protocol. By which auditor can audit without having knowledge of user's data contents. Wang and Sherman also proposed a batch auditing protocol where multiple auditing tasks from different users can be performed simultaneously by a TPA. A public auditing scheme consisting four algorithms (KeyGen, SigGen, GenProof, VerifyProof) has been used. KeyGen is run by the user to set up the scheme. SigGen is used to generate verification metadata. GenProof is executed by Cloud Server to provide a proof of data storage correctness. VerifyProof is run by TPA to audit the proof from Cloud Server.

"Enabling Public Vefiraibility and Data Dynamics for Storage Security in Cloud Computing (2009)" describes that "Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for seamless integration of these two salient features in our protocol design.

Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing

This paper proposed some services for data security and access control when users outsource sensitive data for sharing on cloud servers. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and on the other hand allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents. This scheme enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. This goal can be achieved by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption [4].

3. PROBLEM STATEMENT

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten.

3.1 User:

User, who have data to be stored in the cloud and rely on the cloud for data computation, consists of both individual consumer and organization and want access to cloud server for doing job with effect of Security blanket algorithm

3.2 Cloud service provider (CSP):

Cloud service providers offer cloud solutions, like Google Apps, that are delivered electronically over the internet. Unlike a managed service provider, cloud service providers do not sell or install hardware – everything they offer is stored online and accessible securely from anywhere. There are many advantages to working with a cloud service provider like Cloud Sherpas when switching from your old email and collaboration software.

3.3 Authentication Service AS:

An authentication service that knows the password of all users and stores these in a centralized database in addition, the AS shares a unique secret key with each server.

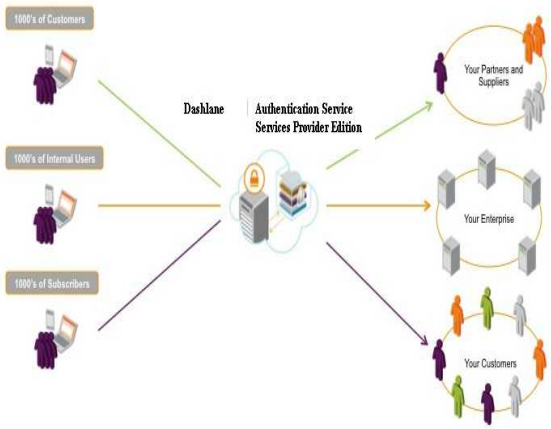


Figure 1: Authentication using Security blanket algorithm

4. PROPOSED METHOD

Security blanket algorithm is a new password manager that can best be described as a mix of Roboform and LastPass. With Security blanket algorithm users have the ability to securely store their logins. These logins can then be kept locally on your computer only or synced with your Security blanket algorithm account and accessible on any computer or device that you install Security blanket algorithm on. Currently Windows, Mac OS X, Android, and iOS are supported by Security blanket algorithm so with the sync feature you could potentially have your logins on every computer or device you use.

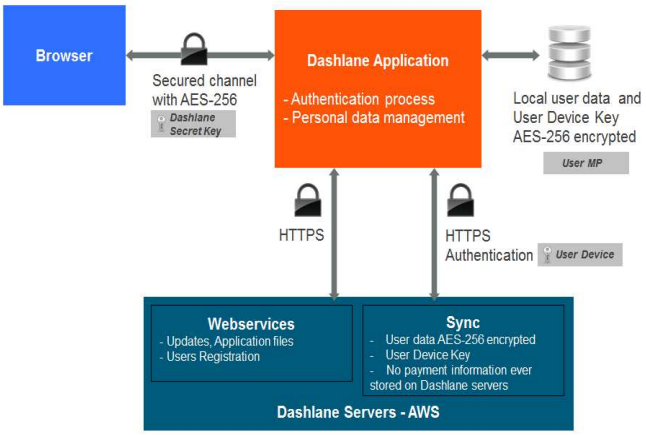


Figure 2: Security blanket algorithm Server-AWS

All communications between the Security blanket algorithm application and the Security blanket algorithm servers are secured with HTTPS. HTTPS connections on the client side are performed using OpenSSL.

The HTTPS communications between Security blanket algorithm application and Security blanket algorithm's servers are using SSLv3, TLS_RSA_WITH_AES_256_CBC_SHA connections.

SSL protocol main steps are as follows:

- The client and the server negotiate to choose the best cipher and hash algorithm available on both sides.
- The server sends his digital certificate.
- The client verifies the certificate by contacting a Certificate Authority.
- The client encrypts a random number with the server's public key, and sends it to the server.
- The server decrypts this number, and both sides use this number to generate a symmetric key, used to encrypt and decrypt data.

Finally, communication between the Security blanket algorithm Browser Plug-in and the Security blanket algorithm Application is secured using with AES 256 with the OpenSSL library:

- A 32 bytes salt is generated using the OpenSSL RAND_bytes function (ciphering) or reading it from the inter process message (deciphering) The Security blanket algorithm Private Key is used, with the salt, to generate the AES 256 bit key that will be used for (de)ciphering. This generation is performed using the OpenSSL EVP_BytesToKey, using SHA1, with 5 iterations.
- The 32 bytes initialization vector is generated with the OpenSSL EVP_BytesToKey function, using SHA1 .
- Then, the data is (de)ciphered using CBC mode.
- When ciphering, the salt is written on inter process message.

5. IMPLEMENTATION

- Allows users to store unlimited logins (usernames and passwords).
- Logins can be sorted into specific categories, e.g. email or social media.
- Has excellent browser integration — supports Firefox, Chrome, and Internet Explorer.
- In addition to logins, users can store credit card numbers, bank accounts, contacts, social security numbers, tax ids, and more.
- UPDATE: It looks like notes are only available in Premium (paid version) now.

- Has an optional built-in receipt tracker to help you keep track of your purchases, online or offline.
- Has a built-in tool that tells you how strong your passwords are.
- Can generate random passwords.
- Secures data with AES 256 encryption.

Has the ability to sync data across Security blanket algorithm on all computers and devices — Windows, Mac OS X, Android, and iOS

- Sync is optional — users can opt to keep data stored locally only.
- Has the ability to import data from LastPass, Roboform, KeePass, Password Wallet, 1Password, Chrome, Firefox, and Internet Explorer.

Has a web version for access to your logins when at a computer which doesn't have Security blanket algorithm installed.

6. RESULT AND EVOLUTION

The initial registration for a user follows the flow described

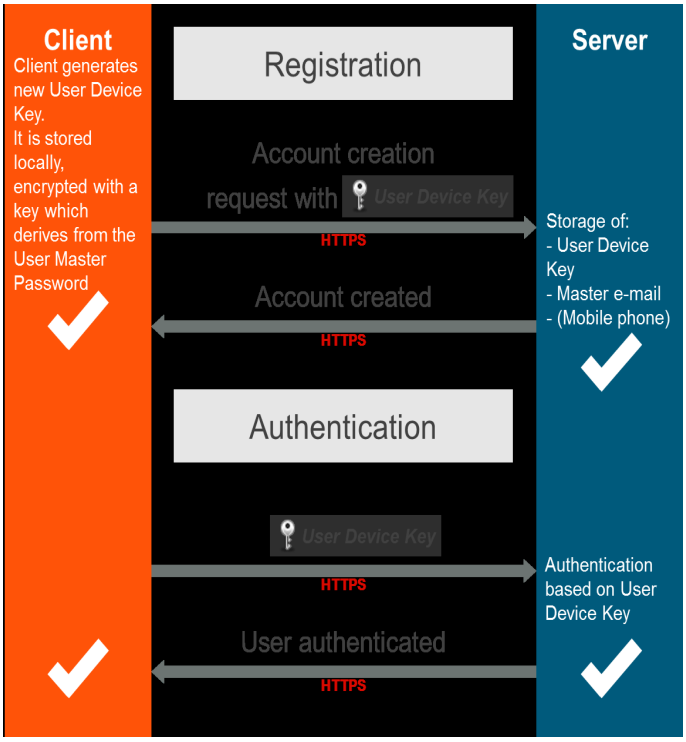


Figure 3: Authentication flow during registration.

As can be seen in Figure 3, the User Master Password is never user to perform Server Authentication, and the only keys stored on our servers are the User Device keys.

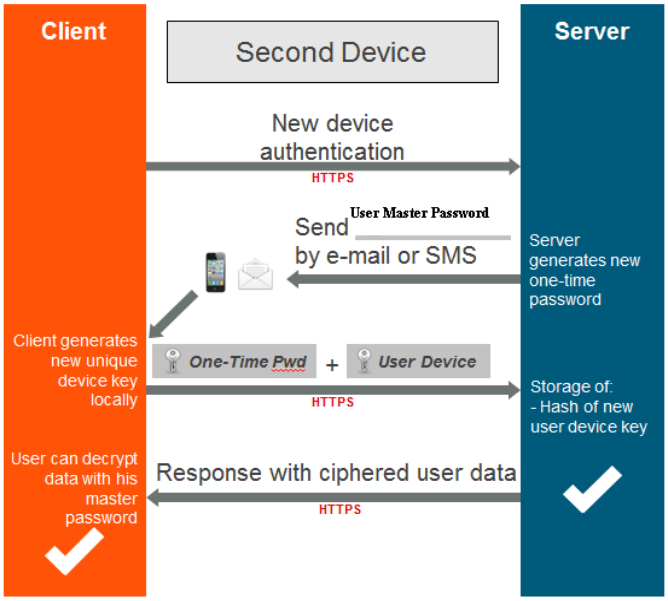


Figure 4: Two-Factor authentication

When adding a second device, the important point is that Security blanket algorithm needs to make sure the user adding the additional device is indeed the legitimate owner of the account. This is to gain additional protection in the event the user Master Password has been compromised and an attacker who does not have access to his already enabled device is trying to access the account from another device.
As shown on Figure 4, when a user is attempting to connect to a Security blanket algorithm account on a device that has not yet been authorized for this account, Security blanket algorithm generates a One-Time Password (a Token) that is being sent to the user either to the email address used to create the Security blanket algorithm account initially, or by text message to the user's mobile phone if the user has chosen to provide his mobile phone number.

In order to enable the new device, the user has to enter both his User Master Password and the Token. Only after this Two-Factor authentication has been performed will Security blanket algorithm servers start synchronizing the user data on the new device. All communication is handled with HTTPS and the user data only travels in AES-256 encrypted form. Please note again that the user Master Password never transits on the Internet.

Even though what goes on in the background during the initial registration steps is complex (See Figure 3) and highly secure, the perception by the user could not be simpler. All he has to do is to pick a (strong) User Master Password. All the other keys are generated by the application without user intervention.

When adding an additional device, the process is equally simple, while remaining highly secure through the use of Two-Factor authentication described in Figure 4.

CONCLUSIONS

Sensitive data storage on cloud platform is challenging while adopting cloud services for data storage. Cryptographic keys are sensitive data and required on cloud platform in different cases but cannot store directly on cloud. This paper discuses Security blanket algorithm key management on cloud based environment. Security blanket algorithm is a new service that does that, audits those passwords for strength, saves your form information for quick entry on new web sites, and even keeps track of the purchases you make with that information so you can see it all in one view—one that's only available to you, not even Security blanket algorithm employees.

REFERENCES

[1]. A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS '07, pp. 584–597, 2007

[2]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. of SecureComm '08, pp. 1–10, 2008.

[3]. Wang, Sherman, Kui, Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", INFOCOM, 2010 Proceedings IEEE, 14-19March, 2010.

[4]. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.

[5] L. Chen, Gongde Guo "An Efficient Remote Data Possession Checking in Cloud Storage", Fujian Normal University, vol. 5, no. 4, April 2011.

[6] Sheng Zhong and Zhuo Hao. "A Privacy-Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability," IEEE Internet Computing, 2010.

[7] Cong Wang, Kui Ren, Qian Wang and Wenjing Lou "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, vol 5, no. 3, pp 220-232, 2011.

BIOGRAPHIES

Post Graduate student Department of MCA, Acharya Institute of Technology, Karnataka, India,

Assistant Professor, Department of MCA, Acharya Institute of Technology, Karnataka, India. Teaching Experience: 9 year