Research Paper | Computer Science | E-ISSN : 2454-9916 | Volume : 2 | Issue : 1 | Jan 2016

SECURITY IN BANKING SECTOR USING CLOUD COMPUTING WITH TPA

Akanksha Pawar | Sarabjeet Kaur Popli | Priyanka Rawat | Prajakta Salke
Bharati Vidyapeeths College of Engg. For Women

ABSTRACT

Cloud is a growing trend now a days. It is used in almost all growing sectors. It also finds its application in banking sector. Clouds In banking sector is used to store the account information of the bank customers. Using clouds puts the security of the data in a fix. Data integrity is not guaranteed. Online transactions are not yet safe to be done. We propose a system that contains Clouds and public auditing scheme which provides data integrity check by a Third Party auditor (TPA). The TPA is enabled to perform audits for multiple user simultaneously. Along with the alpha numeric passwords we enable the user to set an image password which uses visual cryptography as its underlying mechanism. K-N sharing algorithm is use in this. This effectively increases the security by reducing the risk password hacking. Our system also provides an additional feature of de-duplication in order to avoid duplications of files stored at the main server. This saves the memory usage as well as the bandwidth. Thus our system includes the features of cloud computing with public auditing using TPA, Visual Cryptography, and de-duplication.

KEYWORDS: Cloud computing, De-duplication, Digital Signature, Public Auditing, TPA, Visual Cryptography.

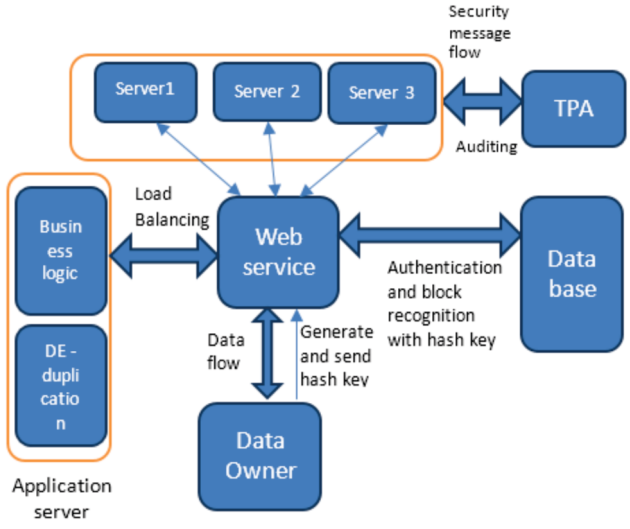
Introduction:
Online banking is a growing trend and along with it the online frauds are also growing. Keeping in mind this growing social problem we have done the survey and found that in today's banking sector user is provided only with alphanumeric passwords in order to secure their accounts. There is no de-duplication check done at the administrator level to save the bandwidth and memory. So in order to enhance the existing systems security and efficiency we propose a system that will provide image passwords along with alphanumeric passwords .whenever the user wants to login into the account he/she needs to enter both the passwords right. After logging in a message will be sent to the user's mail id that he is login into his bank account. We introduce a TPA that does public auditing of the account by maintaining digital signatures of the account data. Any change I the account changes the digital signature evaluated by TPA and then it notifies the user by sending a message on user's mail id that so and so changes are made to your account. An additional feature is added to the administrator field of de-duplication. Here whenever the admin updates any document related to the user to the bank database the document is checked for its existence in the bank database. If it is already present then it is not updated or stored again.

Materials and methods:
K-N sharing:
For including visual passwords i.e. images we are using K-N sharing algorithm. In this Shamir's Secret Sharing algorithm a secret i.e. an image in our case is divided into 4 parts. Out of these 4 parts 3 are present with the users and 1 share is with the system server. When the authenticated user provides the 3 shares in the order which they are required the system provides the 6^{th} share, and in this way the password is completed.

RSA:
RSA is an algorithm used for encrypting the users account data and store it on different clouds. It is an asymmetric algorithm that uses public and private key for encryption and decryption of data. The data is encrypted using the public key of the receiver of the data and then the receiver using its own private key decrypts the encrypted message.

Md5:
MD5 is a message digest algorithm. It is an algorithm producing a 128-bit hash value using cryptographic hash function. This hash value is represented as a 32 digit hexadecimal number in text format.

Design Architecture:



Discussion:
The data owner is the user or the account holder or the administrator that logins into the system of the bank using the web service. Web service is the method for communication between two electronic devices. Application server has 2 modules Business logic and de-duplication checking modules. Business logic is used as a part of program to encode the real world business rules that determines how the data can be created, displayed, stored and changed. De-duplication module is a module created to store only a single copy of each file regardless of how many clients asked to store that file. Thus the disk space of cloud servers as well as network bandwidth are saved. Here the servers compute the cloud. TPA is the

privacy preserving public auditing module used to evaluate the integrity of the data by checking the digital signature calculated each time the account is logged out. Database is used to store the data. Web service and load balancing modules are responsible for load balancing of the data on the cloud. The data is encrypted and divided in order to store on the cloud. This job is done by web services.

Conclusion:

Aiming at achieving data integrity and security in online transactions we have introduced a Third Party Auditor who provides privacy preserving public auditing by maintaing the original digital signature of the data and then comparing it with the temporary signature audited each time a user logs out his account in order to verify whether the user is authenticated or not. We also introduce image passwords along with alpha numeric passwords to enhance the password security. De- duplication ensures the memory and bandwidth usage wisely. Hence by introducing this system we make the current banking system more reliable , secure and safe to use.

REFERENCES:

1. Cong Wong, Sherman S.-M. Chow ,Qian Wang, Kui Ren (2013) : Privacy-Preserving Public Auditing for Secure Cloud Storage , IEEE.
2. J. Yaun and S. Yu (2013): Secure And Constant Cost Public Cloud StorageAuditing With De-duplication, IEEE Conference on Communication and Network Security.
3. S.Halevi, D. Harnik, B. Pinkas and A. Shulman (2011): Proofs of ownership in remote storage system, ACM .
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring (2007): Provable Data Posession at Untrusted Stores, ACM, New York.
5. H. Wang (2013):Proxy Provable data possession in public clouds, IEEE Transactions on Services Computing.
6. Q. Wang , C. wang, J. Li, K. Ren (2009):Enabling Public Verifi ability and Data Dynamics For Storage Security in Cloud Computing, ESORICS.
7. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom (2012):Cloud Computing Security:From Single To Multi-Clouds , !EEE, Melbourne.
8. M.A. AlZain and E. Pardede(2011): Using Multi Shares for Ensuring Privacy in Databases-as-a-Service, Hawaii Intl. Conf on System Sciences.
9. K. Birman, G. Chockler and R. Van Renesse (2009): Toward A Cloud Computing Research Ageda , SIGACT news
10. C.Cachin, I. Keidar and A. Shraer(2009): Trusting The Cloud, ACM SIGACT news.
11. G.Chockler, R. Guerraoui, I. Keidar and M. Vukolic (2009): Reliable Distributed Storage Computer 42.
12. Clavister (2008): Security in Cloud, White paper.
13. S.I. Garfinkel (2003):Email Based Identification and Authentication:An Alternative to PKI?, IEEE.
14. Jingwei Li, Jin Li, Dongqing Xie and Zhang C (2015): Secure Auditimg and Deduplicating Data in Cloud, IEEE
15. M. Armbrust, A. Fox, R.Griffith, A.D. Joseph, R. Kartz, A. Rabkin, M. Zaharia (2010): A View of Cloud computing.
16. S. Keelveedhi, M. Bellare and T. Ristenpart(2013): Dupless: Server aided encryption for deduplicated storage, USINEX, Washington.
17. H. Sharcham and B. Waters(2008): Compact Proofs of Retrievability, ASIACRYPT , Berlin
18. Guided by: Prof.Jayashree Jadhav