# Security in Banking Sector using Cloud Computing with TPA.

Akanksha Pawar, Sarabjeet Kaur, Priyanka Rawat, Prajakta Salke, Prof. Jayashree Jadhav
*Bharati Vidhyapeeth's College Of Engineering for Women.*

***Abstract-*** **The world is stepping its foot towards becoming digital. Everything has an online solution. Each sector be it shopping, education or banking is getting an online solution for itself. This online solution brings along with it many problems like breach of security, frauds, etc. We propose a system for the banking sector in which we secure the login to the bank account using image passwords along with the alphanumeric passwords. The alphanumeric username and the password would also be provided by our system which would be random number. This would be impossible to be cracked. After logging in the system user can perform transactions only when he correctly enters the OTP (one time password) which he receives on his registered mobile number. This OTP is also a random number which is impossible to be guessed. In this way only the authenticated user will be able to perform the transaction. The OTP module and the image password module is handled by a TPA (Third Party Auditor). It checks for the correct image shares inserted by the user at the time of login and correct OTP entered by the user at the time of performing transaction. Our system would be deployed on cloud for its working as the banks use clouds.**

## I. 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 and before performing transactions a message will be sent to the user's registered mobile number that contains an OTP (one time password) that he has to enter for the transaction to happen. We introduce a TPA that does public auditing of the account by maintaining digital signatures of the account data. The OTP and the share of images generated for the image passwords is done by the Third Party Auditor. The Third Party Auditor does the authentication of the images and the OTP in order to recognize the legitimate user and disable the frauds.

## II. MATERIALS AND METHODS

**K-N sharing:**

It is also known as Shamir's secret sharing algorithm. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret**.** 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 4th share, and in this way the password is completed.

The goal is to divide secret S into n pieces of data. (S1,….,Sn) in such a way that :

1. Knowledge of any k or more Si pieces makes S easily computable.
2. Knowledge of any k-1 or fewer Si pieces leaves S completely undetermined.

This scheme is called (k,n) threshold scheme.

If k=n then all participants are required to reconstruct the secret.

**AES:**

AES is advanced encryption algorithm. It is current standard for secret key encryption. The algorithm uses a combination of Exclusive OR operation (XOR), octet substitution with an S-box, row and column rotation, and a MixColumn.

Steps:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plain text).
3. Add the initial round key to the starting state array.
4. Perform 9 rounds of state manipulation.
5. Perform the $10^{th}$ and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

**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. MD5 processes a variable length message into fixed length output of 128 bits.

The man MD5 algorithm operates on a 128 bit state, divided into four 32 bit words, denoted A,B,C and These are initialized to certain fixed constants. The main algorithm ten uses each 512 bit message block inturn to modify the state. The processing of a message block consist of four similar stages, termed rounds: Each round is composed of 16 similar operations based on a non linear function F, modular addition and left rotation. There are four possible functions F: a different one is used in each round.

F(B,C,D)=(B∧C)v(¬B∧D)
G(B,C,D)=(B∧D)v(C∧¬D)
H(B,C,D)=B XOR C XOR D
I(B,C,D)=C XOR (Bv¬D)

**Math Random Function:**

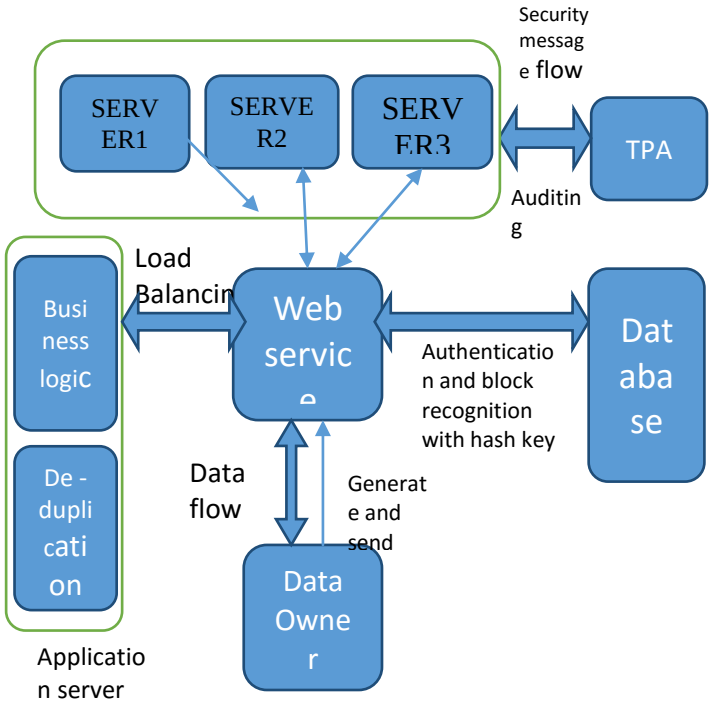
Math.random generates a number between 0 and 1 i.e. not a whole number, and also it is not 1.To get a number , for example between 0 and 10 ,multiply your answer by 10:

Math.random() *10

To get it to a whole number,i.e. an integer,apply Math.floor, which rounds down to the nearest whole number:

Math.floor(Math.random*10+1)

## III. DESIGN ARCHITECTURE




## IV. 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.

## V. INTEGRATION AND WORKING OF THE MODULES

The user firstly registers or opens his account in the bank. Here he needs to provide his correct email id, mobile number, his id proof, pan card and adhaar card scanned images. The admin then checks the uploaded documents of the user and if these documents are valid the admin then approves the user. The approval message is sent to the user on his mail id. The uploaded images are encrypted and splitted in 4 parts each using K-N sharing algorithm for splitting and md5 algorithm along with AES for encrypting. The id proofs encrypted parts are used as the image password for which 3 parts of the image are sent to the users registered mail id along with the alphanumeric username and password after the admin approves the account. 1 share out of the 4 is on the banks server. When the user provides 3 shares of the password in correct order along with the correct alphanumeric password the fourth share is provided by the server inorder to complete the image and the user logs in the account successfully. The task of validating the shares of the image password provided by the user at the time of login with the stored shares is done by the TPA. Now after login is done by the user he can check his account details or perform transactions. The statement of the transactions can also be seen by the user. For performing the transaction user needs to enter the recipients account number. Then the recipients details would be seen by the the user. The user then has to enter the amount to be transferred. Following this the user will be sent with an OTP on his registered mobile number. He has to enter the right OTP to continue the transaction. Once the right OTP is entered the transaction is done successfully. The user can then log out.

## VI. DEPLOYMENT OF PROJECT ON THE CLOUD

This system is deployed on the cloud of Amazon using the AWS service. AWS is Amazon Web Service. Using the " RDB" that is the relational database service the database data is deployed on the cloud . Using "SES" the Send Email Service the email ids of the customers are verified and using the "Elastic Bean Stalk" service the code is deployed.

## VII. 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 maintain 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 Verifiability 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] Q. Wang, C. Wang, J li, K. Ren(2009) : Enabling public verifiability and data dynamics for storage security in cloud computing, ESORICS
[18] R. Di Pietro and A. Sorniottio(2012) : Boosting efficiency and security in proof of ownership for deduplication, ACM Symposium on Information.
[19] W. K. Ng, Y. Wen and H. Zhu(2012) : Private Data deduplecation Protocols in cloud storage, ACM Symposium on Allied Computing, USA.
[20] N. Askari, H.M. Heys, C.R. Moloney (2013): An extended visual cryptography scheme without pixel expansion for halfton images, IEEE Canadian Conference Of Electrical and Computer Engineering.