Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Managing Password Authentication Scheme for Secure Cloud Storage

Swathi .U
Student, M.Tech CSE Dept,
Institute of Aeronautical Engg.,
Hyderabad, Andhra Pradesh, India

Chandra Sekhar Reddy .N
Professor, CSE Dept.,
Institute of Aeronautical Engg.,
Hyderabad, Andhra Pradesh, India

Satish Babu
Asst.Professor, CSE Dept.,
Institute of Aeronautical Engg.,
Hyderabad, Andhra Pradesh, India

Abstract: Cloud computing is the future of the next generation architecture of IT solutions. Cloud provides computing resources on subscription basis over the internet. The Cloud data storage network includes a Third Party Auditor which has the power and capabilities that a client does not have. It is a trusted entity that has the access to, other than cloud and check on the exposed risk involved in cloud storage data on behalf of the client. In this paper, the problem of data security and integrity has been presented. Also, a scheme to provide maximum data integrity. In proposed scheme, existing fully homomorphic encryption is integrated with TPA auditing system is proposed. This scheme can audit data integrity without decrypting it.

In cloud computing we can share our data and application at common place. This uses internet and share resources to provide services. Security is important issue because cloud having many benefits so, it have many users. This paper focuses towards security to cloud. It is based on distributed storage on 3 machines. It uses homomorphic token for checking integrity of data. This helps user low cost communication and computational cost. The auditing result ensures strong cloud storage correctness as well as simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. It allows client to perform secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append [1]. Data privacy is one of the biggest challenges in Cloud Computing. By the introduction of the OTP password protection schemes, the privacy of the user will now be assured to a great extent. The OTP provides a user new password each time.

Keywords: Cloud Computing, Security constraints, data storage,onetime password,privacy preserving.

I. INTRODUCTION

Cloud is the category of parallel and distributed computing. It is the collection of interconnected and dynamical virtualized system. Many number of cloud service providers are available in market. Those service providers are Amazon [4], IBM and HP. Different number of consumers are access the different number of clouds services. This paper concerned with Software as a service. Previous cloud data storage security solutions identified with the help of technical environment. That is called application logic. It controls the less number of attackers. New different weak spots are available. In those weak spots attackers it may chance to enter and create the risks and problems. It’s not possible to control the all dimensions of attackers [2][3].

Some more number of security properties we add in technical solution environment and increases the detection of attacker’s in cloud data storage areas. Newly we add the one time password authentication procedures for increasing the security.

II. RELATED WORK

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows end-users to use applications such as data storage, email, word-processing, spreadsheets, collaboration, file conversation, social media, etc. without installing on their personal computers and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing various resources such as storage, memory, processing and bandwidth. CLOUD computing has been envisioned as the next generation information technology(IT)architecture for enterprises,due to its long list of unprecedented advantages in the IT history:on-demand self-service,ubiquitous network access ,location independent resource pooling, rapid resource elasticity ,usage-based pricing and transference of risk[2]. While cloud computing make s thes e advantages more appealing than ever, it also brings new and challenging security threats toward users ’ou t sourced data. Since cloud service providers(CSP) are separate administrative entities, data out sourcing is a ctually relinquishing user’s ultimate control over the fat e of their data. As a result,the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful an dreliable than personal computing devices ,they are still facing the broad range of both internal and external threats for data integrity.

For examples,CSP might reclaim storage for monetary reasons by discarding data that have not been or are rarely accessed,or even hide data loss incidents to maintain a reputation.In short, although out sourcing data to the cloud is economically attractiveforlong-termlarge-scale storage,it does not immediately offer any guarantee on data integrity and availability. This problem,if not properly addressed,may impede the success of cloud architecture. As users no longer physically possess the storage of their data ,traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted.In particular,simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost a cross the network. Besides, it is often in sufficient to detect thedata corruption only when a ccessing the data,a sit does not give users correctness assurance for those un accessed data and might be too late to recover the data loss or damage. To fully ensure the data integrity and save the cloud users' computation resources as well as online burden,it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third-party auditor(TPA) to audit the out sourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on be half of the users, which provides a much more easier and affordable way for the users. To ensure their storage correctness in the cloud.using encryption does not completely solve the problem of protecting dataprivacy against third-party auditing but just reduces it to the complex key management domain. Unauthorized data leakage still remains possible due to the potential exposure of decryption keys. Therefore,how to enable a privacy-preserving thirdparty auditing protocol,independent to data encryption,is the problem we are going to tackle in this paper. Toaddress these problems,our work utilizes the technique of publickey-based homomorphic tokens and password authentication.which enables TPA to perform the auditing with out demanding the local copy of data and thus drastically reduces the communication and computation over head as compared to the straight forward data auditing approaches.

III. PROBLEM STATEMENT

The data integrity threats to ward users' data can come from both internal and external attacks at CS. These may include: software bugs, hardware failures, bugs in the network path,economically motivated hackers, malicious or accidental management errors, etc. Besides, CS can be self-interested.For their own benefits, such as to maintain reputation, CS might even decide to hide these data corruption incidents to users. Using third-party auditing service provides a cost-effective method for users to gain trust in cloud.We assume the TPA,who is in the business so auditing,is reliable and independent.However, it may harm the user if the TPA could learn the out sourced data after the audit.

Note that in our model, beyond users' reluctance to leak data to TPA, we also assume that cloud server has no incentives to reveal their hosted data to external parties.On the one hand, there are regulations,e.g.,HIPA A requesting CS to maintain users'data privacy. On the other hand, as users' data be long to their business as set. there also exist financial incentives for CS to protect it from any external parties.There fore,we assume that neither CS nor TPA has motivations to collude with each othe r during the auditing process. In other words, neither entities will deviate from the prescribed protocol execution .

IV. THE PROPOSED SCHEMES

This section presents our public auditing scheme which provides a complete out sourcing solution of data—not only the data it self,but also its integrity checking.After introducing one time pass words, A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work.

A. How OTPs are generated and distributed

OTP generation algorithms typically make use of pseudorandomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)

Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).

Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging. Finally, in some systems, OTPs are printed on paper that the user is required to carry.

V. PERFORMANCE EVOLUTION GRAPH

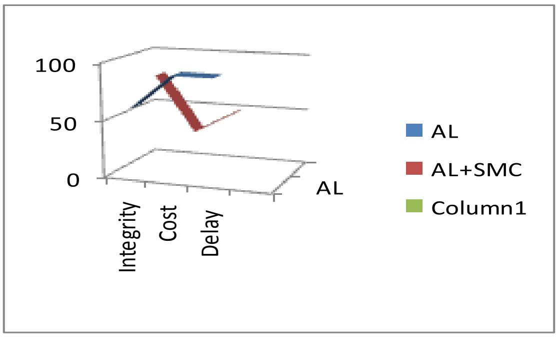

Fig.1 Using password authentication provide the data integrity and low cost.

Algorithm

A. *User Authentication*
B. Step 1: The user inputs login credentials to the HRM System.
C. Step 2: Apply symmetric key-based security
D. Step 3: Provide One-Time Password.
E. Step 4: Check for client information request.
F. Step 5: Execute Data Retrieval Program.
G. Step 6: Check for data needs to be saved.
H. Step 7: Execute Data Storage Program.
I. *B. User Data Request*
J. Step 1: Check user's login successfully verified.
K. Step 2: Sends request for information to the Storage Service System.
L. Step 3: HRM Service System transmits the user ID to the Storage Service System.
M. Step 4: Searches for the user's data.
N. Step 5: Send request to the Encryption/Decryption Service System along with the user ID

VI. CONCLUSION

Data privacy is one of the biggest challenges in Cloud Computing. By the introduction of the OTP password protection schemes, the privacy of the user will now be assured to a great extent. The OTP provides a user new password each time.

VII. FUTURE WORK

In future, this proposed model could be used to get the secure cloud computing environment which would be a great enhancement in the privacy preservation.

REFERENCES

[1] Wang, B.; Baochun; Wang, H. L. 2012 Oruta: Privacy- Preserving Public Auditing for Shared Data in the Cloud, IEEE Fifth International Conference on Cloud Computing, 2012 IEEE, DOI 10.1109/CLOUD.2012.46.

[2] Syed, M. R.; and F, Mohammad; "PccP: A Model for Preserving Cloud Computing Privacy", 2012 International Conference on Data Science & Engineering (ICDSE), 2012 IEEE.

[3] http://en.wikipedia.org/wiki/One-time_password.

[4] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, Jesus Molina ,Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control, 2009

[5] Hassan Takabi and James B.D.Joshi, Gail-JoonAhn Security and Privacy Challenges in loud Computing Environments, 2010

[6] R.C.Merkle,"ProtocolsforPublicKeyCryptosystems,"Proc.IEEESymp.SecurityandPrivacy,1980.

[7] G.Ateniese,S.Kamara,andJ.Katz,"ProofsofStoragefrom Homomorphic Identification Protocols,"Proc.15thInt'lConf. Theory and Application of Cryptology and Information Security: Advancesin Cryptology(ASIACRYPT),pp.319-333,2009. [26]M.BellareandG.Neven,"Multi-Signatures in the Plain Public Key Model and a General Forking Lemma, "Proc.ACMConf. ComputerandComm.Security(CCS),pp.390-399,2006.

[8] Amazon.com,"AmazonElasticComputeCloud,"http://aws. amazon.com/ec2/,2009. [8]Y.Zhu,H.Wang,Z.Hu,G.-J.Ahn,H.Hu,andS.Yau,"Efficient Provable Data Possession for Hybrid Clouds,"CryptologyePrint Archive,Report2010/234,2010