International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP345-348

SECURE FILE ACCESS USING MD5 FOR ONE TIME PASSWORD GENERATION ON CLOUD

Ankita Patil[1], Kiran Zambare[2], Preeti Yadav[3], Pankaj Wasulkar[4]
Nisha Kimmatkar[5]
Computer Department, Savitribai Phule Pune University,
JSPM's Rajarshi Shahu College of Engineering, Tathawade,Pune.

Abstract :- Cloud computing is emerging technology which offer better performance and can be use to provide types of services such as Software as a Service (SAAS), Platform as a Service (PAAS) and Infrastructure as a Service (IAAS) at low cost. The issue in providing SAAS is security of cloud user's data when it is uploaded on cloud and authentication of cloud user before accessing the data. To improve the security for the data retrieval from cloud environment, the client user has to use the One Time Password (OTP) provided by the cloud environment and provides data encryption which protects data from cloud vendor, an attacker. In this paper we are providing the OTP using MD5 and the encryption is done by using RSA. The One Time Password is sent to the user phone number to view the original data and help to share public data with other authenticated cloud user.

Keywords :- Authentication, Cloud Computing, MD5, One Time Password, RSA.

I. INTRODUCTION

Cloud computing is one of the latest developments in the IT industry also known as on-demand computing. This technology is grouped into sections which include SAAS, IAAS and PAAS. Now days Cloud computing makes everything flexible and easier but there is another aspect that is what about security? Data security over the Cloud also a major concern and various methodologies are proposed, considering the customer point of view, we have made an extensive research to obtain what are the main security problems in Cloud computing security. In proposed security model Cloud computing providing services in layered medium, so there must be some SLA (Service Level Agreement) or service management, must be applied over the layers, which eventually increase the confidence of the user. This new technology improves the Cloud security based on two phases. Cloud computing technology is used worldwide to improve the business infrastructure and performance. However, to utilize these services by intended customer, security of cloud user's data when it is uploaded on cloud and authentication of cloud user before accessing the data.

In this paper we want to develop the security system that will provide security to the cloud and will be very fruitful for both the client user and also the cloud data owner, that we can perform trusted computing. To improve the security for the data retrieval from cloud environment, the One Time Password is used using MD5 and provides data encryption which protects data from cloud vendor, an attacker. The One Time Password is sent to the user phone number to view the original data and help to share public data with other authenticated cloud user.

We provide here an overview of cloud computing. The rest of this paper is arranged as follows: Section 2 introducing cloud computing security; Section 3 describes about proposed approach; Section 4 describes Conclusion and future work;

II. SECURITY OF CLOUD COMPUTING

All the possible threats of the cloud computing are discussed in this section. All the security of the cloud environment depends on the security provided by the cloud service provider. Cloud providers control the hardware and the hypervisors that stores the data and applications are run. Cloud Service provider security must be top-of-the-line.

First on the list are data breaches. If a multitenant cloud service database isn't designed properly, a single flaw in one client's application could allow an attacker to get at not just that client's data, but every other clients data as well. The challenge in addressing these threats of data loss and data leakage. The second-greatest threat in a cloud computing environment, according to CSA, is data loss. A malicious hacker might delete a target's data. Compounding the challenge, encrypting one's data to ward off theft can backfire if one lose the encryption key. Data loss isn't only problematic in terms of impacting relationships with customers, the report notes. The third-greatest cloud computing security risk is account or service traffic hijacking. If an attacker gains access to your credentials, he or she can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Fourth on the list of threats are insecure interfaces and APIs. IT admins rely on interfaces for cloud provisioning, management, orchestration, and monitoring. APIs are integral to security and availability of general cloud services. From there, organizations and third parties are known to build on these interfaces, injecting add-on services. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency. Denial of service ranks as the fifth-greatest security threat to cloud computing. DoS has been an Internet threat for years, but it becomes more problematic in the age of cloud computing when organizations are dependent on the 24/7 availability of one or more services. DoS outages can cost service providers customers and prove pricey to customers who are billed based on compute cycles and disk space consumed. No. 6 on the list is malicious insiders, which can be a current or former employee, a contractor, or a business partner who gains access to a network, system, or data for malicious purposes. In an improperly designed cloud scenario, a malicious insider can wreak even greater havoc. From IaaS to PaaS to SaaS, the malicious insider has increasing levels of access to more critical systems and eventually to data. Seventh on the list is cloud abuse, such as a bad guy using a cloud service to break an encryption key too difficult to crack on a standard computer. Eight on the list of top security threats to cloud computing is insufficient due diligence; that is, organizations embrace the cloud without fully understanding the cloud environment and associated risks. Last but not least, CSA has pegged shared technology vulnerabilities as the ninth-largest security threat to cloud computing. Cloud service providers share infrastructure, platforms, and applications to deliver their services in a scalable way.

In this paper we mainly concentrate on Secure File Access on cloud. We are mainly concentrating on four problem domain: Insecure API and Interfaces, Malicious Insiders, Data Sharing, Data Loss.

III. PROPOSED SYSTEM

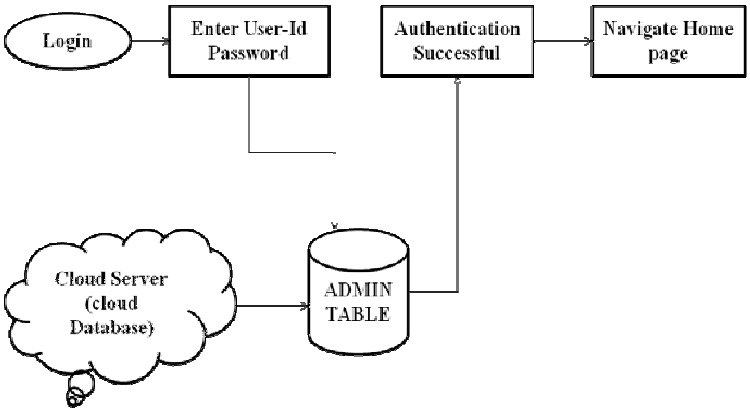

Fig 1: Authentication Of the User

In this paper security can achieve bi-directional as we propose a secure cloud framework. In our proposed approach there is security in the cloud side and also the client data is safe. For this we proposed architecture, using this architecture we can provide security to the cloud environment and to the user. Any normal user can register their detail in this environment and according to the detail, Admin of the cloud provide a user-id and password. After the registration the user has to login and his Authentication is checked by the cloud on basis of his details stored as shown in Figure 1. Only if the user is found Authenticated then and then only he is provided the facilities such as file access, delete and search.

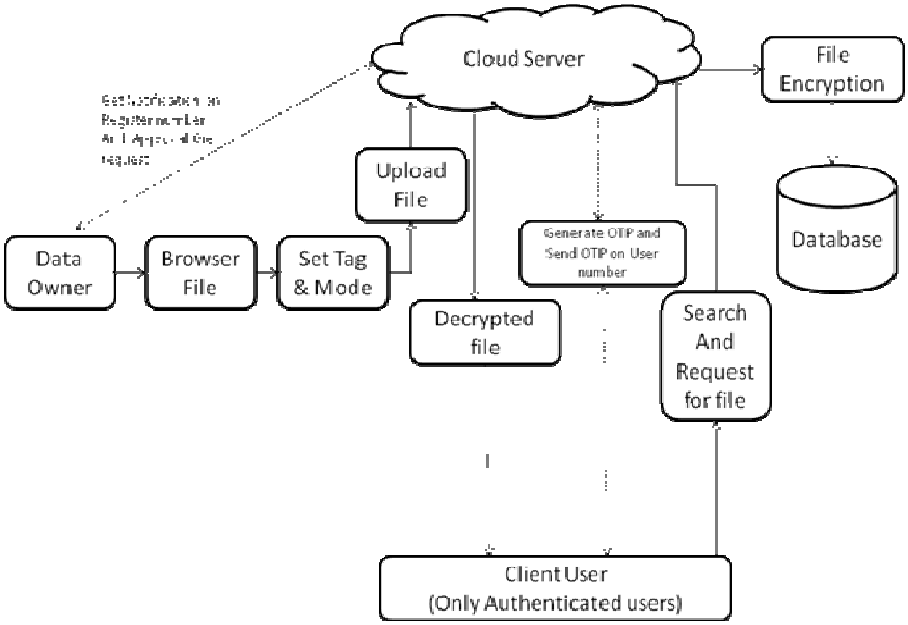

Fig 2: Proposed System

The architecture proposed by us is as shown in the Figure 2 above. In this architecture two entities are considered and both shall have the web browser in their respective laptops or pc's.

In the initial stage the Data owner uploads the file in text or document form and he then sets the tag to the file which make easy for searching the file. These uploaded Files are then encrypted by the Application on

the cloud server using the RSA algorithm and these encrypted file can be accessed by the users only if permission is granted by the data owner.

When the users want to access these files then, client users has to first log into the system. He shall be authenticated by the server if he is a regular user or he shall have to register himself with the application. Client user also needs to sign in into the system. Users can now search the required file by the file name and the tag.

After searching the file, client user has to request for accessing file from the cloud. This request is forwarded by the cloud to the data owner. Data owner get notification on register mobile number. The data owner can approve or deny the request. If the request is accepted then, the OTP is generated and sent to client user on registered mobile number. This one time password is generated using MD5 algorithm and this OTP is valid for only specific time period. Only on entering this OTP client user get access to requested file. After accessing file, the access rights of that user for that file are taken away.

IV. CONCLUSION

In this paper we proposed an efficient framework to provide File storing and sharing in the cloud environment with OTP. We present a secure architecture in which we can enter in two ways, first by computing and second by owner task. Through the owner task environment we can enter by entering the appropriate owner password for performing the owner task. In this paper we taken two most secure algorithm for encryption, decryption and OTP.

The two security approach make our framework more secure in comparison to the previous .In today's era the demand of cloud is increasing, so the security of the cloud and the user is on the top concern. Our proposed algorithm is helpful to fulfil today's requirement. In future we can provide several comparisons with our approach with result to show the effectiveness of our proposed framework.

REFERENCES

[1] Eko Sediyono, Kartika Imam Santoso, Suhartono,"*Secure Login by Using One-time Password Authentication Based on MD5 Hash Encrypted SMS*",IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI),2013

[2] T.Venkat Narayana Rao, Vedavathi K, "*Authentication Using Mobile Phone as a Security Token"*, Hyderabad, A.P, India, IJCSET |October 2011 | Vol 1, Issue 9, 569-574

[3] M. Karthika, J. Vasuki, S. Sugashini,"*Retrieving Secure Data from Cloud Using OTP*" International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 5 (June 2014), 2349-2163

[4] Ashutosh Kumar Dubey , Animesh Kumar Dubey , Mayank Namdev, Shiv Shakti Shrivastava," *Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment*"

[5] Manreet kaur ,Monika Bharti," *Fog Computing Providing Data Security: A Review*", International Journal of Advanced Research in

[6] Gawali M. B, R. B. Wagh,S. P. Patil," *Enhancement For Data Security In Coud Computing Environment*", International Journal of Internet Computing ISSN No: 2231 – 6965, VOL- 1, ISS- 3 2012.

[7] Parsi Kalpana, Sudha Singaraju," *Data Security in Cloud Computing using RSA Algorithm*", International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.