An Illustrative Approach for Secure Key Based Authentication for Cloud Communication

Dr. Richa Purohit
Assistant Professor, MIT Arts, Commerce and Science College, Pune, India
Email: richapurohit81@gmail.com

***Abstract*- The most reasonable and affordable technology to store bulk of data either related to an individual or of related to a big organization, is cloud technology. Cloud technology provides a large scalable area where we can store our numerous data and access it from any device around the world. The paper discusses basic issues that a user or organization must be aware of before getting started with cloud services. Further, it emphasizes the possible breaches in cloud service security and their possible solution approaches for improving security. The paper discusses the solution towards increased secure communication and message passing among user-to-user or among user-to-cloud. The proposed method ensures that the user who sends data to the cloud really belongs to the organization for which the cloud is intended, or if a user receives any data from cloud than it was put there by genuine users only, that belong to the same group or organization.**

Keywords: Cloud security; hash; authentication; secret key; cloud communication

I. INTRODUCTION

The vast amount of data that companies generate and want to refer in future also, are the reason for development and need of cloud services. Cloud provides a better solution for increased demand of storage and fast anytime –anywhere access of the data. In simplest term, Cloud is a place where we can store our data/information along with lengthy applications, not on our computer machine, but on servers of cloud service providers, may be far apart from our location, through internet. The term Cloud Computing encompasses both- the Applications (as SaaS) and the H/W along with S/W that are provided by cloud service providers. The Cloud and its services are broadly categorized into two types- (1) Public Cloud: When any one can use the cloud by paying for its services, such services are utility services and (2) Private cloud: which are internal part of the organization and are not available to other outsiders [1].

VMware vCloud was the first cloud technology that provided its services and brought together the availability and prospect of advantages of cloud applications and services to organizations and users.

But this increased use of cloud technology is definitely not free from security threats. There are few issues, which the organization or individual user should take into consideration [2] such as:

- Is data available to intended users only or is it really widely available to all users around?
- Can any outsider manipulate the data residing at cloud in unauthenticated manner too?
- Are we always receiving the expected results of the operations performed?
- Was the data available all the time or was it become unavailable for some little time?
- Is data always changing as we wish them to change as per our performed procedures or are they changing abruptly without proper procedure calling from intended user?
- Are we aware of the process that service provider is using to provide us the cloud services at its end?
- Do we as user have enough control over the cloud services and their availability to various insiders and outsiders?
- Does service provider provide any mean to overcome security attacks?

Various securities related issues are briefly explained in the following section:

II. SECURITY ISSUES IN CLOUD ENVIRONMENT

Various security related issues and areas of concerns for the same are as listed below:

A. Data Breaches

As more and more companies moving to cloud computing, with their huge amount of data, the intruders are now available with more options to get data online for numerous types of attacks. The attack can become very severe as the data on these clouds could be very crucial for individuals, like their personal information, their bank and account related data, their property related data or for organizations also, like company's' financial

data, its client data or project details etc. This is supported by a study that was conducted by Ponemon Institute [3], stating that more than 50 percent of IT experts believe that company's are not providing as much security services for cloud, as they are needed to keep data safe from adversaries. The study further claims that the security of data on cloud is at least three times lesser than data that is not on clouds. This vulnerability of data is a serious issue.

B. Poor Authentication and Easy Attacks

A tremendous use of clouds, sometimes allows data access with poor authentication, such as weak key, easily traceable passwords, non removal of ex-employee's permissions to access organizations data and mail accounts etc. The growth of cloud usage for data storage, has given a new platform to attackers for obtaining huge confidential data with an ease. Moreover, attackers can modify and even fabricate this data over cloud to make it of their use only. Where we earlier had Man-in-the-middle attack, at the time of message passing from source to destination, now we have man-in-the-cloud attack [4] that is launched to verify individual devices of users without any requirement of actually logging-in by user.

C. Insecurity from Insiders

Usually, the security of data on cloud is in the hands of cloud service provider, who implements simple techniques such as encryption for providing security and confidentiality to its client. But, an insider, i.e. an ex-employee, a current employee, a system administrator can easily pose a threat to security by simply using his keys and forge the data. Employees' authorization can be used to access organization's critical data in an unauthorized manner either intentionally or accidentally.

D. Permanent data loss

Any malicious attack or an unavoidable accident can lead to a permanent loss of data related to the organization, from the cloud [5]. Similarly, Google also went through the same issue, when its power grid was struck by lightning four times. Furthermore, if the user is using its own private key for encryption before sending its data to cloud, then it becomes only the user's responsibility to keep its key safe, as the data will not be recoverable on loss of key or malicious change of key by attacker, if possible. This problem can be solved by not sharing the key with anyone and by keeping back of crucial data at some another physical location too.

E. Inadequate Information

Sometimes the organizations adopt cloud architecture and cloud services without getting complete knowledge of all services provided by the cloud service provider. This may also happen, when the organization itself is not clear about its goal, agendas, resources and various organizational policies. In such a case, organizations quickly move to cloud, without giving proper consideration to the specific type of requirement that can be fulfilled by a particular service provider and the type that cannot be. Few of the expectations can not even be matched with the selected service provider either. Thus, it is essential to be very much clear and firm about all the organization's requirements and at the same time, the service provider must also clearly state all the functionalities and features that it can provide to the organization, to avoid any risk later on.

F. Mishandling of Cloud services

Cloud not only provides a better mechanism to deal with and manage client's data but also a huge amount of space to store it. This feature is maltreated by many of the attackers to impose various kinds of viruses, malware and phishing. Sharing of virus infected files, pirated videos and clippings etc. can result into huge fine and also in deprecate of organization. Sometimes, customers do not get directly affected by this misuse of cloud, but their data can still result in unavailability and face integration related issues. For example, attacker can impose Denial of Service (DOS) attack and further lead to unavailability of services from cloud to designated customer or whole organization. Hence, it is the responsibility of service provider to identify such misuses and attacks.

G. Sharing of insecurity: Sharing of responsibility

Various applications, platforms, infrastructure and services are shared over the cloud including huge amount of confidential data also. A problem at any one place may result in problem at all stages as a consequence. Thus, security should be taken care of at all possible levels, from network management to privilege and key management. Both service provider and client share the responsibility of maintaining this security. Many service providers like Dropbox, Google, and Microsoft etc. have taken the charge of standardization of security procedures, but still allocating privileges and securing their own keys, is still in the hands of organization an individual user.

H. Unsafe Application Program Interfaces

The APIs can be treated as the mechanism through which users can customize their cloud services. Authentication, access rights encryption can be modified using APIs. To provide better user experience, more strong APIs are developed, but this gives rise to more chances of attacks. APIs come across as most vulnerable part of cloud and are more suitable to imply a security threat.

As we have seen various security threats towards cloud computing, the next session discusses few available solutions to these threats:

III. Security Approaches for Cloud Computing

Fundamentally, the responsibility of providing and encompassing a secure and safe cloud environment, is divided among a mixture of entities involved, such as the user, the vendor and the software/hardware providers that supply configuration and security software at various levels [6]. Security of particular running application is the duty of individual user of cloud. The physical security like implementation of firewall for the users or organizations is the task of cloud service provider. Intermediate layers of the model are the responsibility of both- the user and the service provider. Usually, user responsibility of security is taken care by another third party who is expert in providing such precise services. But the main issue here is the protection of authenticated and trusted users from each other.

There are various solutions of security for cloud computing, following are few of them:

1. Framework for Strong Authentication: A strong authentication scheme for both user-end and server-end is required which includes verification and validation of identities, and their mutual authentication, may provide security to cloud computations [7, 8]. Transfer of data to and from cloud must be authenticated using mutually exclusive, and thus secure passwords. The use of these passwords authenticates the user or server interacting with each other.

2. Framework for privacy preserving digital identity management: Digital Identities can be verified to authenticate source and destinations in cloud computation. If the concerned entities authenticate each other's identities then they recognize and acknowledge the argument passed between them as part of communication. These digital identities can include (i) digital signatures, which each authenticated party can later on verify or (ii) certain type of secret key which shared only between these two involved parties and has not been shared over net at any time in past.

3. Framework for virtualization of clouds: Each user in cloud is endowed with an occurrence of virtual machine. Cloud virtualization is the main system towards security in most of the cases. It helps in conveying defense of attacks where one user attempts to harm another user or the cloud infrastructure itself. It prevents the user code from accessing sensitive portion of cloud infrastructure, as the user always works in its dedicated virtual cloud. Similarly to prevent data theft, encryption should be accentuated at user site.

4. Involvement of a trusted third party: The use of third party that distributes public certificate to involved parties can resolve issues like repudiation and may act as notarization, in case of any dispute [9]. When the message passes through an insecure Transport layer, the signature should be imposed in the header part [10]. Timestamp used with these signatures also ensure the validity of the message transferred.

IV. Proposed Method for Secure communication over cloud

The data or message transferred over cloud can be made more secured if proper use of cryptographic keys and message digest can be forced. One possible type of attack over the cloud from insiders or from one user to another user can be replay attack or masquerading or spoofing. Further consequence of it can be denial of attack. Moreover, it is also an important issue to restrict the outsiders from modifying the data on cloud, especially if the cloud contains data of a particular organization, which the organization does not want to disclose to outsiders or they do not want outsiders to make any changes to the data on cloud. This problem can be solved if we can ensure the receiver of the cloud that the data sent towards the cloud actually came from some authorized user of cloud and it is further not possible to repudiate the stated content by the originator.

This paper proposes such a secure solution for cloud communication based on user authentication. We assume that the two parties are involved in communication of some data or message over the cloud, and the parties belong to same organization. On behalf of being a member of that organization, they are provided with a secret key, namely 'K'. Thus, we may further take the assumption to the next level where all employees or users of that organization have a common secret key 'K'. This key will used to transfer any data over the cloud of that organization. That is, it ensures that one can only transfer data to and from the cloud of the organization, if it belongs to that organization.

As general security practice, these parties must trust third party for notarization and authentication purpose. The key 'K' should be distributed to these parties via their certificate, which itself should be encrypted using their individual private keys Ka and Kb respectively. This key based approach authenticates all users that access cloud services belonging to an organization.

Before sending message over cloud, these parties must calculate digest of the message or data using a predetermined hash function [12]. For calculation of this hash, the earlier stated key 'K' can be used. The practice can be followed as given:

(a) For calculating hash, the message must first be divided into equal sized blocks-512 bit block each.

(b) Each block can be provided as input to a hash function (for example Tiger Hash Function [11]). The output of such hashing will be 192 bit digest.

(c) Further divide 192 bit hash value in three equal size parts: each one of 64 bit.

(d) Then apply a secret key encryption function using key 'K' on all of these three parts disjointedly. The output will be three 64 bit encrypted parts.

(e) Again, in next step merge these three parts and use this 192 bit code as input for processing of next block.

(f) The 192 bit last output obtained from processing of last block of message becomes the hash value of overall message.

(g) The 192 bit digest, generated in such a manner is transmitted along with data or message towards the cloud. An authenticated user for that part of data or message must surely possess the same secret key 'K'.

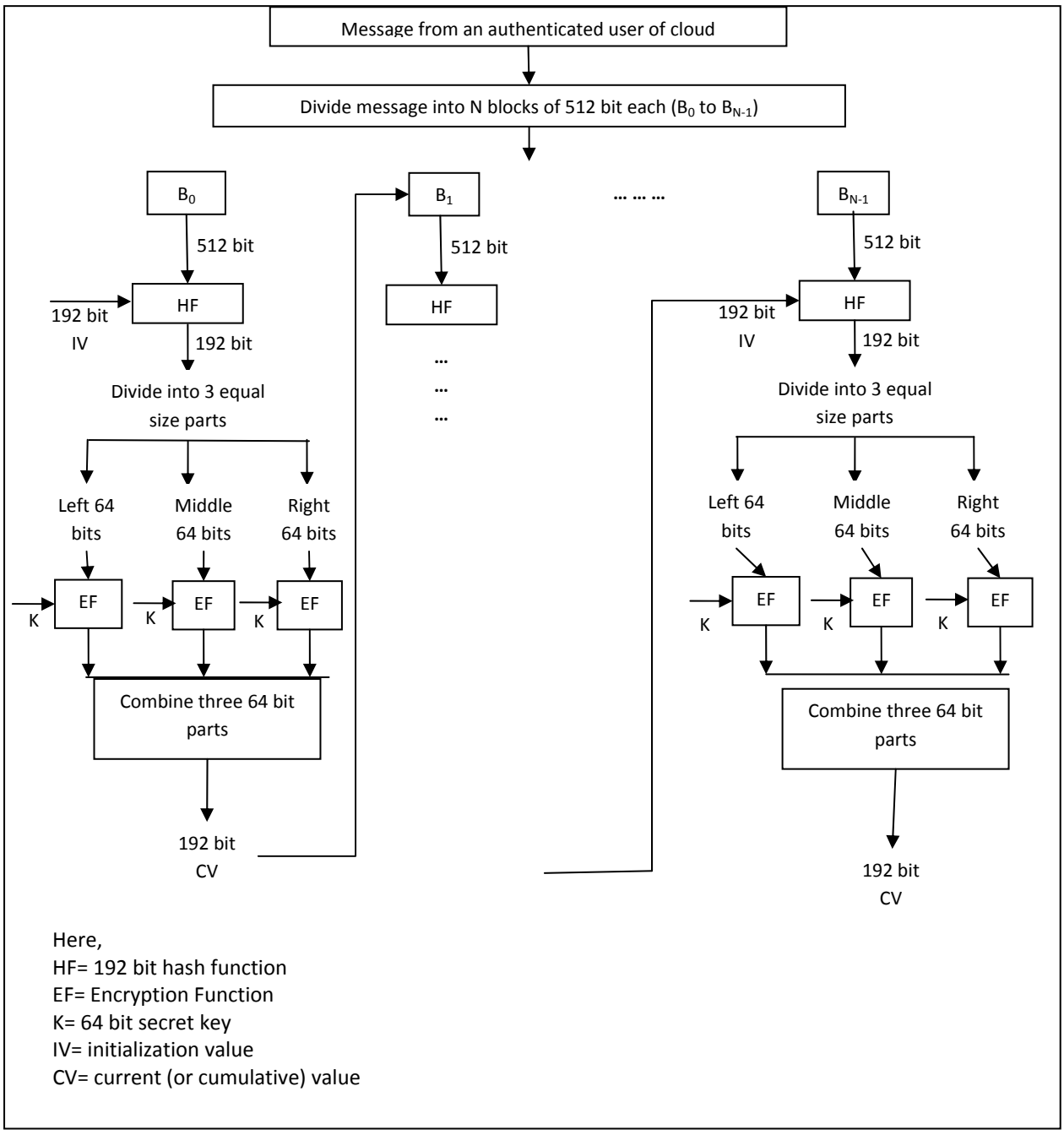

Figure 1: A Proposed solution for secure message communication over cloud

Using this it can verify the authenticity of sender and the received message from it. The use of secret key 'K' ensures that the originator of the message is authenticated user of the organization. The verification at the receiver end using the same key 'K' also authenticates him. Arbitrary changes by any of the unauthorized user, are vetoed by application of the key only. Thus if the cloud contains data for internal users of the organization, they may share this key among them and now nobody from outside the organization can either update the contents deliberately or can send spurious data over the cloud anytime with the name of any authenticated user.

The whole procedure can be shown as figure 1.

Time to time this secret key may be changed or updated considering the possibility of any security breach or snooping by adversaries. As soon as a new key is selected, it must be communicated to all users simultaneously and at the same time use of previous key must be blocked.

V. CONCLUSION

With an increase of personal and organizational data, more and more storage space is required. This ever increasing demand of storage space is now a days being fulfilled by Cloud. Clouds provide a huge space at disposal to be used. But being a comparatively new area, it is open for many kinds of security threats. In this paper many of such security issues were discussed. Further it discusses various approaches for enhancing the security over cloud data. The paper also proposes a technique for enhanced security over cloud using some secret key 'K', which is common to all authorized users of any particular organization. This secret key ensures communication between organization's cloud and its authentic user only.

REFERENCES

[1] Zhang, Q., Cheng, L. & Boutaba, "Cloud computing: state-of-the-art and research challenges". Journal of Internet Services and Applications. May 2010, Vol. 1(1), pp 7–18. DOI:10.1007/s13174-010-0007-6.

[2] S. Singh, Y S Jeong, J H Park. "A survey on cloud computing security: Issues, threats, and solutions". Journal of Network and Computer Applications. Vol 75. November 2016, pp 200–222.

[3] Available at: https://www.netskope.com/blog/cloud-multiplier-effect-data-breaches/. Last Accessed on: 17 March 2017.

[4] A. Singh, M. Shrivastava. "Overview of Attacks on Cloud Computing". International Journal of Engineering and Innovative Technology. Volume 1(4) , April 2012, pp-321-323.

[5] R. Clarke. "Data Risks in the Cloud". Journal of Theoretical and Applied Electronic Commerce Research. Vol. 8(3), December 2013, pp- 60-74.

[6] M. Armbrust et. al. "A View of Cloud Computing". Communications of the ACM. Vol.53(4), April 2010, pp-50-58. DOI: 10.1145/1721654.1721672.

[7] A J Choudhury et. al. "A Strong User Authentication Framework for Cloud Computing". In proceedings of IEEE Asia -Pacific Services Computing Conference, 2011.

[8] E. Bertino, F. Paci, R. Ferrini, N. Shang. "Privacy-preserving Digital Identity Management for Cloud Computing". Bulletin of the IEEE Computer Society Technical Committee on Data Engineering, 2009.

[9] D. Zissis, D. Lekkas. "Addressing cloud computing security issues". Future Generation Computer Systems. Vol. 28(3), March 2012, pp- 583–592.

[10] K. Zunnurhain1 and S. V. Vrbsky. "Security in Cloud Computing". In Proceedings of the 2011 International Conference on Security & Management, 2011.

[11] F. Mendel, V. Rijmen. "Cryptanalysis of the Tiger Hash Function". In: Kurosawa K. (eds) Advances in Cryptology – ASIACRYPT 2007. ASIACRYPT 2007. Lecture Notes in Computer Science, Vol 4833. Springer, Berlin, Heidelberg.

[12] R. Purohit, U. Mishra, A. Bansal. "Design and Analysis of a New Hash Algorithm with Key Integration". International Journal of Computer Applications. Vol. 81(1), November 2013, pp-33-38.