International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 6 (2018) pp. 3719-3724
© Research India Publications. http://www.ripublication.com

Highly Secure Virtual Identity Approach in Cloud Computing Environment

Garima Rastogi[1*] and Rama Sushil[2]

[1]Computer Science and Engineering Department, DIT University, Dehradun INDIA*
[2]Department of Information Technology, DIT University, Dehradun INDIA

Abstract

In this technological era, cloud computing has become a buzz word for all the service sectors, be it banking, health or any other business sector. Primarily, it provides significant benefits in terms of storage and maintenance of data and services. However, data security has always remained one of the biggest challenge in cloud. Therefore it is very important to focus on the security measures and techniques on the cloud environment so that cloud usage can be increased. This paper proposes a novel approach for enhancing security in cloud environment using virtual identity by hiding actual user identity. For achieving high security, Diffie-Hellman algorithm with station to station protocol has been used by the system. Paper also analyses the performance of system by taking various scenarios and discussion of previous research works.

Keywords: Security measures, virtual identity, Diffie-Hellman, station to station protocol, performance.

SIGNIFICANCE STATEMENT

As rapid changes in technology and the need for reduction of cost, organizations are moving towards cloud computing. Besides various benefits of cloud computing, organizations face different kind of challenges too. The three main challenges are –data protection, authentication of users and breaching of data. Apart from this, one more challenge that is of concern now a day is breaching of identity and accessing of data by unauthorized users.

This research study proposes a novel approach for enhancing security in cloud environment using virtual identity by hiding actual user identity. For achieving high security, Diffie-Hellman algorithm with station to station protocol has been used by the system. From the experimental analysis and verification of model we found that proposed model is quite secure and trustworthy for cloud environment.

INTRODUCTION

In traditional systems, software and hardware data deployed and developed within an organization in trusted boundaries having proper static methods for controlling and monitoring whole environment. Now a day's organizations want to save cost in various aspects like infrastructure, software licensing, service maintenance etc. with enhanced performance [1] [2]. In cloud computing, key features which attract organizations towards its adoption are small initial investment, low maintenance, dynamic provisioning, independence of location etc. to name few. Besides all the benefits, organizations face different kind of challenges too. The three main challenges are –data protection, authentication of users and breaching of data [2] [3]. Apart from this, one more challenge that is of concern now a day is breaching of identity and accessing of data by unauthorized users. This issue has become bigger challenge due to the usage of social networks like Face book, twitter and other platforms of networking, where user generally share their personal details, videos, pictures etc. thus disclosing their identity without knowing the implications. Therefore it is very critical to maintain privacy of identities in cloud environment. Traditionally, the term identity only meant userid and password for accessing a service over internet. But with time, the meaning of identity has become little bit critical due to security reasons and besides userid and password it contained some more parameters like age, gender, email id etc. This is now further extended to include biometric identity like face recognition, finger print etc. All these aspects can be used according to the required degree of complexity in security [4] [5] [13]. In virtual environment like cloud a virtual identity is used to improve the security for anonymous communication. Table 1 shows some schemes for anonymous communication used now a days.

Table 1. Some techniques of anonymous communication

Schemes	Parameters			
	Purpose	Merits	demerits	Anonymity
Proxy	Prevent unwanted request of internet user and IP address	Hide user data from unauthorized destination	Can be disclosed using traffic analysis	better
Private Browsing	It is feature which can be used to disable history and web cache.	Cleans browsing history and web cache	Can be disclosed using real time attack	Low
Virtual Private Network (VPN)	Encrypts all packets sent out	Out packets and encrypted	Disclosed it VPN server is hacked or key found	Best

This paper is focused on anonymous communication in cloud environment and proposes a novel virtual id management system which can be used for anonymous communication. The model establishes secure communication by using four entities- certificate authority (CA), authentication server (AS), user and cloud service provider (CSP). This model uses Diffie-Hellman algorithm with station to station protocol while key generation and can avoid various kinds of attacks.

The paper is organized as follows – section 2 illustrates the proposed approach. Section 3 illustrates the analysis of proposed system with the help of three experiments. Section 4 discusses the previous research works and uniqueness of the proposed system. Section 5 concludes the paper.

PROPOSED MODEL

Preliminaries

A survey was conducted to propose a new solution for secured communication in cloud environment. The basic purpose of survey was to find out awareness among users about security techniques, importance of security and other issues related to cloud security. Total 200 users were used for survey. The sample in the survey included cloud technology users from different places and backgrounds such as students, teachers involved in technical education, practitioners working on different IT companies and executives working in offices on the post of clerk, operators etc. **Fig. 1** shows the result of the survey.

The survey results showed that users were now becoming conscious and aware about the security and privacy of their data. They knew about the technologies that could be used for providing more security. Although most of the users especially office executives and teachers were still using traditional methods but few others had good knowledge about technologies being used in the market and were using them too.

Proposed Virtual Identity Based Model

In this section, the proposed methodology of the model is illustrated. For defining the model four entities are considered.

- Client – A user who wants to access services from cloud service provider (CSP). A client has to submit id and CSP service request (SerR) to authentication server for getting Transaction certificate (Ts), p and g for generating R1 (public key by using private key x). After generation of R1 the client will submit Ts (to verify) and R1 (to store) to certificate authority (CA).
- Authentication server (AS) – This is a server which is responsible to authenticate client and CSP id and generate random transaction certificate (Ts), p and g (large prime numbers). The Authentication server will send copy of these Ts, p and g to corresponding CSP also.
- Certificate Authority (CA)–It is system which is responsible for protecting public key from forgery. Also, it generates virtual id (Vid) for client with respect to CSP service request (SerR).The CA contains public keys of all the entities involve in the communication whether it is client or CSP.
- While submission of the public key, CA will write it on the certificate and sign the certificate with its private key. Now anyone who wants to access the public key, he or she has to download signed certificate and use the CA's public key to extract the required the required public key.
- Cloud service provider (CSP) – It is responsible to receive request from client by receiving signed virtual identity (SVid). If client's signature is verified then CSP will generate Ks (shared key) by accessing R1 from CA.

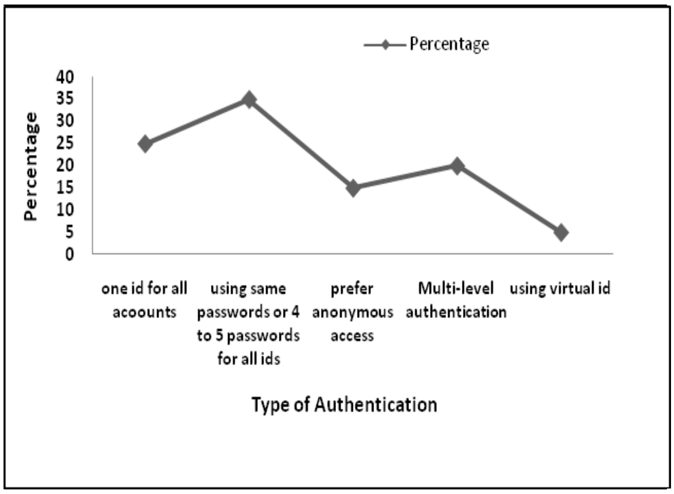

Figure. 1: Plot of survey result between type of identity and percentage

Fig. 2 shows the flowchart of the proposed scheme. The algorithms for proposed model are as follows.

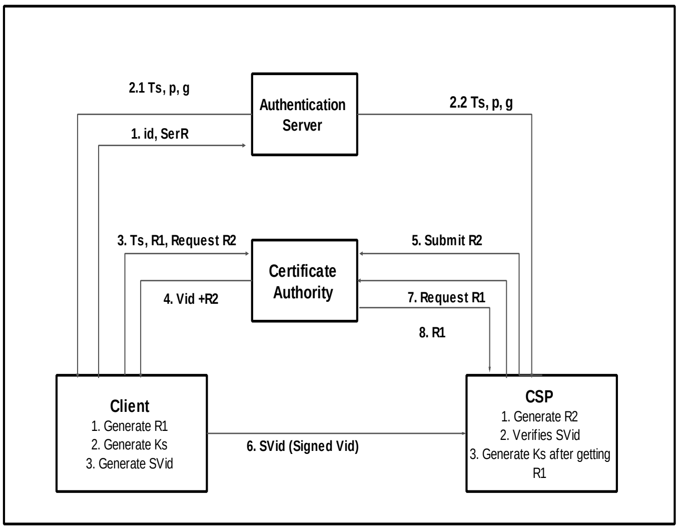

Figure. 2: Flow Chart of the proposed model

Algorithm 1: AS (id, SerR)

```
If id and SerR is valid then
    Generate Ts, p, g
    Send to client and corresponding CSP.
Else
Message invalid client
```

Algorithm 2: GenerateKeyClient ()

```
Ts, p, g =AS(id, SerR)
Generate R1=$g^x$ mod p
Send Ts, R1 and request of R2 to CA
CA will send Vid and R2
Generate Ks=$(R2)^x$ mod p
Generate SVid (digitally signed Vid)
GenerateKeyCSP(SVid)
```

Algorithm 3: GenerateKeyCSP (SVid)

```
Extract Ts, p,g from inbox sent by AS
Generate R2=$g^y$ mod p
If sign of client is verified from SVid then
    Request R1 from CA
Generate Ks=$(R1)^y$ mod p
Else
Delete all the entries received for communication.
```

EXPERIMENTAL WORK AND ANALYSIS

To verify all the security capabilities of the proposed model three experiments have been conducted. For generating the transaction certificate (Ts), Data encryption algorithm (DES) is used and for generation of shared key at both ends (client and CSP), Diffie Hellmen algorithm with the concept of station to station protocol is used. For establishing the experiment setup Linux environment and Java is used. The configuration of systems were - 2x4 core Intel ® Xeon CPU E5540 @ 2.53GHz and 12 GB RAM. We have used four hosts at the start. All the host servers could access the shared storage 50TB based on NetApp 3210V NAS and HP EVA6400 SAN with FC disks. For Virtualization we have used KVM (Kernel Virtual Machine) as open source.

Experiment-1 Man in Middle attack

In this experiment there is an unauthorized user, who is not a part of the communication but wants to have the information sent by authorized user. Authorized user name in the experiment is A and intruder is B. Here, B creates two keys- one key between A and B and another between B and CSP by generating self p and g. Now A chooses x and calculates R1. A sends R1 to CA. CA signs it with its private key and stores R1. Apart from public key, A sends it's Ts which contains SerR also. Now if B tries to communicate with CSP on the behalf of A, then B needs to submit its public key to CA with Ts (which can be generated by AS). If by chance, B hacks the Ts from the communication path of A and CA and wants to change and submit that Ts on behalf of A then also he needs key for decryption. If in case B tries to have new Ts from AS then AS will verify its identity in his database and denies to generate Ts. The experiment clearly shows that proposed scheme is capable enough to resist man-in-middle attack.

Experiment -2 Communication Path Interception

If any hacker tries to interrupt the communication path between client and CSP and tries to hack SVid. Hacker will not be able to extract because the Vid is digitally signed by client using its private key. B requires A's public key to extract SVid. Now suppose B hacked R2 by interrupting path of CSP and CA and generates Ks by using its private key z and also generates SVid by using its signature. After SVid is received by CSP, it will send request to CA for retrieving its public key and CA will deny for that and CSP will immediately declare B as unauthorized user.

Experiment-3 Authentication Server is hacked

In this experiment, an unauthorized user B tries to get the Ts from AS by hacking ID of A. To handle this in the proposed system, some human intervention is added. While registration of the ID with AS, there are some security questions that needs to be answered. These security questions will act as an extra security measure for authentication server as well as client. These questions will be asked randomly every time whenever user will submit request to generate Ts. **Fig. 3** shows the detailed model flow with all steps and human intervention checks. This small human intervention can reduce the chances of accessing AS by unauthorized user. There will be two security questions asked. If user is not able to answer the questions in three attempts then he will be declared as unauthorized user. Apart from this, the data stored in AS is also in encrypted form using concept of homomorphic encryption technique RSA [6].

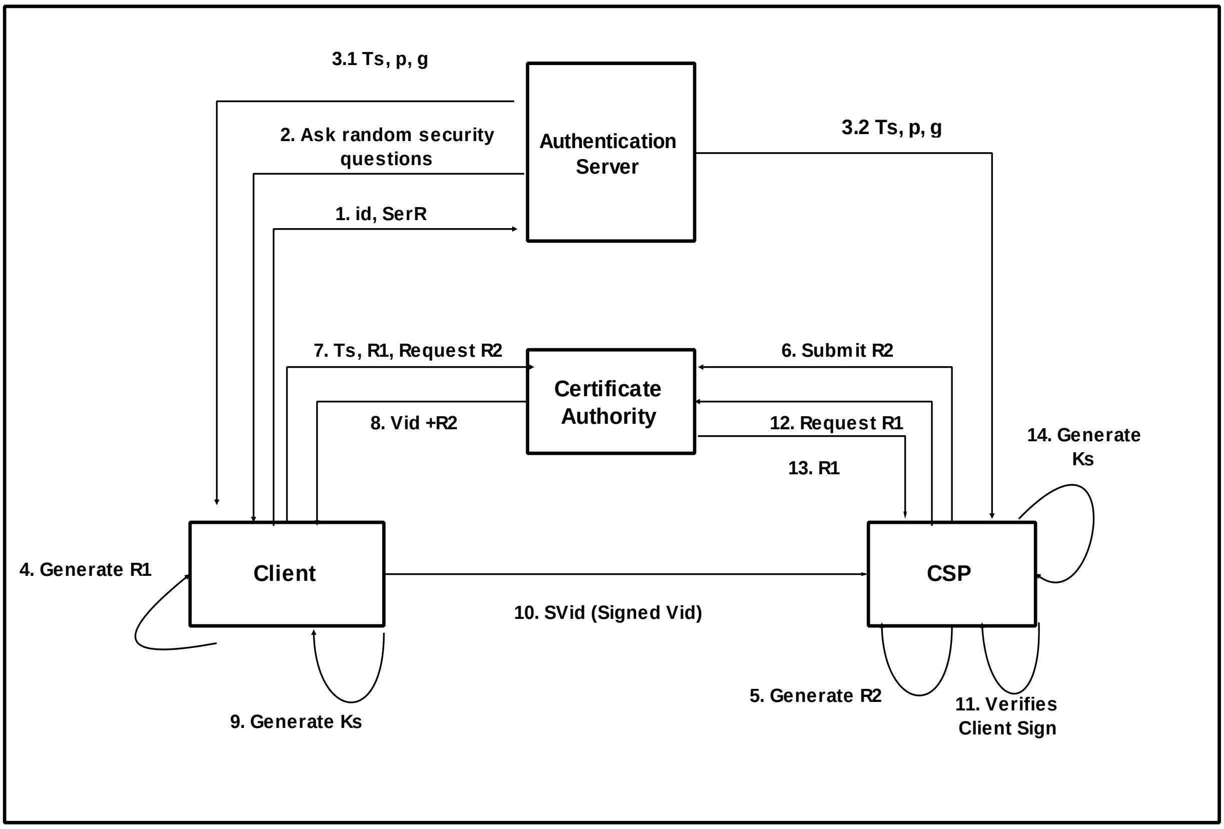

Figure 3: Virtual Identity model with human intervention

DISCUSSIONS

Cloud is based on internet and users who are using cloud or working on cloud are always concerned about privacy of data. With the popularity of social networking sites like face book, twitter etc. a large number of users share their photos, videos and other personal details [7] [8]. According to the report of 2013, there are approximately more than one billion users active on Face book monthly [9], so through these sites users disclose their privacy, largely inadvertently, as most of the users do not read privacy policies of these sites in detail [10]. In a report published in 2015 on data breach, it was investigated that most of the social networking platforms suffer from social engineering attacks and it is increasing drastically due to continuous usage of these sites [11] [12]. Since, these sites are not only used by general people for sharing information now, but it has become a productive platform and advertising channel for lot of business organizations. Therefore, it is extremely important that only authorized users and cloud service providers (CSP) only can access their data. In this scenario the role of virtual identity becomes very critical on internet environment. Anonymous communication on internet must protect privacy. There are various anonymous techniques used, today, for this purpose. Google chrome’s Incognito feature for anonymous browsing and Firefox’s private browsing etc. are few examples in this case [13]. Many researchers have done work on this area to enhance security on social network. In a study [14] authors proposed anonymous credential system which uses digital certificates issued by a trusted authorities for personal usage. They also applied some techniques to make certificates non transferrable. In a study [15] authors proposed a scheme called as string designated verifier signature. It is a digital signature scheme which focuses in ID based crypto system. The scheme was also able to resist against key-compromise attack.

Identity management through conventional system using username and password is also not secure for internet environment. One of the main reasons for this is that most of the users either keep same passwords or maximum of 4 to 5 passwords for all online identities. Therefore it is very easy for hacker as if he or she can break one then all identities can possibly be accessed [16]. Various alternatives are introduced by researchers in view of overcoming this threat. Some solutions are token generation, multi-level authentication, biometric authentications etc. In a study [17] the authors proposed a scheme for identity management system which uses the concept of token generation and multiple authentications. The scheme can resist against network traffic interception attack as well as replay attack. In a research study [18] the authors proposed a protocol using trapdoor proxy signature with the compilation of all access policies. Main features of the proposed protocol includes on-demand operation and non-interactive with flexible access control policies. In a study [19] the authors have discussed about OAuth. An analysis was done to brief that OAuth system used token with limited time and scope for accessing of resources. The authors also identified some attacks like server trust, timing attack on OAuth system. In a study [20] authors proposed a model for identity as a service called as BlindIdM. The model was proposed to provide access to the network without having access to user’s information. In a study [21] authors proposed an algorithm for identity and access management named as PRIAM. The model was built for privacy preserving and secure authentication.

This proposed work is unique in the sense that it uses the concept of virtual identity which will exist only for single communication. From the experiment it can be seen that the scheme is able to provide protection from various kinds of attacks such as man in middle attack, communication path interception and hacking of authentication server etc. There are different mechanisms used in the schemes proposed by various researchers in the literature. This proposed model tries to accommodate all the positives of the existing models and also enhance some security level by adding human intervention. This kind of human intervention is very much required in cloud systems because everything is handled by the third party. For more details the survey has been done in this study which clearly shows that most of the users are very casual while keeping passwords and making Ids so this human intervention will give some kind of security layer above the ID and password level.

CONCLUSION

Identity management system is a kind of system that works on the behalf of service providers to authenticate the users who wants to access the resources from cloud. In this paper new virtual identity management scheme has been proposed to perform the secure communication in cloud environment. The proposed algorithm is tested and validated through series of experiments. The results of experiments show that the scheme can resist some important attacks like man in middle attack, communication path interception etc. Apart from that the scheme is using shared key concept eliminating the need to transfer keys on the communications path. Scheme also has some security enhancement by using human intervention by asking random security questions to the user while generating the transaction certificate from authentication server. For protecting from discrete logarithmic attack both CSP and client will delete there private keys after generating shared keys so that private keys will be used only once and in case any intruder will try to hack client system or CSP , he will not be able to find private keys. Scheme is using a special system called as certificate authority which is acting as repository of all the public keys used in the system. Hence no unauthorized user can access public key of any user.

REFERENCES

[1] K., Ronald L. and Vines R. D., 2010. Cloud Security: A comprehensive guide to secure cloud computing Wiley Publishing, Inc. Indianapolis, Indiana, pp. 61-120.

[2] Hoang N. and Pishva D., 2014. Anonymous communication and its importance in social networking. In proceedings of Advanced communication technology IEEE conference, pp: 43-39.

[3] Gopalakrishnan A., 2009. Cloud Computing Identity Management. SETLabs Briefings, 7: 45–54.

[4] Zissis D. and Lekkas D., 2012. Addressing cloud computing security issues. Future Generation Computer System, 28(3): 583–592.

[5] Habiba U., Masood R., Shibli M. A., and Niazi M. A., 2014. Cloud identity management security issues & solutions: a taxonomy. Complex Adaptive Systems Modeling, 2(1):2-37.

[6] Rastogi G. and Sushil R., 2015. Cloud Computing Security and Homomorphic Encryption. IUP Journal of Computer Sciences, 9(3):48-58.

[7] Ramachandran M. and Chang V., 2016. Towards performance evaluation of cloud service providers for cloud data security. International Journal of Information Management, 36(4):618-625.

[8] Yang G., Yu J., Shen W., Su Q., Fu Z., Hao R., 2016. Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability. Journal of Systems and Software, 113: 130-139.

[9] Face book reports second quarter 2013 results, Face book, Retrieved 13 May 2017.

[10] Threat Actions, the 2014 data breach investigations report, Verizon enterprise, page 9, http://www.verizonenterprise.com/DBIR/2015/, last visit: May, 2017

[11] Yu Y., Xue L., Au M. H., Susilo W., Ni J. , Zhang Y., Vasilakos A. V., and Shen J., 2016. Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Generation Computer Systems, 62: 85-91.

[12] Yan Z., and Shi W., 2017. CloudFile: A cloud data access control system based on mobile social trust. Journal of Network and Computer Applications, 86: 46-58.

[13] Gomaa, IA., Abd-Elrahman E., and Abid M., 2015. A Novel Virtual Identity Implementation for Anonymous Communication in Cloud Environments. Procedia Computer Science, 63: 32-39.

[14] Camenisch J. and Van Herreweghen E., 2002. Design and implementation of the idemix anonymous credential system. In Proceedings of the 9th ACM conference on Computer and communications security, pp: 21-30. ACM.

[15] Lin H.Y., 2014. Toward secure strong designated verifier signature scheme from identity-based system. International Arab Journal of Information Technology, 11(4): 315-321.

[16] Gomaa, IA., Abd-Elrahman E., and Abid M., 2016. Virtual Identity Approaches Evaluation for Anonymous Communication in Cloud Environments. International journal of advanced computer science and applications, 7(2): 367-376.

[17] Khalil I., Khreishah A. and Azeen M., 2014. Consolidated Identity Management System for Secure Mobile Cloud Computing. Computer Networks, 65: 99-110.

[18] Chandrasekhar S, Ibrahim A., and Singhal M., 2017. A novel access control protocol using proxy signatures for cloud-based health information exchange. Computers & Security, 67: 73-88.

[19] Hardt D., 2012. The OAuth 2.0 Authorization Framework, Ed. Microsoft. July 31.

[20] Nunez D. and Agudo I., 2014. BlindIdM: A privacy-pre9serving approach for identity management as a service. International Journal of Information Security, 13(2): 199-215.

[21] Xiong J., Yao Z., Ma J., Liu X., Li Q. and Ma J., 2014. PRIAM: Privacy Preserving Identity and Access Management Scheme in Cloud. KSII Transactions on internet and information systems, 8(1) : 282-30.