Attribute based Multifactor Authentication for Cloud Applications

T.Lakshmi Praveena
M.Tech Scholar
VVIT College of Engineering
Nambur,Guntur(Dt),AP

V.Ramachandran
Asst.Professor
VVIT College of Engineering
Nambur, Guntur(Dt),AP

CH. Rupa, Ph.D
Associate Professor
VVIT College of Engineering
Nambur, Guntur(Dt),AP

ABSTRACT

Online information maintenance through cloud applications allows users to store, manage, control and share their information with other users as well as Cloud service providers. There have been serious privacy concerns about outsourcing user information to cloud servers. But also due to an increasing number of cloud data security incidents happened in recent years. Proposed system is a privacy-preserving system using Attribute based Multifactor Authentication. Proposed system provides privacy to users data with efficient authentication and store them on cloud servers such that servers do not have access to sensitive user information. Meanwhile users can maintain full control over access to their uploaded files and data, by assigning fine-grained, attribute-based access privileges to selected files and data, while different users can have access to different parts of the System. This application allows clients to set privileges to different users to access their data.

General Terms

Elliptic curve cryptography, Key generation algorithm using ElGamal. Algorithm for Zero knowledge proof.

Keywords

Multifactor authentication, Digital Identity Management, Zero Knowledge Proof Protocol, Inter cloud authentication, SAAS,ElGamal**.**

1. INTRODUCTION

A cloud application allows utilizing resources in an efficient way. This is also known as Internet Computing or sharing of resources. Cloud users can share database resources, Infrastructure resources and system resources through Internet from anywhere; it doesn't require any maintenance or management of resources. These are dynamic applications and scalable applications of cloud servers. Cloud Apps are aimed to deliver different services like storage resources, computing resources, network resources, etc. These services are reliable, scalable, portable and flexible. In fact, it is a very independent platform in terms of computing. The best Example of cloud application is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet and Media Fire which provides infrastructure as a service.

1.1 Security Issues in cloud

Cloud computing is presenting itself as a good servant to the end user, but it has some challenges and issues.

Security issues are the most vital issues of the cloud applications. It is high risk issue to store company data and information on cloud server and running an application at another's place is also at stake. Because data loss, phishing the data, threat is the common problem.

Privacy and reliability are to be maintained during transferring and storing of the data. Cloud is made for sharing the workload into the common infrastructure and users have to rely on the cloud provider about their identity information, operation histories and perceptive data. Cloud is not responsible for unauthorized usage and its retrieval, lack of user administration and third party access.

Interoperability Issues of different identity attributes and client centric protocols and identity based protocols.

1.2 Authentication Issues Of Cloud Computing

- Cloud service providers store client information on the cloud server which is remote server and managed by CSP. So the privacy is the major issue of authentication.
- The lack of transparency in the privacy information of the user on the cloud.
- If the multiple services are used from the different cloud servers then the login information is repeated on each cloud. This is the security issue of cloud user and the cloud server.
- For every service of different clouds, the user has to exchange their information which leads to exploit of the authentication mechanism.
- The different authentication technologies are used by the different users. This show less impact on PaaS,SaaS and IaaS. This is another issue of authentication.

2. RELATED WORK

Over some years Cloud Apps Security got progress by applying different methods. There is a strong need for providing security for accessing cloud applications. Many concepts which are providing security for Cloud Apps are introduced. Here some works which are based on user authentication are given.

1. In 2001 M. Looi presented Enhanced Authentication Services for Internet Systems using Mobile Networks with the concept of adding additional factors to Internet user authentication significantly improves the strength of authentication.
2. In 2002 Taekyoung Kwon proposed a concept called Impersonation Attacks on Software Only Two-Factor

Authentication Schemes. However it can be vulnerable to impersonation attacks via interleaved sessions if a single server is compromised
3. In 2008 Manik Lal Das prposed Secure and Efficient Authentication Scheme for Remote systems which provides efficient mutual authentication scheme for remotesystems,
4. In 2009 M.L Das has proposed two factor user authentication for WSN which provides stronger user authentication, session key establishment and achieves efficiency.
5. In 2010 Qiong Pu introduced An Improved Two-factor Authentication Protocol. He suggests key-compromise impersonation resilience should be added as one more important security requirement for two-factor based authentication scheme

The proposed system is based on security certificate which is generated by Zero Knowledge Proof Protocol. The two factors are used to authenticate user. One factor is verifying identity attributes of user and generating a key. Second factor is conforming authentication by cross checking the parts of keys send to email and phone of user.

3. PROPOSED SCHEME

When the user wishes to authenticate to the system, the system attempts to access the user's software-based certificate, which is stored in a file or in the registry on the hard drive. When the certificate is located, the user is prompted to provide their PIN or password to unlock the certificate store. If successful, the software installed on the computer assists the user to verify their identity by signing an authentication request with the user's private key.

The Identity Management on cloud has different entities, Identity providers, Cloud service providers, Registrars, users. *Service providers* provide the service to the users to access data and software on cloud servers. *Registrars* store and manage information related to the attributes used in multifactor authentication. These identity attributes are used in Zero Knowledge Proofs of Knowledge. The Registrar stores each user information as an Identity Record (IdR) containing an identity tuple for each user's identity attribute *m*. Each identity tuple consists of a *tag*, that is, an attribute name, of m, denoted by M_i, the signature of the registrar on *M*, denoted by μ_i, two types of assurance, namely *validity assurance* and *ownership assurance*, and a set of nyms (also called leak identifiers) $\{W_{ij}\}^3$[10]. M_i is computed as $g^m h^r$, where *m* is the value of the identity attribute, *r* is a random number in Z_p and only known to the client, and g and h are generators of a group G of prime order p. G, g, h and p are public parameters of the Registrar. *Validity assurance* corresponds to the confidence about the validity of the identity attribute based on the verification performed at the identity attribute original issuer. *Ownership assurance* corresponds to the confidence about the claim that the principal presenting an identity attribute is its true owner. The identity tuples of each registered client can be retrieved from the Registrar by CSPs (*online* mode) or the Registrar can release to the client a certificate containing its identity record (*offline* mode) [10].

Proposed multifactor authentication protocol takes place between a client and CSP1, CSP1 to CSP2. It consists of two phases. The first phase is user logins with username and password, then the CSP generates a random prime number or key based on the identity attributes of the user. This key value is splitted as K_1 and K_2. K_1 is send as message the email account of user and K_2 is send as SMS message to the user mobile. The identity attributes are matched based on the vocabulary with its own attributes. After providing the complete key K, an *identity verification policy* is used to check the set of attributes to prove the identity of the user. The values of these identity attributes are only needed for verification purposes but not for the execution of the service required by the client. In the second phase, the client executes the Zero Knowledge Proof Knowledge Protocol[7] to prove the CSP the knowledge of the matched identity attributes. The use of this protocol allows the client to convince the CSP that the client knows the values of the identity attributes without having to reveal to the CSP the values in clear.

3.1 Multifactor Authentication

Registration Phase

Client registers with the cloud application by providing all information required for authenticating the user.

Login Phase

Client uses login form to access the cloud application and its services. This accepts username and password. And submits username and password.

Key generation Phase

Once the client logins with username and password the a key K is generated. For the key generation, the CSP accesses matching attributes of user from Registrar. M_i is the set of matching attributes and μ_i is the corresponding signatures. CSP finds the aggregate by computing

$$M=\sum_{i=1}^{n} M_i = g^{m_1+m_2+\cdots\ldots\ldots+m_i} * h^{r_1+r_2+\cdots+r_i}$$

And signatures as

$\mu=\prod_{i=1}^{n} \mu_i$ where μ_i is the registrars signature in the value of M_i[10]

Split Phase

The M value is the key K and is splitted as two parts K_1 and K_2. The K_1 is send to the email id provided by the client in the process of registration and K_2 is send as SMS to the mobile phone no. provided at the time of registration of the user. This information is stored at the registrar.

Zero Knowledge Proof Protocol

According to the Zero Knowledge Proof protocol, the client randomly picks y, s in [1, ..q], computes $d = g^y h^s$ (mod p), and sends d, μ, M, M_i , 1 <= i <= t, to the CSP. The CSP sends back a random challenge e ∈ [1, .., q] to the client. Then the client computes u = y+em(mod q) and v = s+er (mod q) where m = m1 + . . . mt and r = r1 + . . . rt and sends u and v to the CSP. The CSP accepts the aggregated zero knowledge proof if $g^u h^v = dc^e$. If this the case then CSP conforms with the correctness of user identity.

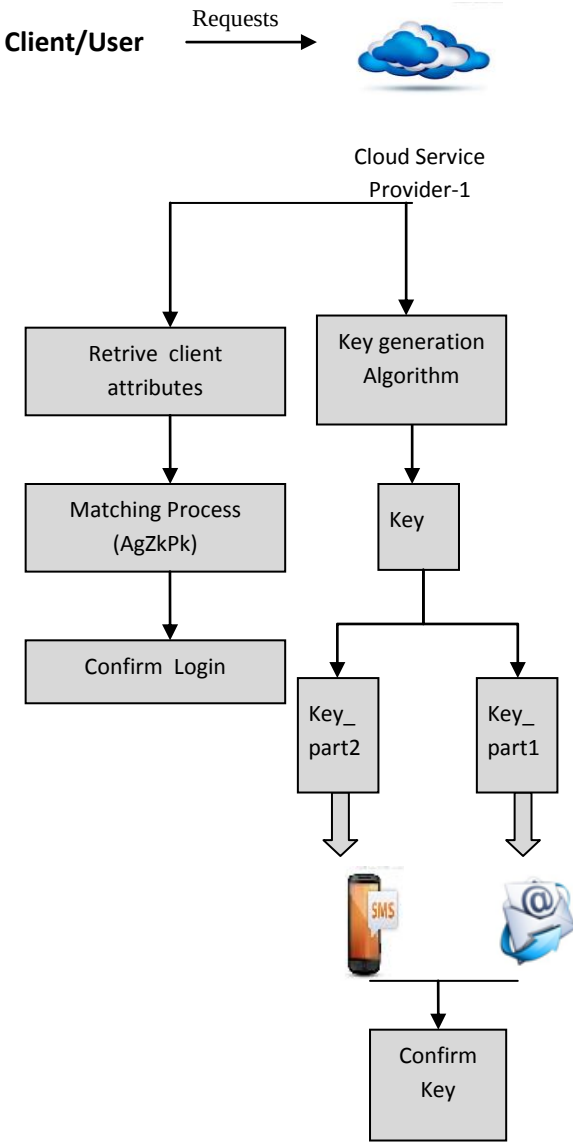

Fig 1. Attribute Based Multifactor Authentication System

The AgZkPk is the process of matching the attributes of client by generating a identity certificate. Whenever user request for the service then the generated certificate is issued to client and a key is generated at client side also. These are compared each other. Then the login is confirmed by matching these certificates. This process is known as Zero Knowledge Proof because without having login information, user is authenticated with this process.

The following figure demonstrates the structure of AgZkPK.

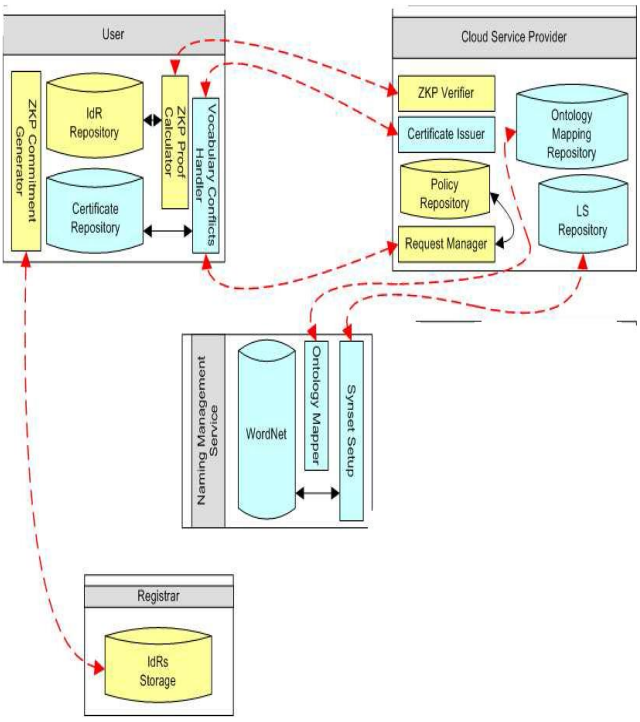

Fig 2. Zero Knowledge Proof Architechture

4. SYSTEM IMPLEMENTATION

Algorithms used in the implementation

Generating elliptic curve points

gen_points(p,a,b) [11]

```
{
        x=0;
        While(x<p)
        {
                W=(x^3 + ax + b ) mod p
                If( w is a perfect square in Zp)
                display( (x,sqrt(w) ),(x,-sqrt(w)))
                X=x+1
        }
}
```

Generating public key [11]

1. Select a point E(a,b) with an elliptic curve over GF(p).
2. Select a point on the curve, e1(x1,y1).
3. Choose an integer d.
4. Calculate e2(x2,y2)=d * e1(x1,y1)
5. Combination of E(a,b), e1(x1,y1) and e2(x2,y2) is key.

Encryption process:

Select P, a point on the curve,as plain text,P. Then calculate a pair of points on the text as cipher text.

Process of proposed system implementation:

1. Compute $M_i = g^m h^r$ where m is identity attribute, r is random number in Z_p
2. g ,h are the generators of group G of elliptic curve.
3. Now find the M as product of M_i for n attributes.

4. Find the μ as the product of μ_i for n attributes. This value is used as signature of registrar.
5. Now split the M value and send parts of key to mobile and email accounts.
6. As another factor of authentication, according to the ZkPk client selects y,s in [1,.., q].
7. Client calculates d=$g^y h^s$ (mod p)
8. Client sends d, μ,M,M_i to the CSP service.
9. CSP sends a value e to the client. Then client calculates u,v as follows and sends to CSP.
   u= y + em(mod q) where m=m1+m2+....+mt
   v= s + er (mod q) where r=r1+r2+.....+ rt
10. If $g^u h^v = dc^e$ then authentication is conformed by CSP.

5. EVALUATION

This system is SAAS based cloud service. The application implementing Identity Matching protocol, Zero Knowledge Proof Protocol and attribute based multifactor authentication protocol. Application uses attribute based key generation process to generate the security key. Apart from the computer, the system is using different devices to send security information. This process makes difficult to break the privacy. If cracker success in accessing one device and may fail to access another device. The key also generated based on the attribute information given by the client at the time of registration. If user accesses from same CSP for more than once then it skips the verification process.
After evaluating the AgZKPK protocol that characterizes our approach to multi-factor identity verification and the identity attribute names matching process. The expected experimental evaluations are:

- The time taken by the Client to generate the aggregate ZKP by varying the number of identity attributes being aggregated from 1 to 50.
- The time taken by the cloud service for aggregate ZKP verification execution time varying the number of identity attributes being aggregated from 1 to 50.

6. CONCLUSIONS

In this paper we have proposed an approach to the verification of digital identity for cloud platforms. Our approach uses efficient cryptographic protocols and matching techniques to address heterogeneous naming. We plan to extend this work in several directions. Biometric way of authentication can also be implemented as further implementation. Security algorithms can be used to provide more security to the generated authentication information. This system provides less complexed and efficient privacy policy for cloud based applications. If the user is unable to access mobile phone or email account then the system provides alternate ways by checking all the identity attributes of the user. And it also suggests the user to change their mobile phone no and email account ids whenever they are lost or modified. The transactions log information is also send to user accounts.

7. ACKNOWLEDGEMENTS

The author is thankful to Professor CH.Rupa, Professor A. Kalavathi for their valuable suggestions and help. The author is greateful to Asst. Professor V. Rama Chandran for his valuable suggestions and continuous help throughout the preparation of this paper.

REFERENCES

[1] Bhargav-Spantzel, A., Squicciarini, A.C, Bertino, E.: Establishing and Protecting Digital Identity in Federation Systems. Journal of Computer Security, IOSPress, 14(3), pp. 269–300, (2006)

[2] Choi, N., Song, I. Y., Han, H.: A survey on ontology mapping. SIGMOD Record 35, (3), pp. 34–41.

[3] Falcon, http://iws.seu.edu.cn/projects/matching/

[4] Y. Kalfoglou, and M. Schorlemmer. "Ontology mapping: the state of the art." The Knowledge Engineering Review, 18(1), pp. 1–31, (2003).

[5] Pedersen, T.P.: Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. Advances inCryptology, Proc. CRYPTO '91, pp. 129–140, (1991).

[6] WordNet, http://wordnet.princeton.edu/

[7] White paper: AEP Smartgate Security, Strong Multi Factor User Authentication for secure information sharing, white paper, AEP Networks, December 1998, http://www.aepnetworks.com/products/downloads

[8] Jae-Jung Kim* and Seng-Phil HongA Method of Risk Assessment for Multi-Factor Authentication, Journal of Information Processing Systems, Vol.7, No.1, March 2011 DOI : 10.3745/JIPS.2011.7.1.187

[9] Ming Li *Member, IEEE,* Shucheng Yu, *Member, IEEE,* Yao Zheng, *Student Member, IEEE,* Kui Ren, *Senior Member, IEEE,* and Wenjing Lou, *Senior Member, IEEE,*Scalable and Secure Sharing of Personal Health Records in Cloud computing using Attribute-based Encryption, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS VOL. XX, NO. XX, XX 2012

[10] Elisa Bertino , Federica Paci , Rodolfo Ferrini , Ning Shang ,Privacy-preserving Digital Identity Management for Cloud Computing, *Copyright 2009 IEEE,* Bulletin of the IEEE Computer Society Technical Committee on Data Engineering

[11] Behrouz A. Forouzan, Cryptography & Network security,TATA McGraw Hill .

AUTHOR BIOGRAPHY

T.Lakshmi Praveena, is a M.Tech scholar at VVIT(Vasireddy Venkatadri Institute of Technology),Nambur. She got his B.TECH Computer Science & Systems engineering Degree from Nagarjuna University. She is very much interested in Cloud Computing, Information Security.

V.Ramachandran, is a research scholar at Acharya Nagarjuna University, Nambur. He got his B.TECH Computer Science & Systems engineering Degree from Andhra University and M.TECH in Computer Science Engineering from JNTU, Kakinada. He is very much interested in image processing, medical retrieval , human vision & pattern recognition. He did several projects in image processing.