DATA STORAGE SECURITY USING PRIVACY PRESERVING WITH ANONYMOUS AUTHENTICATION IN CLOUD

Foram Kansar[1], Jaydeep Viradiya[2]

[1] Student, Information Technology, Parul Institute of Engineering and Technology, Gujarat, India
[2]Assistant Professor, Computer Science and Technology, Parul Institute of Engineering and Technology, Gujarat, India

ABSTRACT

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as service over the Internet. This paradigm also brings many new challenges for data security and access control when users outsource sensitive data for sharing on cloud. To access the data stored in cloud, existing work apply cryptographic method such as attribute based encryption and attribute based signature. But in doing so, these solution leak the identity information of the users. For the purpose of securing access control in cloud while keeping the user's privacy, proposed the idea of identity-based group signature and apply it to realize the anonymous authentication to the cloud.

---

1. INTRODUCTION

Cloud computing is a way of offering services to a customer, it is based on a number of characteristics like On-demand self-service, Location independent resource pooling, Broad network access, Rapid Elasticity and Measured service. These characteristics promise faster implementations times, lower cost, bigger scalability and more end user satisfaction.

Software As A service (SaaS), Services at the software level consist of complete applications that do not require development. Such applications can be email, customer relationship management, and other office productivity applications. Enterprise services can be billed monthly or by usage, while software as service offered directly to consumers, such as email, is often provided for free. Platform As A Service (PAAS) ,At this layer customers do not manage their virtual machines, they merely create applications within an existing API or programming language. There is no need to manage an operating system, let alone the underlying hardware and virtualization layers. Clients merely create their own programs which are hosted by the platform services they are paying for. Infrastructure As A Service (IAAS), The infrastructure layer builds on the virtualization layer by offering the virtual machines as a service to users. Instead of purchasing servers or even hosted services, IaaS customers can create and remove virtual machines and network them together at will. Clients are billed for infrastructure services based on what resources are consumed. This eliminates the need to procure and operate physical servers, data storage systems, or networking resources

1.1 Existing Work

Considering one situation, A law student, Alice, wants to send a series of reports about some malpractices by authorities of University X to all the professors of University X, research chairs of universities in the country, and students belonging to Law department in all universities in the province. She wants to remain anonymous while publishing all evidence of malpractice. She stores the information in the cloud. Access control is important in such case, so that only authorized users can access the data. It is also important to verify that the information comes from a reliable source. Problems of access control, authentication, and privacy protection should be solved simultaneously.

1.2 Attribute-Based Encryption

Step 1: System initialization

The secret key of Key Distribution Center A_j is

$SK[j] = \{\alpha_i, y_i, i \in L_j\}$

Where,

L_j = Set of attributes that KDC A_j possesses

A_j = j-th KDC

α_i and y_i two random exponent

Step 2: Key Generation and Distribution by KDC

$sk_{i,u} = g^{\alpha i} H(u)^{yi}$

Where,

$\alpha_i, y_i \in SK[j]$

H = hash function

Step 3: Encryption by sender

ABE.Encrypt(MSG, χ) and outputs the ciphertext C

Where,

MSG = Message

χ = access policy

Step 4: Decryption by Receiver

ABE.Decrypt(C, $\{sk_{i,u}\}$)

Where,

C = cipher text

$sk_{i,u}$ = secret key

Attribute Based Signature

Sign,

Attribute based signature with trustee's public and KDC's private key with message and access policy y.

Verify

Trustee public key, message and access policy is verified by the verifier if verification is true then returns 1 otherwise 0.

2. PRPOSED WORK

Attribute based access control, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data. For instance, in the above example certain records might be accessible by faculty members with more than 10 years of research experience or by senior secretaries with more than 8 years experience. This is the example of access policy. Using Attribute Based Encryption, the records are encrypted under some access policy and stored in the cloud. Users are given sets of attributes and corresponding keys. Only when the users have matching set of attributes, can they decrypt the information stored in the cloud. Here the user might want to post a comment on an article but does not want to reveal the identity. For this attribute based signature has been applied. Attribute Based Signature can be combined with Attribute Based Encryption to achieve authenticated access control without disclosing the identity of the user.

First user needs to register to the group manager. Group manager response with the group id to the user, through which user can get access to the cloud without access policy.

The proposed identity based group signature scheme is comprised of the following procedures:

Step 1: Setup

Let G1 be a group of prime order q, G2 be a cyclic multiplicative group of the same prime order p. The Group Manager chooses the input of security parameters and a group secret key of the group manager G_{mass} and output a group public key Gpub. A bilinear pairings is a map ê: G1×G1 → G2. Suppose H1 and H2are secure one-way hash functions.

− Computes Ppub = sec·g, where generator g and sec $\in$ Zp*.

− Gpub = (H1, H2, G1, G2, g, Ppub, ê, p).

− GM Secret key is G_{mass} = sec

Step 2: Member Key Generation

In this algorithm the group member private key is generated by the Group Manager. The Group Manager will not know the secret parameters used by the member. The group signing key is generated by any group member using their member secret key and member certificate. The communication between the GM and the group member is secured.

Group Member:

-computes $v = r1 \cdot g$, where $r1 \in Zp^*$

-Sends v with Group Member identity ID_i to GM.

Group Manager:

-Computes $S_{IDi} = sec.H_2(ID_i \parallel v)$(group member's private key)

-Sends S_{IDi} to the group member.

Group Member:

-Private key pair (r_1, S_{IDi})

Step 3: Join

Suppose now that a user wants to join the group in the Identity based system performs the following protocol and becomes a member of the group.

− User chooses a random $r_2 \in Zp^*$.

− Sends $(r_1\ r_2\ g, r_1g, ID_i, r_2g)$ to GM and proves to GM that the user knows S_{IDi}.

If GM is convinced that the user knows S_{IDi}

− Group Manager sends $S = sec\ .\ H_2\ (ID_i \parallel r_1r_2g)$ to the user using secured channel.

− Secret keys r_2 and r_1r_2

− The member key r_2g

− The member certificates (r_1, r_2g, S)

Step 4: Signing

This algorithm uses the group's public key, a membership certificate, a membership secret and a message as input and outputs a group signature on the message. To sign a message msg the group member executes Sign(private key, msg).

-Chooses a random $r_{3} \in Zp^*$

-Compute

$R_1 = r_3.r1r2g$

$R_2 = (p - r_3).\ R_2g;$

$R_3 = r_4.H_2(IDi \parallel R_1 + R_2);$

The resulting signature on the message is (R_1, R_2, R_3)

Step 5: Verification

An algorithm that is used to verify the group signature with respect to the group public key on input of a message. The identity of the group member who has generated the group signature is available only to the Group Manager, not to others. The receiver verifies that the signature was generated by the group member is valid and finds out the signer is an authorized member of the group or not.

3. EXPERIMENTAL RESULTS

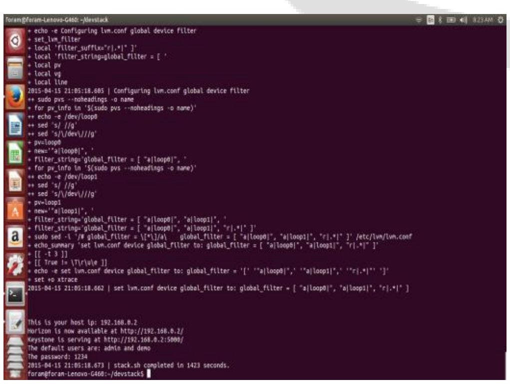

Figure- 1 Openstack cloud Horizone

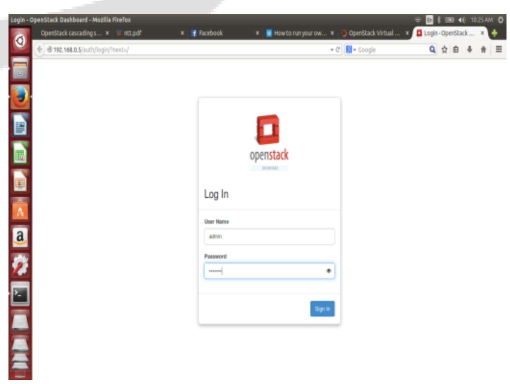

Figure-2 Openstack Login

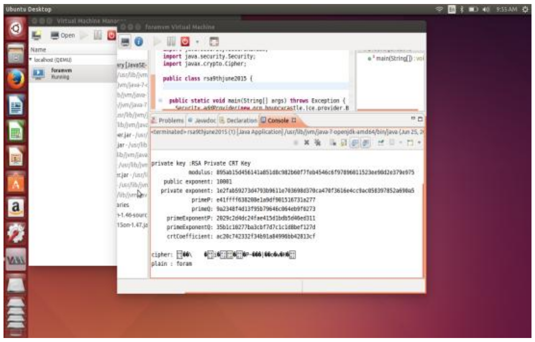

Figure-3 RSA Implementation in VM

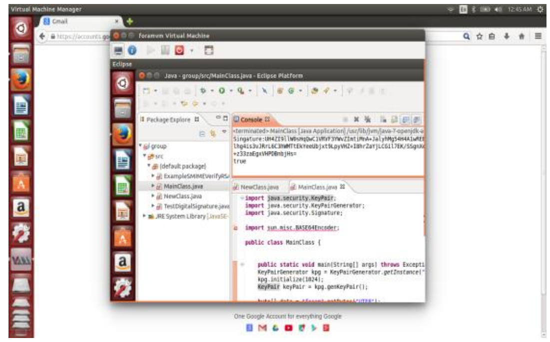

Figure-4 Signature Implementation in VM

4. CONCLUSIONS

Presented a decentralized access control technique with anonymous authentication which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.The privacy preserving technique is proposed so that the cloud cannot able to know the access policy for each record stored in the cloud. The attribute is also hidden by the identity-based group signature scheme.

REFERENCES

[1] Meiko Jensen, Sven Schage, Jorg Schwenk "Towards an Anonymous Access Control and Accountability Scheme for Cloud Computing" 2010 IEEE 3rd International Conference on Cloud Computing.

[2] Safwan Mahmud Khan and Kevin W. Hamlen "AnonymousCloud: A Data Ownership Privacy Provider Framework in Cloud Computing" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[3] Zhusong Liu"A Secure Anonymous Identity-based Access Control over Cloud Data" 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies.

[4] R. Ranjit, D.Kayathri Devi"Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication" 2013 IJARCCE

[5] Lan Zhou, Vijay Varadharajan, Michael Hitchens"Trusted Administration of Large-Scale Cryptographic Role-based Access Control System" 2012 IEEE

[6] S.Kuzhalvaimozhi "Privacy Protection in Cloud Using Identity Based Group Signature" IEEE 2014

[7] Bharti Ratan Madnani, Sreedevi N "Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation" International Journal of Innovative Research in computer and Communication Engineering Vol. 1, Issue 3, May 2013

[8] Mostafa Hajivali, Faraz Fatemi Moghaddam, Maen T. Alrashdan, Abdualeem Z. M. Alothmani "Applying an Agent-Based User Authentication and Access Control Model for Cloud Server" ICTC IEEE,2013

[9] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" IEEE Transactions on Parallel and Distributed Systems, February 2014

[10] Junbeom Hur and Dong Kun Noh,Member, IEEE"Attribute-Based Access Control with Efficent Revocation in Data Outsourcing System"IEEE Tranasaction on parallel and distributed systems, VOL. 22, NO. 7, JULY 2011

[11] 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. 24, NO. 1, January 2013

[12] http://whatiscloud.com/cloud_deployment_models/index

[13] http://www.cloud-competence-center.com/understanding/cloud-computing-service-models/

[14] http://www.infoworld.com/article/2653764/database/microsoft-sql-server-2008-is-the-best-sql-server-yet.html

[15] http://gas.dia.unisa.it/projects/jpbc/docs/pairing.html#.VSeLxOLDR8A

[16] http://www.thoughtsoncloud.com/2014/08/quick-overview-openstack-technology/

[17] http://www.ibm.com/developerworks/cloud/library/cl-openstack-overview/

[18] http://arielsilverstone.com/cloud-computing-security/clearing-the-cloud-ii-cloud-computing-security/

[19] http://www.centre4cloud.nl/nl/kennis-ontwikkeling/definition-cloud-computing/deployment-models/

[20] http://sandeepkejriwal.com/2012/04/01/what-is-cloud-computing/