Data Security in Cloud Computing with Elliptic Curve Cryptography

Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi

Abstract: ***Cloud computing is one of today's hottest research areas due to its ability to reduce costs associated with computing while increasing scalability and flexibility for computing services. Cloud computing is Internet based computing due to shared resources, software and information are provided to consumers on demand dynamically. Cloud computing is one of the fastest growing technology of the IT trade for business. Since cloud computing share disseminated resources via the network in the open environment, hence it makes security problems vital for us to develop the cloud computing applications. Cloud computing security has become the leading cause of hampering its development. Cloud computing security has become a hot topic in industry and academic research. This paper will explore data security of cloud in cloud computing by implementing digital signature and encryption with elliptic curve cryptography.***

Index Terms: cloud computing, cloud security, data security, digital signature, encryption, elliptic curve cryptography.

I. INTRODUCTION

A cloud typically contains a virtualized significant pool of computing resources, which could be reallocated to different purposes within short time frames. The entire process of requesting and receiving resources is typically automated and is completed in minutes. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service. Share resources, software and information are provided to computers and other devices on demand.

It allows people to do things they want to do on a computer without the need for them to buy and build an IT infrastructure or to understand the underlying technology. Through cloud computing clients can access standardized IT resources to deploy new applications, services or computing resources quickly without reengineering their entire infrastructure, hence making it dynamic.

The core concept of cloud computing is reducing the processing burden on the users terminal by constantly improving the handling ability of the cloud. All of this is available through a simple internet connection using a standard browser.

However there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for people to shift to cloud computing.

II. RELATED CONCEPTS ABOUT CLOUD

A. DEPLOYMENT CLOUD MODELS

- Public cloud: the cloud infrastructure is made available to the general public people or a large industry group and provided by single service provider selling cloud services.
- Private cloud: the cloud infrastructure is operated solely for an organization. The main advantage of this model is the security, compliance and QoS.
- Community cloud: the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.
- Hybrid cloud: the cloud infrastructure is a combination of two or more clouds. It enables data application portability through load balancing between clouds.

B. CLOUD CHARACTERISTICS

- On demand service: cloud is large resource and service pool that you can get service or resource whenever you need by paying amount that you used.
- Ubiquitous network access: cloud provides services everywhere though standard terminal like mobile phones, laptops and personal digital assistants.
- Easy use: the most cloud provider's offers internet based interfaces which are simpler than application program interfaces so user can easily use cloud services.
- Business model: cloud is a business model because it is pay per use of service or resource.
- Location independent resource poling: the providers computing resources are pooled to serve multiple customers using multitenant model with different physical and virtual resources dynamically assigned and reassigned according to demand.

C. CLOUD SOLUTIONS

- Infrastructure as a service: it delivers a platform virtualization environment as a service rather than purchasing servers, software, data centers.
- Software as a service: it is software that is deployed over internet and or is deployed to run behind a firewall in your LAN or PC.
- Platform as a service: this kind of cloud computing provide development environment as a service. You can use the middleman's equipment to develop your own program and deliver it to the users through internet and servers.
- Storage as a service: this is database like services billed on a utility computing basis, e.g., gigabyte per month.
- Desktop as a service: this is the provisioning of the desktop environment either within a browser or as a terminal server.

Manuscript received on May 30, 2012

Veerraju Gampala, Information Technology, GMR Institute of Technology, Rajam, Andhra Pradesh ,India.

Srilakshmi Inuganti, Information Technology, GMR Institute of Technology, Rajam, Andhra Pradesh,India.

Satish Muppidi, Department of Information Technology, GMR Institute of Technology, Rajam, Andhra Pradesh, India.

III. CLOUD SECURITY CHALLENGES

The cloud services present many challenges to an organization. When an organization mitigates to consuming cloud services, and especially public cloud services, much of the computing system infrastructure will now under the control of cloud service provider.

Many of these challenges should be addressed through management initiatives. These management initiatives will requires clearly delineating the ownership and responsibility roles of both the cloud provider and the organization functioning in the role of customer.

Security managers must be able to determine what detective and preventative controls exist to clearly define security posture of the organization. Although proper security controls must be implement based on asset, threat, and vulnerability risk assessment matrices. Cloud computing security risk assessment report mainly from the vendor's point of view about security capabilities analyzed security risks faced by the cloud. Here are security risks list.

- Regulatory compliance: cloud computing providers who refuse to external audits and security certifications.
- Privileged user access: sensitive data processed outside the organization brings with it an inherent level of risk.
- Data location: when you use cloud, you probably won't know exactly where your data hosted.
- Data segregation: data in the cloud is shared environment alongside data from other customers.
- Recovery: even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster.
- Investigative support: investigating inappropriate or illegal activity may be impossible in cloud computing.
- Long term viability: you must be sure your data will remain available even after such an event.

IV. PROPOSED SECURITY SOLUTIONS

The cloud computing is a virtual environment that requires transfer data throughout the cloud. Therefore, several data storage concern can arise. Typically, users will know neither the exact location of their data nor the other sources of the data collectively stored with theirs.

To preserve security of your cloud-based virtual infrastructure, perform security best practice at both the traditional IT and virtual cloud. To ensure data confidentiality, authentication, integrity, and availability, the provider should include the following:

- Encryption: the sensitivity of data may require that the network traffic to and from the virtual machine be encrypted, using encryption at the host OS software.
- Physical security: keep the virtual system and cloud management hosts safe and secure behind carded doors, and environmentally safe.
- Authentication and access control: the authentication capabilities within your virtual system should copy the way your other physical systems authenticate. One time password and biometrics should all be implemented in the same manner. Also authentication requires while you are sending data or message from one cloud to other cloud. To provide message authentication we will use digital signatures.
- Separation of duties: as system get more complex, misconfiguration take place, because lack of expertise coupled with insufficient communication. Be sure to enforce least privileges with access controls and accountability.
- Configuration, change control, and patch management: this is very important and sometimes overlooked in smaller organizations. Configuration, change control, patch management, and updated processes need to be maintained in the virtual world as well as physical world.
- Intrusion detection and prevention: what's coming into and going out of your network has to know. A host based intrusion prevention system coupled with a hypervisor based solution could examine for virtual network traffic.

Among these proposed security solutions, we consider in this paper authentication and encryption for secure data transmission from one cloud to other cloud that requires secure and authenticated data with elliptic curve cryptography.

V. ELLIPTIC CURVES IN CRYPTOGRAPHY

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. An elliptic curve over a field K is a nonsingular cubic curve in two variables, f(x,y) =0 with a rational point (which may be a point at infinity). The field K is usually taken to be the complex numbers, reals, rationals, and algebraic extensions of rationals, p-adic numbers, or a finite field. Elliptic curves groups for cryptography are examined with the underlying fields of Fp

$$y^2 = x^3 + ax + b$$

(where p>3 is a prime) and F2m (a binary representation with 2m elements). An elliptic curve is a plane curve defined by an equation of the form

Consider elliptic curve

$$E: y^2 = x^3 - x + 1$$

If P1 and P2 are on E, we can define addition

$$P3 = P1 + P2$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

As shown in picture. Let P1=(x1, y1), P2=(x2, y2), P3=(x3, y3) and P1 not equals P2

$$m = \frac{y_2 - y_1}{x_2 - x_1};$$

To find the intersection with E. we get

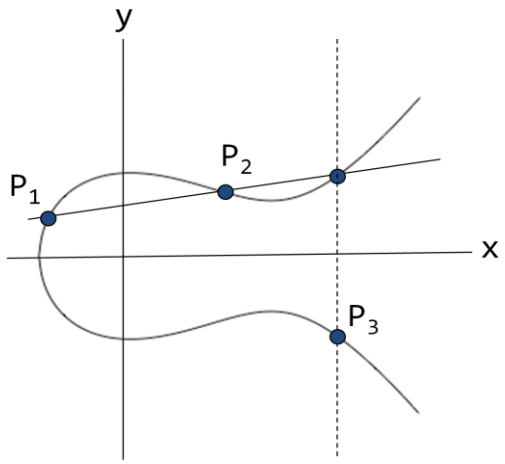
$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

$$or, 0 = x^3 - m^2x^2 + \ldots$$

$$So, x_3 = m^2 - x_1 - x_2$$

$$\Rightarrow y_3 = m(x_1 - x_2) - y_1$$

Multiplication is defined as repeated addition, for example: 3P=P+P+P.



Elliptic curve cryptography [ECC] is a public-key cryptosystem. Every user has a public and a private key. Public key is used for encryption/signature verification. Private Key is used for decryption/signature generation. Elliptic curves are used as an extension to other current cryptosystems. That is Elliptic Curve Diffie-Hellman Key Exchange and Elliptic Curve Digital Signature Algorithm.

VI. PROPOSED PROCEDURE TO ENHANCE DATA SECURITY IN CLOUD

Let us assume we have two organizations A and B. A and B act as public clouds with data, software and applications. A want to send data to B's cloud securely and data should be authenticated. We are here trying to send a secure data from A to B by applying digital signature and encryption to data with elliptic curve cryptography. Suppose B wants an XML document from A's cloud then B's user will place a request to A's user. A's user select corresponding XML document from A's cloud data storage and then apply the hash function, it will give message digest. Sign the message digest with his private key by using A's software. It is called digital signature. Encrypt digitally signed signature with B's public key using ECC algorithm. Encrypted cipher message will be send to B. B's software decrypt the cipher message to XML document with his private key and verify the signature with A's public key.

VII. PROPOSED ALGORITHM FOR DATA SECURITY USING ECC

Both clouds agree to some publicly-known data item.

a. The elliptic curve equation
   i. values of a and b
   ii. prime, p
b. The elliptic group computed from the elliptic curve equation
c. A base point, B, taken from the elliptic group

Key generation:

1. A selects an integer dA. this is A's private key.
2. A then generates a public key PA=dA*B
3. B similarly selects a private key dB and computes a public key
   PB= dB *B
4. A generates the security key K= dA *PB. B generates the secrete key K= dB *PA.

Signature Generation:

For signing a message m by sender of cloud A, using A's private key dA

1. Calculate e=HASH (m), where HASH is a cryptographic hash function, such as SHA-1
2. Select a random integer k from [1, n − 1]
3. Calculate r = x1 (mod n), where (x1, y1) = k * B. If r = 0, go to step 2
4. Calculate s = k − 1(e + dAr)(mod n). If s = 0, go to step 2
5. The signature is the pair (r, s)
6. Send signature (r, s) to B cloud.

Encryption algorithm:

Suppose A wants to send to B an encrypted message.

i. A takes plaintext message M, and encodes it onto a point, PM, from the elliptic group.
ii. A chooses another random integer, k from the interval [1, p-1]
iii. The cipher text is a pair of points
   PC = [(kB), (PM + kPB)]
iv. Send ciphertext PC to cloud B.

Decryption algorithm:

Cloud B will take the following steps to decrypt cipher text PC.

a. B computes the product of the first point from PC and his private key, dB
   dB * (kB)
b. B then takes this product and subtracts it from the second point from PC
   (PM + kPB) – [dB(kB)] = PM + k(dBB) – dB(kB) = PM
c. B cloud then decodes PM to get the message, M.

Signature Verification:

For B to authenticate A's signature, B must have A's public key PA

1. Verify that r and s are integers in [1, n − 1]. If not, the signature is invalid
2. Calculate e = HASH (m), where HASH is the same function used in the signature generation
3. Calculate w = s −1 (mod n)
4. Calculate u1 = ew (mod n) and

u2 = rw (mod n)

5. Calcúlate (x1, y1) = u1B + u2PA
6. The signature is valid if x1 = r(mod n), invalid otherwise.

VIII. CONCLUSION

Now a day's cloud computing facing many security challenges. Users put their data in the cloud and transfer from one cloud to another, the privacy of users at risk result from last control of data. Users most concerned about data security, so virtualization security and data security are the main problem of the cloud computing security. We concern here data security with Elliptic curve cryptography to provide confidentiality and authentication of data between clouds. In future we will concern more security issues of cloud computing and try to find better solutions using cryptography.

REFERENCES

1. Liu Peng, the definition and characteristics of cloud computing, http://blog.sina.com.cn/s/blog_5f0da5590100cmxw.html http://www.chinacloud.cn, March 9, 2009
2. Ya-Qin Zhang, the future of computing in the "cloud - Client", The Economic Observer reported, http://www.sina.com.cn, 2008 Nian 07 Yue 12 Ri 14:30
3. Jianfeng Yang and Zhibin Chen "Cloud Computing Research and Security Issues"
4. D. L. Ponemon, "Security of Cloud Computing Users," 2010.
5. C.Almond, "A Practical Guide to Cloud Computing Security," 27 August 2009 2009.
6. IBM, "Google and IBM Announced University Initiative to Address Internet-Scale Computing Challenges," http://www-03.ibm.com/press/us/en/pressrelease/22414.wss.
7. http://en.wikipedia.org/wiki/Cloud_computing
8. http://www.cloudcomputing china.cn/Article/luilan/200909/306.html
9. http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci 1287881,00.html
10. http://www.boingboing.net/2009/09/02/cloud-computing-skep.html
11. Google, "Google app Engine," http://code.google.com/appengine/.
12. http://cloudsecurity.trendmicro.com/

AUTHORS PROFILE

Veerraju Gampala B.tech,M.Tech is working as an Assistant Professor in the Department of Information Technology at GMR Institute of Technology in Rajam,Andhra Pradesh. His areas of interest are Cloud Computing and Network Security. He has 6 years of teaching experience. He presented 1 paper in International Conference and published 1 paper in National Conference and attended several workshops and FDPs.

I.Srilakshmi B.tech,M.Tech is working as an Assistant Professor in the Department of Information Technology at GMR Institute of Technology in Rajam,Andhra Pradesh. Her areas of interest are Network Security,Image Processing etc..She has 9 years of teaching experience. She presented 1 paper in International Conference and published 1 paper in National Journal and attended several workshops.

Satish Muppidi M.Tech., is working as an Assistant Professor in the Department of Information Technology at GMR Institute of Technology in Rajam, Andhra Pradesh. His areas of interest are Cloud Computing and Soft Computing. He has 4 years of teaching experience. He presented 3 papers in International Conference, presented 7 papers in National Conference and published 1 paper in International journal and attended several workshops and FDPs.