Enhancing Security of Cloud Computing using Elliptic Curve Cryptography

Abhuday Tripathi
MTech
Amity University
Lucknow

Parul Yadav
Sr.Lecturer
Amity University
Lucknow

ABSTRACT

Cloud computing is a form of distributed computing environment. It provides an environment where thousands of computers work in parallel to perform a job in much less times than traditional client server model. This parallelism happens because of low cost virtualization of hardware resources. Cloud computing abstracts the complexity of services provided to the user. In this article we have tried to explore various cloud computing model and how their security requirement differs from traditional computing model. We have analyzed various security risk associated with them, different ways to mitigate them and limitations of current cryptographic schemes. We have analyzed elliptic curve cryptographic schemes for cloud based applications in comparison to RSA based schemes. Here we have tried to give theoretical and experimental results to proof that elliptic curve based public key cryptography is far better than RSA based schemes. We have implemented ecdsa algorithm and compared its performance with RSA based algorithm in cloud. It supports our conclusion from the survey of cloud based applications.

General Terms

Network Security.

Keywords

Cloud computing, network security, cryptography.

1. INTRODUCTION

Cloud computing is an umbrella term which involves different types of technology like distributed computing ,parallel programming ,grid technologies etc .Cloud computing provides tremendous opportunity for small and medium scale enterprises to grow their business using IT services with zero deployment cost.

Several authors have defined cloud in various ways .NIST defines Cloud Computing**[1]** as," Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.".Here technical aspects of cloud computing has been shown.. According to Buyya[2] cloud can be defined as "A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers. ". Clouds offer high scalable, elastic and resilient services on a pay-as-you-use model which can be utilized by the business houses for growing their business to reduce their infrastructure cost and power saving. Cloud provides flexibility and portability to its users. Cloud based services are being used by small and medium scale enterprises to achieve greater speed in business processing and higher flexibility .Cloud Computing run on subscription based service model (pay as per you use) using internet as the infrastructure .Small and Medium Enterprises can set up the website and software on the cloud and hence get rid of the upfront infrastructure investments (cost incurred in purchasing and installing hardware, power and cooling cost and maintenance cost). This results in reduced cost of the services. Quality of services also gets better as the organization can spend the saved amount and time on improving it .With cloud based services innovative ideas can be easily implemented with reduced risk. Cloud based software are playing same role in IT industry that banks are playing in finance sector .Cloud can manage our data as bank manages our fund. Cloud Computing runs on virtualization technology where multiple operating systems runs on a server .Clouds supports multi tenancy where multiple organization's data are stored on a single server using virtualization technology. Cloud computing is growing very rapidly due to availability of high speed internet .Web browser can be used to access software deployed on cloud computing which earlier used to get installed on the desktop. So users are able to access the same service at less cost or sometime totally free. These causes lot of transaction to happen on the network and hence security issues also rise along with them. Although cloud computing has evolved a lot, it has not won complete confidence of its user and it's being used mainly for experimental and testing projects. There are various reasons behind it and one of them is security of data stored on the cloud.

In rest of paper we have analyzed the deployment and service model of the cloud. Then we go on to analyze the clients of cloud computing in section 2. In section 3 we have analyzed security issues of cloud computing. In section 4 we discuss simulation of elliptic curve cryptography. In section 5 we have conclusion and then we have reference in section 6.

1.1 Selection of cloud deployment model:

A cloud computing based services can be deployed in three ways [3].

*Public cloud***:** A service provider can host the cloud on its infrastructure and provide to other user for free or on pay-as-you-use-model. The user has to store its data outside its network so it cannot be used for storing private information. Multiple tenants may exist on the server which raises the security risk of data isolation. This is the most popular deployment model. Organizations like Google and Amazon provide services on this model.

Private Cloud: Private cloud is owned by a particular organization and only employees of the organization have the rights to access the cloud. Organizations have the freedom to define the protocol and access rights of its users though cloud could be managed by third party only. It's preferred for organization that have lot of sensitive data or government organizations

Hybrid Cloud: Hybrid cloud computing is mixed of public and private cloud. As public cloud can never be considered perfectly secure for sensitive data for them private cloud is used.

Community Cloud: It is very similar to grid computing were set of computers interoperates with each other to form network .

Private cloud has least security issues among the entire deployment model. They are completely owned by organizations. They are not multi-tenant in nature so they don't have privacy issues. These benefits come at the cost of investment on infrastructure and its maintenance. So they lack the major benefits that cloud computing can provide. On the other hand public cloud provides all kind of services and has maximum security issues and concerns. In this paper we are more concern about public cloud. If we can take care of public cloud, security issues of other kind of deployment model are taken care of.

1.2 Selection of Cloud Service Model

There are three different kinds of service model for the cloud [3].

Software-as-a-service: Software is deployed on cloud and delivered as a service using web browser or as web services. User need not worry about buying hardware and installing software on them. SaaS applications need not be installed on the local machine and user does not has to worry about its update and maintenance. With SaaS vendors makes the required software available to a business on subscription basis and charges are made on product usage. SaaS model can save both infrastructure cost and operational cost. Database can be deployed on cloud on SaaS model but privacy hinders users from adopting it. In case of SaaS security related issues are completely handled by the providers.

Platform-as-a-service: It is application development and deployment platform deployed on cloud and delivered as a service. It also provides application programming interface, database and middleware to its user. The provider is responsible for maintenance and control of the underlying cloud infrastructure including network server and operating system. PaaS service provides great deal of flexibility allowing companies to build PaaS environment on demand with no capital expenditure. In case platform as a service security issues are handled by the provider partially and user or organizations need to add layer of security from their side also.

Infrastructure-as-a-service: Delivery of hardware along with basic software as a service falls in domain of infrastructure as a service e.g storage as a service. With IaaS company can rent fundamental computing resource for deploying and running or storing data. It enables companies to deliver applications more efficiently by removing the complexity involved with managing their own infrastructure. IaaS enables fast deployment of applications and improves the agility of services by instantly adding computing processing power and storage capacity when needed e.g amazon ec2. Moreover server failure and network failure are taken care of by the vendors while security concerns arising out of applications and web services are managed by the user.

So before choosing between SaaS, IaaS and PaaS, organization need to understand it's need perfectly. If a software is used rarely it can be purchased on SaaS model from cloud based service provider. This will save the organization from paying huge sum of money as license fees. IaaS is good for small organization whose requirements for computers are of small duration. Cloud based storage are example of IaaS. They are useful for backup of data. PaaS based service are more consistently used. They are bought only for long term needs. All these service model have different kind of security issues.

So we can conclude form here that SaaS user are more encumber with security issues than PaaS user and IaaS user are least concerned about the issue. *Web services* along with web browser are used to deliver services deployed on cloud .

2. CLIENTS OF CLOUD COMPUTING

There are various kind of clients for cloud computing [3][4]. There are hardware client like thick client (full featured computer), thin client (designed for specific purpose mainly with i/o interface), mobile thin clients (phones with operating system which lets you access cloud from anywhere). Software clients include rich or fat client (desktop applications connected to internet), smart client (runs locally but installed over network), web applications/thin clients (they run on web browser like Google calendar). There are lots of resource sensitive clients of cloud computing like RFID. Figure 1 shows various kinds of clients of cloud computing along with services provided by the cloud.

Mobile devices are of various kind smart phones, notebooks, tablets etc .They all have less weights, memory and dependent on battery life. So application developed for them had to keep these constraints in mind. Cloud Computing can be used as savior for such application as some of the computation can be easily outsourced to the cloud .This can be implemented in two different ways. We can transfer the whole computation to the cloud or develop an application which uses cloud for some specific task.

These clients were considered useless in LAN environment. With the growth in internet speed and increase in computing power of Smartphone and tablets number of user who will access applications and services on cloud will increase exponentially. So the service provider needs to develop their applications keeping such facts in mind. Operating systems running on such clients are designed to conserve the battery life with networking support built in the operating system. They are of small sizes and capable of running in such environment. .

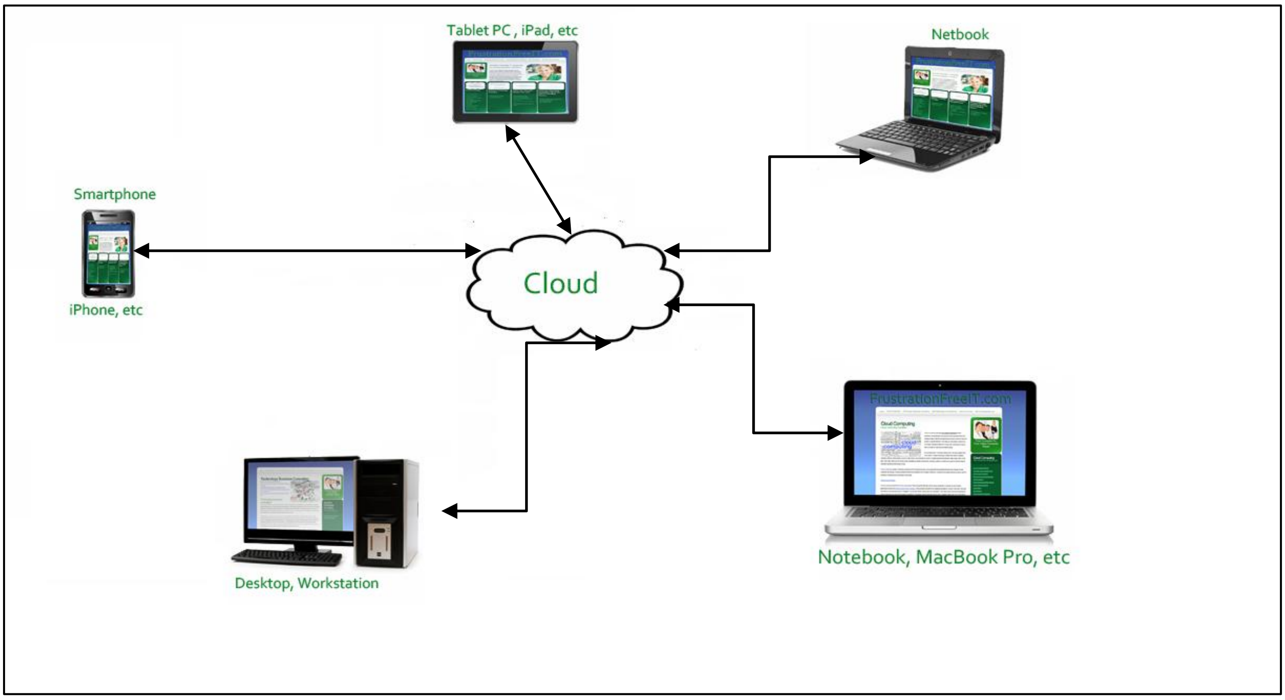

Figure 1: Clients of cloud computing.

3. SECURITY ISSUES OF CLOUD COMPUTING

A cloud computing based service faces various kinds of security challenges. An intruder can use the vulnerabilities of network infrastructure to attack the services on cloud .Characteristics of cloud like multi-tenancy; on demand self service, broad network access etc creates lot of vulnerabilities in the service delivered [5]. A survey conducted by IDC shows that security is major concern for the users staying away from the cloud [6]. In this section we analyze various kind of security challenges arise for applications deployed on cloud. They include both traditional security challenges and recent challenges which came into existence because of cloud computing [7][8][9]**.**

Security Risk due to network infrastructure: Network infrastructure raises several security issues with the service being provided. Distributed Denial of Service attacks are performed to prevent the server from providing service to its user by sending uncountable request. A system on cloud can be hacked and used as base to perform ddos attack on other machine. Attacker analyzes all packets passing through the system to gather important information's about the user. Port scanning[10] is done too find out the open port that can be used to get into the system. SQL injections are used to attack the cloud based database.

Security risk due to use of web services: Web services are vulnerable to several kinds of attacks. These vulnerabilities arise due to implementation mechanism and existing protocols in web services. There are as follows.

Buffer Overflows: Xml can be forced to call itself thereby overflowing the memory. This can trigger error message and hence application reveal information about itself

XML injections: XML injections can be used to insert a parameter into a sql query and let the server execute the data.

Sessions Hijacking: An attacker can hijack a soap message and obtain the session id thereby representing himself as an authenticated user to the server. Later on he can go on to perform some serious damage to server.

Security risk due to cloud characteristics: Security risk arises for services based on cloud due to its characteristics. Service user losses control over data as it is stored on other's server. It has to depend on the provider's security arrangement and its employees. A situation may arise where service provider might have to move to other provider or back to its server at different geographic location. Data stored on cloud gets locked in other's server and it's difficult to move them from one provider to another. Most of the cloud service provider support multi tenancy. Isolation of data from other organization's employee residing on the same server is also a challenge for the service provider. If client ceases to use the service provided than data ownership issues do arises as some provider refuses to release them. Availability of applications running on cloud is great concern for the user as cloud outages has happened several times gmail(one-day outage in mid-October 2008), Amazon S3(over seven-hour downtime on July 20, 2008) and FlexiScale(18-hour outage on October 31, 2008) **.**

Security issues of applications available through cloud: Applications deployed on cloud can face same kind of attacks as that on client-server model. SaaS based applications are vulnerable to the virus .Online operating systems are available on cloud to the user for free .Viruses can spread as attachments of email, of part of the software or can stay in MBR of the operating system available on cloud. Worms residing on one system in cloud can migrate to another system on its own. Trojan horse is software with wrong intentions. It gets divided into two parts when loaded from the memory.

SaaS applications depend on web services and web browser to deliver their services to user. They face security challenges arising out of network infrastructure and web services .IaaS and PaaS services are hardware dependent and face more, challenges arising out of characteristics of cloud computing, than SasS applications. Public key cryptography is one of the various ways to handle some of the issues. There are various kinds of public key cryptographic schemes. Elliptic curve cryptography is one of them

.

4. SIMULATION OF ELLIPTIC CURVE CRYPTOGRAPHY

It was proposed by Koblitz and Miller independently [11][12].IT gives same level of security as RSA and ElGamal cryptosystem gives but with smaller key size. In ECC discrete points on the elliptic curve over a finite field are used as a cyclic group. All type of public key cryptography based schemes can get implemented using elliptic curve cryptography. Elliptic curve cryptography gives same level of security as other cryptographic schemes provide but it has not gained same popularity. It is based on group theory and field theory. Its security is based on elliptic curve discrete logarithm problem [13].

Table1: Equivalent key size recommended by NIST

Type	ECC Key Size	RSA Key Size	Ratio
Type-1	112	512	1:5
Type-2	163	1024	1:6
Type-3	192	1536	1:8
Type-4	224	2048	1:9
Type-5	256	3072	1:12
Type-6	384	7680	1:20

Table-1 shows the comparison of ECC key size and equivalent RSA key size [13]. As the usage of cloud computing and computing power grows requirement of key size for RSA based public key cryptographic schemes will also grow. Clients of cloud computing are thin client. So they will find it difficult to handle huge computations. On the contrary key requirement of elliptic curve based computing dos not grow exponentially as shown in the Figure-2. We have implemented ECDSA algorithm and RSA algorithm in an environment similar to those available on cloud. We have used jdk1.6 and Bouncy Castle cryptographic service provider[14] to implement our system on windows operating system, Intel Celeron 1.86Ghz processor. Our simulation in figure -3 and figure-4 shows clearly that ECDSA score better than RSA as far as performance is considered. In Figure -3 key generation algorithm is compared. Figure -4 shows overall performance of two algorithms.

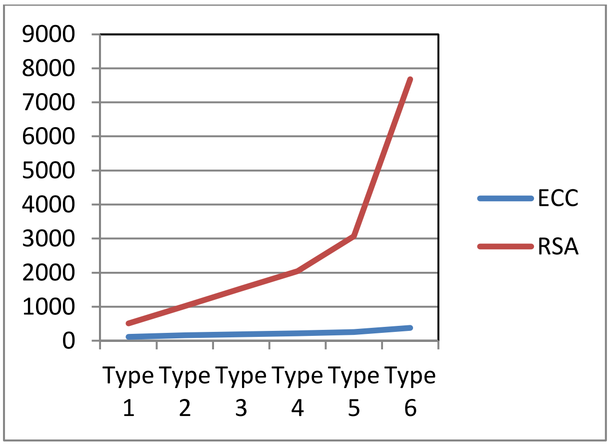

Figure 2: Comparison of growth in RSA and ECC key size

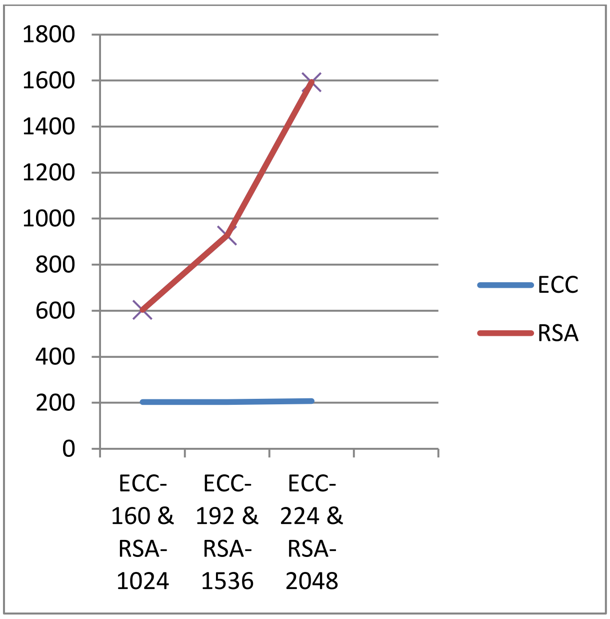

Figure 3: Key Generation Algorithm (ms)

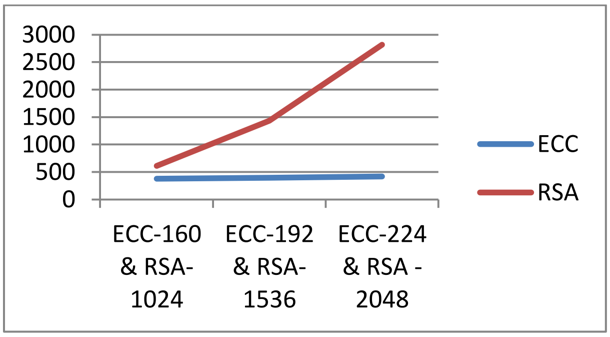

Figure 4: Digital Signature Algorithm

5. CONCLUSION AND FUTURE SCOPE

Cloud computing as a business model has great potential to change IT industry. As bandwidth availability grows more and more users will go to cloud for daily computer use as it abstracts the complexity of computing .Security is main concern which prevents large organization for using cloud. A service provider needs to ensure that applications are safe from all possible attacks. The experiments conducted indicate that ECC scores over RSA because of less key generation time and overall the difference increases with the growth in key size. As cloud computing grows popular, number of user will increase which would lead to increase in number of keys held at given point of time. Signature generation and verification time are almost same .Public key cryptography depends a lot on key generation algorithm hence ECC is better option than RSA where lot of user connects to cloud based application with small session time like cloud based storage offered free of cost while for application like Amazon web service, Google app engine etc each user create sessions of long duration so overall difference will appear to be less. As the growth in computing power happens the requirement of strong key size will also grow. Cloud based application uses lot of thin and dumb client which has very less battery power, they might not be able handle such huge computations. In such scenario elliptic curve based cryptography will come more useful. So we need to invest more effort and money to make elliptic curve cryptography more implementable and easier to understand.

Signature generation algorithm and key pair generation algorithm of ECDSA needs a random number to be generated. Using this random number as seed private keys is generated. Similarly secret integer 'K' generated during signature verification algorithm should also be random in nature. An attacker can exploit this vulnerability if the algorithm used to generate the random number is not cryptographically secure i.e. it should be unpredictable. So probability of any given value being selected should be very small. As a future scope of this work cryptographically secure random number should be included while generating private keys.

6. ACKNOWLEDGEMENTS

I would like to extend my gratitude to Mrs.Parul Yadav and Dr. Deepak Arora & Amity staff for providing various facilities during the study. I feel privilege to express my special thanks to my parents and all my friends for their deep affection and good wishes.

7. REFERENCES

[1] Peter Mell and Tim Grance. The NIST Definition of Cloud Computing, October 2009.

[2] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Bandic, I.: Cloud Computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer System 25(6), 599–616 (2009)

[3] Cloud Computing. http://en.wikipedia.org/wiki/Cloud_computing.

[4] Höfer, M. & Howanitz, G. The Client Side of Cloud Computing. Strategies 1-20 (2009).at http://www.embeddedcmmi.at/fileadmin/src/docs/teaching/SS09/SaI/Hoefer_Howanitz_Paper.pdf

[5] Jamil,Danish.Zaki ,Hassan. "Cloud Computing Security". In International Journal of Engineering Science and Technology.Vol.3 No.4April2011.

[6] Gens, F.New IDC IT Cloud Services Survey: Top Benefits and Challenges. In: IDC eXchange (2009), http://blogs.idc.com/ie/?p=730

[7] Narpat,S.Sekhawat et.al." Cloud Computing Security through Cryptography for Banking Sector".In Proc. 2011 5th National Conference.INDIACom-2011

[8] Foster, Ian et al. "Cloud Computing and Grid Computing 360-Degree Compared." 2008 Grid Computing Environments Workshop abs/0901.0.5 (2008) :1-10

[9] Dijk, Marten Van, and Ari Juels. "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing." Computing 305 (2010): 1-8.

[10] Jensen, M. et al., 2009. On Technical Security Issues in Cloud Computing. 2009 IEEE International Conference on Cloud Computing, 0(2009), p.109-116. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5284165.

[11] Miller, V.S. Use of elliptic curves in cryptography. *Advances in Cryptology: Crypto 85*, 417-426 (1986).

[12] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48, pages 203–209, 1987.

[13] SEC 1 Elliptic curve cryptography. Certicom Research. September 20 2000.

[14] Legion of the BouncyCastle, Bouncycastle, www.bouncycastle.org