Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Services using ECDSA in Cloud Computing

S.Sathish* *Computer Science and Engineering Jaisriram Group of Institutions, India*

D.Sumathi *Computer Science and Engineering PPG Institute of Technology, India*

P.Sivaprakash *Computer Science and Engineering PPG Institute of Technology, India*

Abstract— Cloud computing security is the set of control-based technologies and policies designed to comply to the rules and regulations framed by the provider team to support and protect information, data applications and infrastructure associated with cloud computing use. Cloud computing security process should address the issues faced by the cloud users. Cloud Service Provider needs to incorporate the maintenance activity in order to provide the customer's data security, privacy and compliance with necessary regulations. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a public key cryptosystem used for creation and verification of digital signatures in securing data uploaded by the cloud users. Information security concerns have been focused so that identifying unwanted modification of data, deletion of data is identified.

Keywords— Cloud Computing,ECDSA,Crptography,RSA,

I. INTRODUCTION

Cloud computing is internet-based computing, where by shared resources, software and information are provided to computers and other devises on demand. It is a culmination of numerous attempts at large scale computing with seamless access to virtually limitless resources.

Cloud Computing providers offer their services according to three fundamental models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) which is illustrated in *figure 1*. IaaS is a computing power that user can rent for a limited period of time. In PaaS model, cloud providers deliver a computing platform and/or solution stack typically including os, programming language execution environment, database, and web server. SaaS is a software delivery model in which software and associated data are centrally hosted on the cloud by independent software vendor or application service provider. In this paper discuss about The Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA combines the additional information security services of non-repudiation, authenticity, and integrity that digital signatures offer, with greater protection for a given key size compared with DSA.

Cloud Storage is a service where data is remotely maintained, managed, and backed up. The service is available to users over a network, which is usually the internet. It allows the user to store files online so that the user can access them from any location via the internet. The provider company makes them available to the user online by keeping the uploaded files on an external server. This gives companies using cloud service ease and convenience but can potentially be costly. Users should also be aware that backing up their data is still required when using cloud storage services, because recovering data from cloud storage is much slower than local backup.

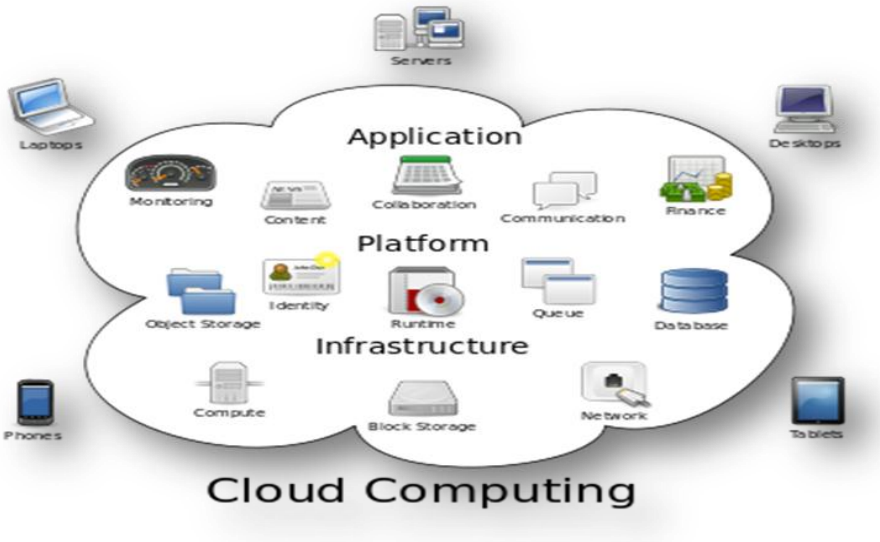

Figure 1: cloud computing service layers

A.**Characteristics and Services Models:**

The list of Services provided by cloud service provider based on National Institute of Standards and Terminology (NIST) are[16]:

- **On-demand self-service**: User can access services and they have a power to change cloud services through an online control panel or directly with the provider. And clients are billed with a monthly subscription or a pay-for-what-you-use scenario. Terms of subscriptions and payment will vary with each software provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The cloud enables clients to enter and use data with business management software hosted in the cloud at the same time, from any location, and at any time.
- **Rapid elasticity**: If anything, the cloud is flexible and scalable to suite client's immediate business needs. They can quickly and easily add or remove users, software features, and other resources.
- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

B. Fundamental Data Security Requirements

The following sections describe the basic security standards which technology must ensure:

- Integrity
- Availability
- Confidentiality

1)Integrity

A secure system ensures that the data it contains is valid. Data integrity means that data is protected from deletion and corruption, both while it resides within the database, and while it is being transmitted over the network.

2)Availability

A secure system makes data available to authorized users, without delay. Information is useless if it is not available. The unavailability of information is just as harm full for an organization as the lack of confidentiality or integrity.

3)Confidentiality

A secure system ensures the confidentiality of data. This means that it allows individuals to see only the data which they are supposed to see. Confidentiality has several different aspects, such as

- Privacy of Communications
- Granular Access Control
- Authenticated Users
- Secure Storage of Sensitive Data

Once it has been collected we can ensure that data remains private. Once confidential data has been entered, its integrity and privacy must be protected on the database and servers where it resides. Hence we are using encryption for securing data. Authentication is a way of implementing decisions about whom to trust. Authentication methods seek to guarantee the identity of system users.

C. Security Issues in Cloud Storage:

Cloud service providers request customers to store their account information in the cloud, where cloud service providers have the access to this information. This presents a privacy issue to the customer's privacy information[16].

1. Many SLAs have specified the privacy of the sensitive information however, it is difficult for customers to make sure the proper rules are enforced. There is a lack of transparency in the cloud that allows the customers to monitor their own privacy information.
2. When a customer decide to use multiple cloud service, the customer will have to store his/her password in multiple cloud, the more cloud service the customer is subscript to, the more copy of the user's information will be. This is a security issue for the customers and the cloud service providers.
3. The multiple copies of account will lead to multiple authentication processes. For every cloud service, the customer needs to exchange his/her authentication information. These redundant actions may lead to an exploit of the authentication mechanism.
4. Cloud service providers use different authentication technologies for authenticating users, this may have less impact on SaaS than PaaS and IaaS, but it is present a challenge to the customers

D. Secure stored data in Cloud Computing: The data should be securely encrypted when it's on the provider's servers and while it's in use by the cloud service[2]. Cloud providers assure protection for data being used within the application or for disposing of your data. Ask potential cloud providers how they secure your data not only when it's in transit but also when it's on their servers and accessed by the cloud-based applications.

E. **User access control.** Data stored on a cloud provider's server can potentially be accessed by an employee of that company, and you have none of the usual personnel controls over those people. The sensitivity of the data you're allowing out into the cloud. Manage your data and the level of access they have to it.

Elliptic curve cryptography (ECC) is a powerful technology that can enable faster and more secure cryptography across the Internet. It is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields. ECDSA offers a variant of the DSA which use ECC.

II. Cryptography

Cryptography is the art of science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible and then transforming that message back to its original form[7].

Encryption is the process of changing information in such a way as to make it unreliable by anyone except those possessing special knowledge (using keys) that allows them to change the information back to its original, readable format.

The modern field of cryptography can be divided into several areas of study. The chief once are

- Symmetric key cryptography
- Public key cryptography

A.Public key Cryptography

In public key cryptography, each person has a pair of keys: a public key and a private key. These are typically numbers that are chosen to have a specific mathematical relationship. In RSA, the public key is a large number that is a product of two primes, plus a smaller number. The private key is a related number. In ECC, the public key is an equation for an elliptic curve and a point that lies on that curve. The private key is a number. The private key can be used to create a digital signature for any piece of data using a digital signature algorithm. This typically involves taking a cryptographic hash of the data and operating on it mathematically using the private key. Anyone with the public key can check that this signature was created using the private key and the appropriate signature validation algorithm. A digital signature is a powerful tool because it allows to publicly vouch for any message.

A website certificate usually contains two things:

- **Identity information:** Typically who owns the certificate and which domains the certificate is valid for.
- **A public key:** The public half of a key pair, the site owner controls and keeps secret the associated private key. The certificate is digitally signed by a trusted certificate authority who validates the identity of the site owner.

Since the introduction of SSL by Netscape in 1994, certificates for web sites have typically used a public/private key pair based on the RSA algorithm. As the SSL specification evolved into TLS, support for different public key algorithms were added. One of the supported algorithms is ECDSA which is based on elliptic curves.

Despite the number of options available in TLS, almost all certificates used on the web today are RSA-based. Web sites have been slow to adopt new algorithms because they want to maintain support for legacy browsers that don't support the new algorithms. Even as late as 2012, out of 13 million TLS certificates found in a scan of the internet, fewer than 50 use an ECDSA key pair.

III. RSA VS ECDSA

The security of a key depends on its size and its algorithm. Some algorithms are easier to break than others and require larger keys for the same level of security. Breaking an RSA key requires factoring a large number[10]. We are pretty good at factoring large numbers and getting better all the time. Breaking an ECDSA key require to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP)[5]. The mathematical community has not made any major progress in improving algorithms to solve this problem since it was independently introduced by Koblitz and Miller in 1985.

This means that with ECDSA can get the same level of security as RSA but with smaller keys[13]. Smaller keys are better than larger keys for several reasons. Smaller keys have faster algorithms for generating signatures because the math involves smaller numbers. Smaller public keys mean smaller certificates and less data to pass around to establish a TLS connection. This means quicker connections and faster loading times on websites.

According to the ECRYPT II recommendations on key length, a 256-bit elliptic curve key provides as much protection as a 3,248-bit asymmetric key[12]. Typical RSA keys in website certificates are 2048-bits. If we compare the portion of the TLS handshake that happens on the server for 256-bit ECDSA keys against the cryptographically much weaker 2048-bit RSA keys

Cloud service providers request customers to store their account information in the cloud, cloud service providers have the access to these information. This presents a privacy issue to the customer's privacy information[6].

Many SLAs have specified the privacy of the sensitive information, however, it is difficult for customers to make sure the proper rules are enforced. There is a lack of transparency in the cloud that allows the customers to monitor their own privacy information.

When a customer decide to use multiple cloud service, the customer will have to store his/her password in multiple cloud, the more cloud service the customer is subscript to, the more copy of the user's information will be. This is a security issue for the customers and the cloud service providers.

The multiple copies of account will lead to multiple authentication processes. For every cloud service, the customer needs to exchange his/her authentication information. These redundant actions may lead to an exploit of the authentication mechanism.

Cloud service providers use different authentication technologies for authenticating users, this may have less impact on SaaS than PaaS and IaaS, but it is present a challenge to the customers.

IV. ECDSA

The elliptic curve digital signature algorithm is the elliptic curve analogue of DSA and serves the same purposes of key generation, signature generation, and signature verification[1]. ECDSA was first proposed in 1992 by Scott Vanstone in response to NIST's proposal of DSS[9]. It was later accepted in 1998 as an ISO standard (ISO 14888-3), as an ANSI standard (ANSI X9.62) in 1999, and as an IEEE standard (IEEE 1363-2000) and as a NIST standard (FIPS 186-2) in 2000.

A.Security of ECDSA

The generation of the public key in ECDSA involves computing the point, Q, where $Q = dP$. In order to crack the elliptic curve key, adversary Eve would have to discover the secret key d*[3]*. Given that the order of the curve E is a prime number n, then computing d given dP and P would take roughly $2^{n/2}$ operations. For example, if the key length n is 192 bits (the smallest key size that NIST recommends for curves defined over GF(p)), then Eve will be required to compute about 2^{96} operations[11]. If Eve had a super computer and could perform one billion operations per second, it would take her around two and a half trillion years to find the secret key. This is the elliptic curve discrete logarithm problem behind ECDSA[4].

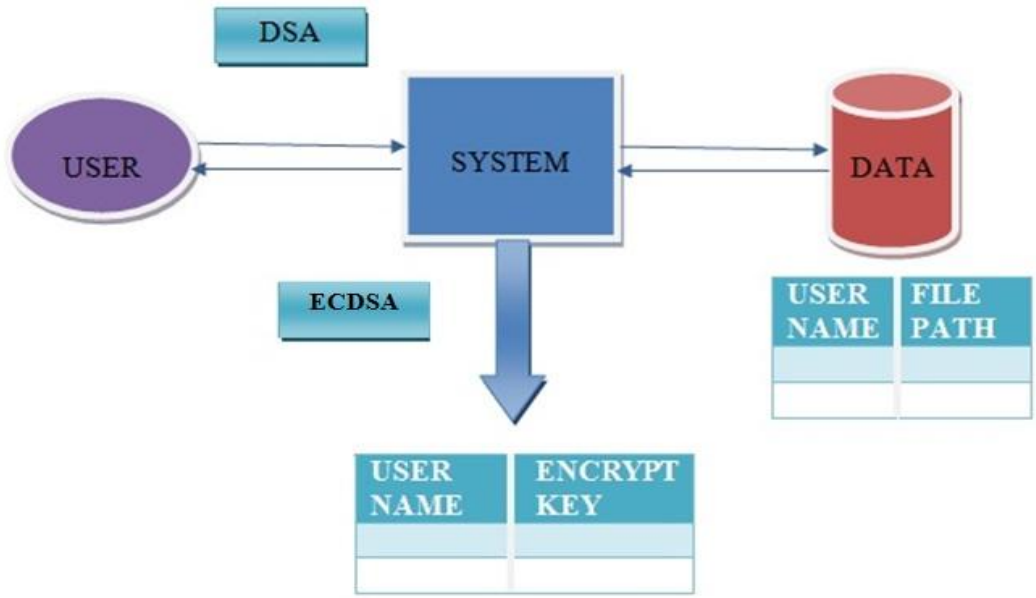

Figure 2: 3-tier architecture for data integrity

B.Key Pair Generation Using ECDSA

Let A be the signatory for a message M. Entity A performs the following steps to generate a public and private key[15]:

Select an elliptic curve E defined over a finite field F_p such that the number of points in $E(F_p)$ is divisible by a large prime n.

1. Select a base point, P, of order n such that $P \in E(F_p)$
2. Select a unique and unpredictable integer, d, in the interval [1, n-1]
3. Compute $Q = dP$
4. Sender A's private key is d
5. Sender A's public key is the combination (E, P, n, Q)

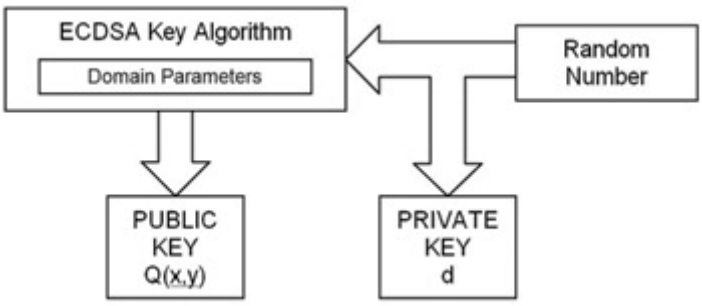

Figure 3: key pair generation process

C. Signature Generation Using ECDSA

Using A's private key, A generates the signature for message M using the following steps[16]:

1. Select a unique and unpredictable integer k in the interval [1,n-1]
2. Compute $kP = (x_1,y_1)$, where x_1 is an integer
3. Compute $r = x_1 \bmod n$; If $r = 0$, then go to step 1
4. Compute $h = H(M)$, where H is the Secure Hash Algorithm (SHA-1)
5. Compute $s = k^{-1}\{h + dr\} \bmod n$; If $s = 0$, then go to step1
6. The signature of A for message M is the integer pair (r,s)

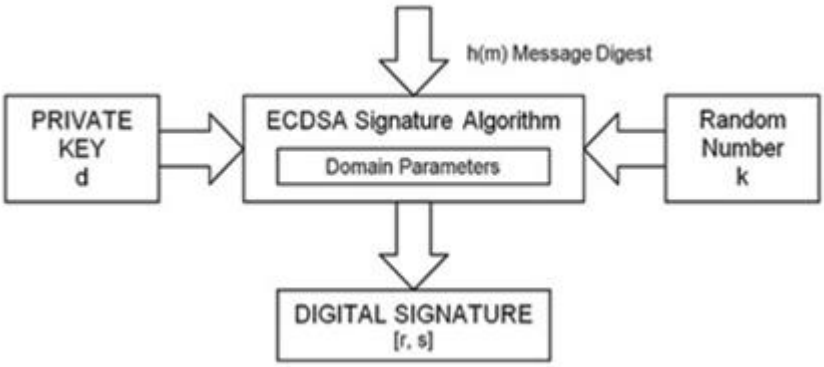

Figure 4: signature computation process

When compared to RSA, ECC offers the same security with smaller bit sizes. The following table taken from "Recommendation for Key Management: General Revised", NIST Special Publication 800-57, National Institute of Standards and Technology, May 2006, compares the bit sizes of ECC and RSA at similar security levels[8].

Table 1 Comparison of RSA and ECC

Bits of security	Symmetric key algorithm	FFC(eg., DSA,DH)	ECC(e.g.,ECDSA)
80	2TDEA	L=1024 N=160	f=160-223
112	3 TDEA	L=2048 N=224	f=224-255
128	AES-128	L=3072 N=256	f=256-383
192	AES-192	L=7680 N=384	f=384-511
256	AES-256	L=15360 N=512	f=512+

V. Conclusion:

Cloud computing has brought new challenges and opportunities for authentication. Security in the cloud should be the primary step for defense of an integrated security strategy. There is increasing demand for usable authentication to access services and data for both enterprises and consumers. At the same time, the cloud provides abilities such as centralized analysis and monitoring, and potential for new and more accurate authentication techniques. Most of the signature schemes are based on Elliptic Curve. The Elliptic Curve based on signature scheme is called as ECDSA. We propose a new variant ECDSA scheme that will produces the high level security with the help of parameters. Advantages of elliptic curves is fast access, less memory used and key size is less.

References

[1] Don Johnson, Alfred Menezes and Scott Vanstone,"The Elliptic Curve Digital Signature Algorithm(ECDSA),International journal of information security (2001),36-63.

[2] Kawser Wazed Nafi, Tonny Shekha Kar et al "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security Architecture", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3 , No. 10, 2012.

[3] http://www.embedded.com/design/safety-and-security/4427811/Using-the-Elliptic-Curve-Digital-Signature-Algorithm-effectively.

[4] Aqeel Khalique, Kuldip Singh, Sandeep Sood, "Implementation Of Elliptical Curve Digital Signature Algorithm", International Journal Of Computer Application (0975-8887) Volume 2- No.2, May 2012.

[5] Miller, V.,1985 Use of Elliptic Curve in Cryptography, CRYPTO 85, Springer-Verlag New York, Inc. New York, NY, USA ©1986 .

[6] Gary Anthes, "Security in the cloud," In ACM Communications (2010), vol.53, Issue11, pp. 16-18.

[7] William Stallings, "Cryptography and Network Security: Principles and Practices", Third Edition, Pearson Education, 2006.

[8] http://www.google.com/patents/EP2076799A1?cl=en
[9] ANSI X9.62,"Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm(ECDSA)",1999.
[10] http://blog.cloudflare.com/ecdsa-the-digital-signature-algorithm-of-a-better-internet
[11] Nesrine Kaaniche, Aymen Boudguiga, Maryline Laurent,"ID-Based Cryptography For Secure Cloud Data Storage", Multimedia Information Networking And Security (MINES), international conference 2010, 851-855.
[12] ANSI X9.63," Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Key Agreement and Key Transport Protocol, working draft, August 1999.
[13] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres1, Maik Lindner, "A Break in Clouds: Towards a cloud Definition," ACM SIGCOMM Computer Communication Review, vol. 39, Number 1, January 2009, pp. 50-55.
[14] I.Blake , G.Serioussi and N.Smart, "Elliptic Curve in Cryptography", Cambridge University Press,1999.
[15] Navneet Randhawa, and Lolita Singh, "A Systematic Way to Provide Security for Digital Signature Using Elliptic Curve Cryptography" IJCST Vol. 2, Issue 3, September 2011.
[16] Kuyoro S. O, Ibikunle F, Awodele O, "Cloud Computing Security Issues and Challenges" International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011.

