International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

ECDSA Algorithm for Cloud Security

B.Gahani Nath, B.B.V.Satya varaprasad, K.Sai Manidhar, Sridevi Sakhamuri

Abstract: ***Cloud computing is the provision of a variety of computing services—servers, databases, storage, programming, network etc—over the Internet ("the cloud") to offer quicker development, adjustable resources and economies of scale. You just pay for what you use, helping bring down your working costs, run your framework on the go effectively and scale up your resources as your business grows.***
Keywords: Cloud computing, server, database, network

I. INTRODUCTION

Cloud data security is fundamental, as you should be confident that your information is protected while its in the cloud. Various prominent hacking cases imply that this issue is topical for some owners, yet your information is a lot more secure in the cloud, and security is an incredibly high need for all distributed cloud storage users and providers. Cloud security is critical for both business and individual clients. Everybody needs to realize that their data is protected and secure and organizations have legitimate commitments to keep customer information safe, with specific segments having increasingly stringent standards about data storage.
Security is a fundamental component of your cloud, and you should check that your cloud provider has the required level of protection to meet your requirement.

II. BASIC REEQUIPMENTS FOR DATA SECURITY :

The following points must be ensured to secure data completely:
• Integrity
• Availability
• Confidentiality

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
B.Gahani Nath*, B.Tech Student, Department of Electronics& Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
B.B.V.Satya varaprasad, Asst.Professor, Department of Electronics& Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
K.Sai Manidhar, B.Tech Student, Department of Electronics& Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
Sridevi Sakhamuri, Asst.Professor, Department of Electronics& Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India

1)Integrity
A safe setup should guarantee the information is legitimate. Data integrity implies that information is shielded from both erasure and corruption, while stays inside a database. Also, the data must be secure while being transferred over a network.
2)Availability
The data that is protected should always be available to the authorized users. It is useless to store the information if it is not accessible to the users when needed without any delay.
3)Confidentiality
A secure system guarantees the privacy of information. It enables people to see just the information which they should see.

III. BASICS OF ELLIPTIC CURVE

1) Prime field:

For a prime field elliptic curve, the condition is Fq = y2 (modulo q) = x3 +a× b+x also 4a3 +27b2 (modulo q) is never equal to zero. The components in the limited field are the whole numbers in between 0 and q-1. All activities, for example, (-, +, / and augmentation) are in range of 0 and q-1. The prime q is picked with the end goal of securing the entire cryptosystem using the elliptic curves.

2) Binary field:

In a double field F2, m can be calculated by y2 + x and y= ax2+x3+ b, where b is never equal to 0. The components of the finite field are whole numbers. These components are picked with the end goal that size of individual ought to be at maximum m bits. These digits can be seen as a twofold polynomial with a degree of m-1. Either 0 or 1 must be the coefficient in a twofold poly. A poly with a degree of m-1 or lower must be picked in every task that is chosen. It is picked with the end goal that there is majority of the focus on the elliptic curves and final make the entire cryptosystem safe and secure.

3) Elliptic Curve Group:

The expansion of points is considered as a gathering activity, an added substance gathering which comprises of the arrangement of arrangements with the elliptic curve condition and an excellent point O called point-at-unendingness is framed. It is outstanding that E/Fq with a parallel task, called expansion of focuses and signified by addition operator (+), is an Abelian amass with O∞ as the personality component. The gathering is signified with E(Fq).

4) **Generating Point**: The generation of public and private keys are the important aspect in this cryptography. Also, the other main focus is to produce an elliptic curve in every possible direction. The request of every single base point has to be equivalent to n where n is sum of focuses for a specific e curve. Assume the point G is in E (Fq), and assume G has a prime request n, at that point, the cyclic added substance subgroup of E(Fq) created by P will be P = {O, G, GP, GP... (n - 1)G}.

IV. Operations on Elliptic Curves:

1) Point Addition: A 3rd point R can be obtained on the curve using two known points say P and Q. The image ' + ' speaks to the addition of elliptic curves P3 = P1 + P2.

2)Multiplication: A whole number e can be multiplied with a point P (e x P) on the elliptic curve using some set of rules. This is practically equivalent to adding P to itself e number of times and this gives a new point on the curve which results in e X P.

In Elliptic curve operations, the following points are to be focused. In order to obtain the sum of 2 points P and Q, draw a line joining those 2 points. This line will intersect the curve at one more point E, which is the sum of P, Q.

In Some cases , the above operation wont be possible. One such case is when both P, Q are exact same point. Then you have to extend the digression line and locate the point where the extended line touches point E. This point will be P*P. Another example for the above operation to be invalid is when the line joining the points p and q is straight up. For this situation, Q+P considered as new point O, Any point passing through O is always vertical. Furthermore, the impression of O about the x-pivot results in O. Think about a point P (xp, yp) on elliptic curve E. To decide 2P, P is multiplied. This ought to be a relative point on EC.

Condition of the digression at point P is: S = [(3xp 2 + a)/2yp] (mod p) At that point 2P has relative directions (xr, yr) given by: xr = (S2 - 2xp) mod p and yr = [S (xp - xr) - yp] (mod p) Presently 3Pcan be controlled by point addition of focuses P and 2P, treating 2P=Q. P has organizes (xp,yp) and Q=2P has organizes (xq,yq). Presently the incline is: S = [(yq-yp)/(xq-xp)] mod p P+Q = - R xr = (S2 - xp - xq) mod p yr = (S (xp - xr) - yp) mod p.

In this manner P*k is determined using progression of point-multiplication, addition.

V. Cryptography:

Cryptography is the art of encrypting a message or data while transferring or storing the data so that it is unreadable by hackers. The message/data is transferred back into its original form when an authorized user requests to view the data. There are several types of cryptography, but the major ones are:

1) Symmetric key cryptography
2) Public Key Cryptography

1.Public key cryptography:

In this type of cryptography, every individual two keys in which one is public and the other one is private. These keys are just numbers which are mathematically related to each other in some form. In RSA, the public key is generated by adding two prime numbers with a smaller number. This public key is generally a very huge value. The public key always lies on the curve in ecc.

Private key can is used to make a computerized mark which is called a digital signature to request any information using an algorithm called ECDSA.

VI. The ECDSA Algorithm

The concept of ECDSA was proposed by Scott Vanstone in the year 1992.Using ECDSA, we obtain the exact same level of security like RSA but the key size in ECDSA is very small when compared to RSA. Due to this, the calculation and computation will be much faster, also the public keys will be smaller to pass around. There are three steps involved in for the ECDSA algorithm:

1. **Key pair generation**
2. **signature generation**
3. **Verification of the signature**

The digital signature is generated by a hash function. The sender transmits the encoded message/data with the signature attached to any message/data. The receiver verifies the signature by using the public key of the sender and the domain parameters. Prime q of the limited field Fq, The elliptic curves condition E , the Point P which is on the curve and n are considered as domain parameters in ECDSA. The private key is generated in range [1, n-1].P is multiplied with the private key d will give us the relating public key Q. The pair (Q, d) is the key pair which is necessary in performing further operations using the ECDSA. The point G (Generating point) and the parameters of curve a and b and few more constraints gives us the space parameters for the elliptic curve. The Receiver selects a random point on the elliptic curve through which he generates his public key. The private key is added with the generation point and the public key.

VII. Generation of Key Pair

The public key can be generated using the following steps:

A. *Key Pair generation:*

1) Choose a random number (integer) in between p 0 to n-1.
2) Using point multiplication function, obtain Q = G*d.
G and Q are two different points on the curve.
3) we now have generated a key pair (d,Q) in which d denotes private key and Q denote the public key

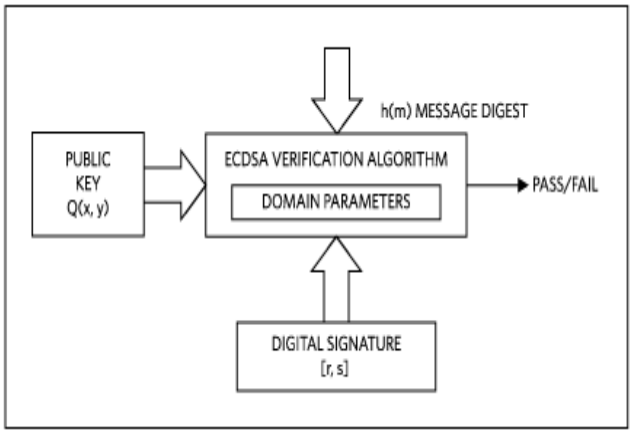
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

B. *Generation of Signature*

Using the private key and the domain parameters, the senders makes a signature for his message M through the following steps:
1)A random integer k is chosen with the condition $1 \leq k \leq n -1$.
2) k*G = (x1, y1) and r=x1 modulo n. when r = 0 then repeat the above step again.
3) calculate K-1mod (n).
4) Calculate z =(M)2*(h-1)
5) Calculate s = (z + d*r)*k-1 mod of n. If s tends to be zero the repeat the 1st step.
6) (r,s) will be the signature for the hashed message which was sent,

C. *Signature verification*

The receiver can verify the originality of the message sent by the following these steps:
1) Make sure that r and s are integers and lie between 1 and n-1.
2) Find z=h-1(M).
3) calculate w =s-1mod (n).
4) Compute u1= w*z mod (n) and u2 = w*r mod (n).
5) Calculate X= u2Q u1G+. Reject the signature if X is equal to infinity.
6) IF NOT, find v=x1mod (n) where X =(x1, y1).
7)The signature is only valid and can be accepted if v is equal to r (v=r).



VIII. Key Size Comparisons:

ECC KEY SIZE (Bits)	RSA KEY SIZE (Bits)	KEY SIZE RATIO	AES KEY SIZE (Bits)
163	1024	1 : 6	
256	3072	1 : 12	128
384	7680	1 : 20	192
512	15 360	1 : 30	256

Algorithm	Encryption Time	Key Strength
RSA	4ms	Less than 2ms
ECDSA	71ms	33ms
RSA	3ms	5ms
ECDSA	63ms	70ms
RSA	7ms	4ms
ECDSA	41ms	92ms

IX. ECDSA Performance

The performance of the ECDSA is depends on how good we implement the point multiplication concept. The points chosen to be multiplied has to be greater for a higher level of security We need both ‘k’ and ‘dA’-
(A random number and a Private key respectively) to find the signature but to verify it only the public key is sufficient. (R and Qa). One good feature of ECDSA is the trap door function of the ECDSA point multiplication. This will prevent intruders to find the random number and private key, even by knowing the public key or digital signature. Therefore ECDSA is very much secured. The signature cannot be faked, and the private key cannot be found or predicted.

Key Generation			
Key Length (bits)		Time (secs)	
ECC	RSA	ECC	RSA
163	1024	0.08	0.16
233	2240	0.18	7.47
283	3072	0.27	9.80
409	7680	0.64	133.90
571	15360	1.44	679.06

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Signature Generation			
Key Length (bits)		Time (secs)	
ECC	RSA	ECC	RSA
163	1024	0.15	0.01
233	2240	0.34	0.15
283	3072	0.59	0.21
409	7680	1.18	1.53
571	15360	3.07	9.20

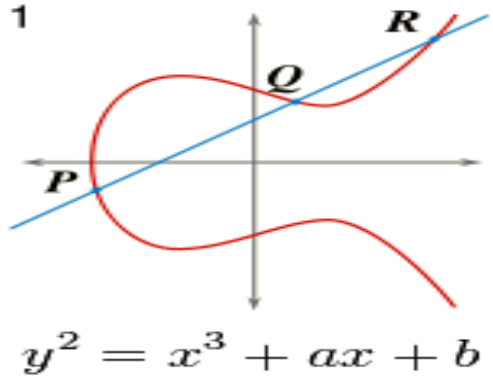
Signature Verification			
Key Length (bits)		Time (secs)	
ECC	RSA	ECC	RSA
163	1024	0.23	0.01
233	2240	0.51	0.01
283	3072	0.86	0.01
409	7680	1.80	0.01
571	15360	4.53	0.03

X. WORKING:

The general form of an elliptic curve is:

$y2 = x3 + ax + b$

The values a and b are used to find the shape of the curve. ECC uses curves over the finite field to lock the message/data which can only be unlocked using a private key. The larger the key size, the larger the curve, and the harder to break.



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

XI. CONCLUSION:

Cloud computing has brought many new opportunities and challenges for authentication. Securing a cloud system must be a major security challenge in the current days. The number of users utilizing cloud technology are increasing day by day. All the users must be ensured that their data is private and secure. The cloud provides potential for new authentication methods like the ECDSA which we propose. The ECDSA gives a top-level security and can be used with different parameters. Also, elliptic curves have the advantages like small key sizes, low memory utilization and a faster access. ECDSA gives some benefits like smaller key sizes but with the same level of security. This feature will also make it useful when a hardware needs to be secured.

REFERENCES:

1. An Elliptic Curve Cryptography based Authentication and Key Agreement, Oregon State University, 1998.'
2. Implementation of Elliptic Curve Digital Signature Algorithm, International Journal of Computer Applications, May 2010.
3. Comparison of ECC and RSA Algorithm in Resource Constrained Devices Mohsen Bafandehkar, Sharifah Md Yasin, Ramlan Mahmod, Zurina Mohd Hanapi
4. A COMPARATIVE ANALYSIS OF ECDSA V/S RSA ALGORITHM AMANPREET KAUR1, VIKAS GOYAL
5. International Journal of Embedded systems and Applications(IJESA) Vol.5, No.2, June 2015 DOI : 10.5121/ijesa.2015.5202 15 COMPARISON AND EVALUATION OF DIGITAL SIGNATURES
6. Federal Office for Information Security, "Technical Guideline TR-03111 Elliptic Curve Cryptography Version 2.0", Germany, 2012.
7. Kessler G. C, "An Overview of Cryptography", 2014.
8. ECC-Based Threshold Digital Signature Scheme without a Trusted Party Qingqi Pei and Jianfeng Ma
9. Performance and Security of ECDSA by Sharon Levy
10. Shweta Lamba, Monika Sharma. "An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA)".

AUTHORS PROFILE

B.Gahani Nath is a UG Student in K L University and belongs to the branch Electronics and Computer Engineering. His areas of interests are cyber security and game development.

Mr. B.B.V.SatyaVara Prasad is working as an Assistant Professor in Department of Electronics and Computer Engineering in Koneru Lakshmaiah Education Foundation. He presented the several research papers in reputed international journals and he attended several national and international conferences. His area of interest is Computer Networks&Security,IoT and Data mining

.

K.Sai Manidhar is a UG Student in K L University and belongs to the branch Electronics and Computer Engineering. His areas of interests are cyber security and coding.

Ms. Sridevi Sakhamuri is working as an Assistant Professor in Department of Electronics and Computer Engineering in Koneru Lakshmaiah Education Foundation.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)