International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 8, August-2018

SECURING SENSITIVE DATA IN THE CLOUD BY USING ONE TIME PASSWORD FOR IMPLEMENTING N-CLOUD TECHNOLOGY

M.Thangam[#1,] *Mr.S Muruganandam* [#2]

M.Phil (full-time) Research Scholar, Assisstant Professor,
PG and Research Department of Computer Science,
Vivekananda College of Arts and Sciences for Women (Autonomous),
Elayampalayam, Tiruchengode, Namakkal, Tamilnadu, India.

ABSTRACT

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). One of most important revolution in data storage and it's retrievability in IT world is emerged in the form of Cloud Computing. Cloud computing have large impact over IT industry. In new existence, Elliptic Curve Cryptography (ECC) has involved the concentration of researchers and produce developers since of its tough mathematical structure and highest security in comparison to other existing algorithms like RSA (Rivest Adleman and Shameer Public key Algorithm).

Key word: Ecdsa, Ecc, Signature schemes, cloud authentication; multi-clouds; one time password

I. Introduction

Cloud storage system is becoming the world's one of simple, fine and popular technology because of data storage on one point from anywhere and we can interact with that data easily from everywhere [1][2]. It was accepted in 1999 as an ANSI standard and in 2000 as IEEE and NIST standards. It was also accepted in 1998 as an ISO standard and is under consideration for inclusion in some other ISO standards. Cloud computing is used upon huge amount of data and processing over that data by various application because cloud computing provides such environment to user [4]. The idea of information security leads to the evolution of Cryptography. Cryptography is the science of keeping information safe. In the mid-1980s, Miller and Koblitz introduced elliptic curves into cryptography, and Lenstra demonstrated how to employ elliptic curves to factor integers demonstrated how to employ elliptic curves to factor integers. The term „cloud computing‟ is made up of two terms, cloud and computing. Cloud could be thought to be synonymous with the Internet where various resources are interlinked with the use of network. One can use the resource they want with the help of simple client-server architecture. The term computing refers to processing. Cloud computing is computing on various resources over the network. In cloud computing Infrastructure, Platform and Application/Software are delivered as service over the network. Use of cloud computing is increasing day by day in many industrial areas[3]. Cloud Storage Service (CSS) gives benefit over managing and maintaining data manually [4]. A Cloud Storage System ensures that user gets the file which user has demanded for i.e. user is able to retrieve the data they want [5].

Different Techniques Involved in Authentication:

Current authentication methods can be classified as follows:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used. Many token based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used with a PIN number.

Different Techniques Involved in Generation of One Time Password

One time password can be generated in any of the two ways:

Time-synchronized OTP: In time-synchronized OTPs the user should enter the password within a certain period of time else it gets expired and another OTP must be generated. A counter-synchronized OTP: With counter-synchronized OTPs, a counter is synchronized between the client device and the server. The device counter is advanced each time an OTP is request

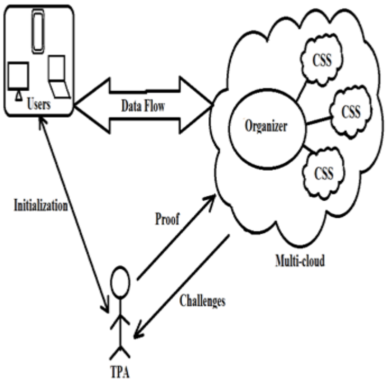

Fig. 1 Multi-cloud Architecture

II. Literature survey

Elliptic curves are Cubic curves. Elliptic curves are called elliptic because of their rapport with elliptic integrals in mathematics which can be used to determine the length of arcof an ellipse. These may be defined as a set of discrete points on the co-ordinate plane, satisfying the equation of the form,y2 [+xy] = x3 + ax2 + b (mod p) [6] The square bracket means that the term is optional. x and y are variables, a and b are constants. Each assessment of 'a' and 'b' gives a diverse elliptic curve. An elliptic curve in its "standard form" is illustrated by y2 = x3 + a×x + b for some fixed values of parameters 'a' and 'b'. This equation is also referred as Weierstrass equation of characteristic 0. The values that the objects x, y, 'a' and 'b' can acquire are meant to be drawn from a set that must be, at least a ring with a multiplicative identity element. The characteristic of such a ring is the number of times identity element multiplicative must be added in order to get the additive identity element. Consider a point P (xp, yp) on elliptic curve E. To determine 2P, P is doubled. This should be an affine point on EC.

DIGITAL SIGNATURE SCHEMES:

Digital signature schemes are designed to provide the digital counterpart to handwritten signatures (and more). A digital signature is a number dependent on some secret known only to the signer (the signer's private key), and, additionally, on the contents of the message being signed. Signatures must be verifiable – if a dispute arises as to whether an entity signed a document, and unbiased third party should be able to resolve the matter equitably, without requiring access to the signer's private key.

SECURITY:

A digital signature scheme should be existentially unforgeable under chosen-message attack.

III. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

The steps involved in ECDSA are formation of key-pair, signature-generation and signature-verification [3]. The digital signature is typically created using the hash function.. The transmitter sends the encrypted data along with signature to the receiver. The public key is a point on the curve and the private key is a random number selected by signer. The public key is obtained by multiplying the private key with the generating point on the curve [4]. There are certain cases for which this definition will not suffice.

One such case is where P and Q are the same point. In this case, draw the tangent line to E at P and find the second point where this line intersects E. Call this point P × P. Again, reflection of this point over the x-axis is P + P. Another case is where the line connecting P and Q is vertical. There are certain cases for which this definition will not suffice. One such case is where P and Q are the same point. In this case, draw the tangent line to E at P and find the second point where this line intersects E. Call this point P × P. Again, reflection of this point over the x-axis is P + P. Another case is where the line connecting P and Q is vertical.

A. Key-Pair generation

Given generating point G, private key d, public key can be generated through following steps:

1) Select a random integer d in the interval [0, n-1].

2) Compute Q = d× G, obtained by point Multiplication.

Q, G are points on the elliptic curve.

3) Now key-pair is (d, Q) where d is the Private Key and

Q is the Public key.

B. Signature generation

Utilizing domain parameters and private key, signer

generate signature for a message M by following steps:

1) Chooses a random integer k with 1≤ k ≤ n −1.

2) Compute k× G = (x1, y1) and r=x1 mod n. If r = 0 then

return to step 1.

3) Compute k-1mod n.

4) Compute z =h-1(M)2.

5) Calculate s = k-1(z + d× r) mod n. If s = 0 then returns

to step 1.

6) Signature for the message hash z is (r, s).

C. Signature verification

Authenticity of the received message can be verified by receiver exploiting following steps:

1) Verify that r, s are integers in the interval [1, n −1].

2) Compute z=h-1(M).

3) Compute w =s-1mod n.

4) Compute u1= z× w (mod n) and u2 = r× w (mod n).

5) Compute X=u1G+ u2Q. If X=O∞ then he will reject the signature.

6) Otherwise compute v=x1mod n where X =(x1, y1).

7) Accepts the signature if and only if v = r.

Consider an Elliptic curve E over prime finite field of characteristic q where q is a prime number greater than 3 and choose parameter a, b and generating point G of order n such that n× G = O. G is treated as the private key of signer. Now randomly select an integer d, 1 ≤ d ≤ n-1. Calculate public key Q by point multiplication of G and random number d using group law. Make d and Q as public parameters. Now Generate a one-time random number k such that 0< k<n-1. Using the same k for two different signatures is a major security breach in the use of this algorithm. major security breach in the use of this algorithm 0< k<n-1. Using the same k for two different signatures is a major security breach in the use of this algorithm.

LOOPHOLES IN ECDSA

Though ECDSA provides better security, verify authenticity, un-forge-ability and non-repudiation, still it is not without different facets of security attack. Basic concept used in ECDSA is, one generating point is made public and an integer treated as private key is multiplied with generating point to create public key. Here discussed one technique to unearth the private key and the private random number used in ECDS.

IV. CONCLUSIONS

One Time Password implementation for multi-cloud environment enforces tight security on the clouds. Passwords can easily be exploited in general. However OTP reduces the chances of misuse of passwords. Proposed ECDSA is less complex algorithm to calculate digital signature. OTP have been in use for quite some time but its implementation in muti -cloud scenario is still not there. Furthermore, it trims down the overhead of calculating the value of ‘r’. Proposed algorithm doesn’t share domain parameter’s elements ‘a’, ‘b’, ‘n’ and ‘q’ publically which makes it nearly impossible for an adversary to compute private key of signer.

V. References

[1] M. Vukolic, "The Byzantine empire in the inter cloud", ACM SIGACT News, 41,2010, pp.105-111.

[2] M.A.Alzain, E.Pardede, B.Soh, J.A.Thom: “Cloud Computing Security: From Single To Multi Clouds”, 45th Hawaii International Conference on System Sciences,2012.

[3] D. Linthicum, “Selecting the right cloud,” book excerpt, InfoWorld Cloud Computing Deep Dive, InfoWorld, Sept 2009.

[4] Elhadiyoussef Wajih, Benhadiyoussef Noura, Machhout Mohsen and Tourki Rached,” Low Power Elliptic Curve Digital Signature Design for Constraned Devices,” International Journal of Computer Science and Security, vol 1, issue 3, 2012.

[5] Tilahun Kiros and Kumudha Raimond,” An Efficient Modified Elliptic Curve Digital Signature Algorithm,” Journal of EEA, vol 26, 2009.

[6] M. Ashkar Mohammed and Dr. S. Suresh Babu,” Realization of Elliptic Curve Cryptography Based on ECDSA,” Current Trends in Technology and Sciences, vol 1, issue 2, sept 2012.

[7] Aqeel Khalique, Kuldip Sihgn and Sandeep Sood,” Implementation of Elliptic Curve Digital Signature Slgorithm,” International Journal of Computer Applications, vol 2, no. 2, may 2010.

[8] Md. Rafiqul Islam, Md. Sajjadul Hasan, Ikhtear Sharif Muhammad Asaduzzaman,” A New Point Multiplication Method for Elliptic Curve

[9] Mrs. Megha Kolhekar and Mrs. Anita Jadhav,” Implementation of Eliptic Curve Cryptography on Text and Image,” International Journal of Enterprise Computing and Business System,” vol 1, issue 2, july 2011.