Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 3 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Secure Elliptic Curve Digital Signature Algorithm for Internet of Things

By B. Sindhu & Dr. R. M. Noorullah
ABIT, JNTU Anantapur, India

Abstract- In the previous couple of years, the internet of things (IoT) is gaining additional and a lot of attention each within the academia and in the industrial worlds. A wide accepted notion of the internet of things (IoT) is stated the chance of militarization everyday objects with adequate technology to permit them to speak with alternative objects, identify themselves, or perhaps participate to distribute computing. These things are customarily stated as SO's (Smart Object), might be drawn as actual relics augmented with computing, communication, actuations and storing functionalities. Their importance resides within the capabilities they need to create physical environments "smart" therefore as to offer novel cyber physical service to individuals. smart Objects, that are vital elements of the IOT, are everyday objects that are equipped with hardware components like radio for communication, a CPU hardware to process tasks, sensors to be responsive to the globe within which they're located and to regulate it at a given instant. Even so, as sensible objects have restricted resource constraints to appoint sturdy protection mechanisms, they're at risk of subtle security attacks. For this reason, a smart authentication mechanism that considers every helpful resource constraints and safety is needed.

Keywords: elliptic curve digital signature algorithm, IOT, elliptic curve, ECDSA.

GJCST-E Classification : C.2.1, G.1.8, G.4

Strictly as per the compliance and regulations of:

Secure Elliptic Curve Digital Signature Algorithm for Internet of Things

B. Sindhu [α] & Dr. R. M. Noorullah [σ]

Abstract- In the previous couple of years, the internet of things (IoT) is gaining additional and a lot of attention each within the academia and in the industrial worlds. A wide accepted notion of the internet of things (IoT) is stated the chance of militarization everyday objects with adequate technology to permit them to speak with alternative objects, identify themselves, or perhaps participate to distribute computing. These things are customarily stated as SO's (Smart Object), might be drawn as actual relics augmented with computing, communication, actuations and storing functionalities. Their importance resides within the capabilities they need to create physical environments "smart" therefore as to offer novel cyber physical service to individuals. smart Objects, that are vital elements of the IOT, are everyday objects that are equipped with hardware components like radio for communication, a CPU hardware to process tasks, sensors to be responsive to the globe within which they're located and to regulate it at a given instant. Even so, as sensible objects have restricted resource constraints to appoint sturdy protection mechanisms, they're at risk of subtle security attacks. For this reason, a smart authentication mechanism that considers every helpful resource constraints and safety is needed. Our projected scheme uses the standards of Elliptic Curve digital signature scheme and evaluates consistently the potency of our scheme and observes that our scheme with a smaller key size and lesser infrastructure performs on par with the prevailing schemes while not compromising the security level.

Keywords: elliptic curve digital signature algorithm, IOT, elliptic curve, ECDSA.

I. Introduction

Digital signature algorithm is a public key cryptology algorithm designed to shield the genuineness of a digital document. A document is signed by a secret key to provide a sign and therefore the sign is verified against the message by a public key. Therefore any party can verify the signature with signer's public key. A legitimate digital signature offers a recipient reason to believe that the message was created by a identified sender who possesses the secret key, which it absolutely was not altered in transit.

Digital signatures are used wide in e-commerce applications, in banking applications, in software system distribution, and in different cases wherever jurisdiction is concerned and it's necessary to notice forgery or meddling. Thus it's crucial to use algorithms that are standardized by government organizations. Despite the fact that there are a varied range of digital signature algorithms in analysis literature, only three algorithms are standardized by the National Institute of Standards and Technology (NIST) and are wide employed in most industrial applications. These are the RSA, the DSA and therefore the ECDSA [7] [9]. The security of the DSA relies on the hardness of the discrete log problem on the multiplicative group of units on the finite field FP. The ECDSA is that the elliptic curve analogous of the DSA and its security is predicated on the distinct log drawback on the group of points on elliptic curve over a finite field. DSA and ECDSA are standardized and wide utilized in universe applications. Their securities are authenticated by the cryptology community for pretty much 20 years. It's affordable to believe that projected new DSA primarily based Elliptic Curve is secure. We have a tendency to confer the correctness of the projected algorithm and show that the security of the algorithm relies on the hardness of the discrete log problem within the underlined group.

II. Internet of Things

Internet of Things (IoT) was initially utilized in 1999 by British technology pioneer Kevin Ashton to explain a system within which objects in the physical world can be connected to the net by sensors. Ashton coined the term as an instance the ability of connecting Radio-Frequency Identification (RFID)tags utilized in corporate supply chains to the web so as to count and track product while not the necessity for human intervention [8]. Today, the net of Things has become a preferred term for describing situations during which internet connectivity and computing capability extend to a range of objects, devices, sensors, and everyday things. Whereas the term "Internet of Things" is comparatively new, the construct of mixing computers and networks to observe and control devices has been around for many years. The internet of Things (IoT) is what happens once every day normal objects have inter-connected microchips within them. These microchips facilitate not solely keep track of alternative objects, however several of those devices sense their

Author α: M.Tech Scholar, Department of CSE, ABIT, Kadapa. e-mail: basettysindhu2016@gmail.com
Author σ: principal & Professor, Department of CSE, ABIT, Kadapa, India. e-mail: noorullahrm@gmail.com

encompassing and report it to alternative machines likewise on the humans. Additionally known as M2M, standing for Machine to Machine, Machine to individual, individual to Machine or Machine to individual, the IoT showing intelligence connects humans, devices and systems. Experts term two divergent kinds of communication within the IoT: thing to individuals and individuals-to-individuals communication. Thing-to-individuals and individuals-to-thing communications cover variety of technologies and applications, whereby individuals act with things and contrariwise, as well as remote access to things by humans, and objects that endlessly report their standing, whereabouts and device information. Thing-to thing communications encompasses technologies and applications wherever in everyday objects and infrastructure act with the human. Objects will monitor alternative objects, take corrective actions and apprise or prompt humans as needed.

III. Elliptic Curve Arithmetic

ECC makes use of elliptic curves in which the variables and coefficients are restricted to elements of a finite field. There are two families of elliptic curves defined for use in cryptography: prime curves defined over odd prime field F_P and binary curves defined over Galois field $GF(2^m)$[1].

In Elliptic Curve Cryptography uses the following curve equation.

$y^2 = x^3 + ax + b$ where a and b are the constant with $4a^3 + 27b^2 \neq 0$

Cryptographic operations on elliptic curve over finite field are done using the coordinate points of the elliptic curve. Elliptic curve over finite field equation is given by:

$$y^2 = \{x^3 + ax + b\} \bmod p$$

Certain formula is defined for operation with the points [6]

a) Point Addition

The two point $P(x_1, y_1)$ and $Q(x_2, y_2)$ are distinct.

$P + Q = R(x_3, y_3)$ is given by the following calculation

$x_3 = \{\lambda^2 - x_1 - x_2\} \bmod p$

$y_3 = \{\lambda(x_1 - x_3) - y_1\} \bmod p$ where

$\lambda = \{(y_2-y_1)/(x_2-x_1)\} \bmod p$

b) Point Doubling

The two point $P(x_1, y_1)$ and $Q(x_2, y_2)$ overlap.

$P + Q = R(x_3, y_3)$ is given by the following calculation.

$x_3 = \{\lambda^2 - 2x_1\} \bmod p$

$y_3 = \{\lambda(x_1 - x_3) - y_1\} \bmod p$ where

$\lambda = \{(3x_1^2 + a)/2y_1\} \bmod p$

c) Point Multiplication

Let P be any point on the elliptic curve. Multiplication operation over P is defined by the repeated addition. $kP = P + P + P + \ldots +$ k times.

d) Elliptic Curve Cryptography

The use of Elliptic Curve Cryptography was initially suggested by Neal Koblitz [2] and Victor S. Miller [4]. Elliptic curve cryptosystems over finite field have some advantages like the key size can be much smaller compared to other cryptosystems like RSA. We have used Fixed and Variable Size Text Based Message Mapping Techniques [5] for message Encryption and decryption.

IV. Existing System

The scheme [3] is apt for a signer who has limited computing capability like, a signer using his smart Card which stocks his secret key.

a) Key-Pair Generation

Using random integer number d and generating point G, public key Q is computed as follows.

1) Select a random integer d in the interval [0, n-1]. 2) Compute $Q = d \times G$, obtained by point Multiplication. Q, G are points on the elliptic curve. 3) Now key-pair is (G, Q) where G is the Private Key and Q is the Public key.

b) Signature Generation

Signer uses parameters q, a, b, p, n, d and private key G, to sign a document or message M where a, b, p and q are constants in elliptic curve equation. To sign a message signer does the following:

1. Chooses a random integer k with $1 \leq k \leq n-1$.
2. Compute $k \times G = (x_1, y_1)$.
3. Compute hash value z of message M, $z = h^{-1}(M)^2$.
4. Compute $s = (z \times d) \times k^{-1} \bmod n$. If $s = 0$ then return to step 1.
5. Signature for the message M is (s, x_1).

c) Signature Verification

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

1. First verify that s is integer in the interval $[1, n-1]$
2. Calculate hash z of the message/document M
3. Calculate the number $w = s^{-1} z \pmod n$
4. Using this number compute the point $(x, y) = w \times Q$ on the curve, and, finally, authenticate the signature by checking whether the equivalence x=x1 holds.

d) Possible Attack

The intruder can easily modify the message and append hash value of the modified message to the signature element. This modification cannot identify by the receiver.

The attack is described as follows.

1. Calculate hash z of the message m
2. Calculate z^{-1}
3. Calculate $s_1 = s \times (z^{-1})$
4. New/modified message m_1
5. Calculate hash z_1 of the message m_1
6. $s' = s_1 \times (Z_1)$
7. Signature for the message m1 is (s', x1).

V. Proposed System

Proposed scheme is secure when compare with existing system. This scheme is developed without modular inversion process in Signature Verification algorithms.

Notations:

To be appropriate in explanation of our work the elements are defined as

d: random integer number

T: private key

Q: Public key

m: message

k: Random number

H() : a secure one-way hash function

r, S_1, s_2: Signature elements

q: field order

FR: field representation

a, b: coefficients

G: Base point

n: Order of G

h: co-factor

a) Key Pair Generation

Key pair d and Q made by the Signer as follows

INPUT: D= (q, FR, a, b, G, n, h)

1. Choose a distinctive random number, j, within the interval [1, n-1]
2. Compute T ←(j×G) Choose a distinctive random number, d, within the interval [1, n-1]
3. Compute Q ←(d×T)
4. Return (Q, T, d)

OUTPUT: Q, T, d

b) Signature Generation

The signer can sign message m as follows

INPUT: D= (q, FR, a, b, G, n, h), d, m, T, Q

Begin

repeat

k = Random [1, 2,…, n-1]

P = k×T

c=X-Co-ordinate (P)

z = H (m) mod n

$S_1 = c \times k \times d \times T \bmod n$

$s_2 = (c + d^{-1}) z \times k \bmod n$

R = z×P

r = X-Co-ordinate(R)

until $r \neq 0$ and $s_1 \neq 0$ and $s_2 \neq 0$ return (r, S_1, s_2)

End

OUTPUT: Signature (r, S_1, s_2)

c) Signature Verification

To verify the signature (r,S_1, s_2) on message m, receiver does the following:

INPUT: D= (q, FR, a, b, G, n, h), Q, m, Signature (r, S_1, s_2)

Begin

If r, S1, s2 doesn't belongs to [1,2…, n-1] then

Return ("Reject the signature")

end if

z= H(m)

$U_1 = s_2 \times Q$

$U_2 = z \times S_1$

$W = U_1 - U_2$

v= X-Co-ordinate (W)

if v = r then

Return ("Accept the signature")

else

Return ("Reject the signature")

end if

end

OUTPUT: Acceptance or rejection of the signature.

d) Proof of Signature Verification

$S_1 = c \times k \times d \times T \bmod n$

$s_2 = (c + d^{-1}) z \times k \bmod n$

$W = U_1 - U_2$

$= s2Q - zS_1$

$= (c + d^{-1}) z \times k \times d \times T - z \times c \times k \times d \times T$

$= c \times z \times k \times d \times T + d^{-1} \times z \times k \times d \times T - z \times c \times k \times d \times T$

$= z \times k \times T$

$= R$

VI. Conclusion

The intruder can easily alter the message or document and replace the existing message hash value with modified message hash value. But in proposed scheme attacker may modify the message but attacker cannot substitute hash value of existing message with hash value of new message. If the message modified without appending the hash value then it rejects the Signature. Considering the above, our proposed digital signature scheme is more secure when compared to the existing scheme.

References Références Referencias

1. Hankerson Darrel, Alfred Menezes and Scott Vanstone,"Guide to Elliptic Curve Cryptography".

2. Koblitz N, "EllipticCurve Cryptosystems", Mathematics of Computation, 48, 1987, pp. 203-209.
3. Lamba Shweta,Monika Sharma, "An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA),2013 International Conference on Machine Intelligence Research and Advancement(ICMIRA),2013,PP.179-183.
4. Miller V, "Uses of Elliptic Curve in Cryptography", Advances in Cryptography, Proceedings of Crypto'85, Lectures notes on Computer Sciences, 218, Springer-Verlag, 1986, pp. 417-426.
5. Muthukuru Jayabhaskar, Prof. Bachala Sathyanarayana, "Fixed and Variable Size Text Based Message Mapping Techniques Using ECC", Global Journal of Computer Science and Technology, Vol-12, Issue-3, Feb-2012, pp. 13-18.
6. Muthukuru Jayabhaskar, Prof. Bachala Sathyanarayana,"A Survey of Elliptic Curve Cryptography Implementation Approaches for Efficient Smart Card Processing", Global Journal of Computer Science and Technology, Vol-12, Issue-1, Jan-2012, pp. 7-12.
7. Seberry Jennifer, Vinhbuu To, Dongvu Tonien, "A new generic digital signature algorithm", 3(2),Apr-2011, pp.221-237.
8. Shelkikar Ravindra P, Nitin S.Wagh,"Review Paper Based On Women Tracking Device Using Concept Of Internet Of Things",IJAIEM, Vol-5,Issue-2, Feb-16,pp.63-73.
9. Tao LONG, Xiaoxia LIU, "Two Improvements to Digital Signature Scheme Based on the Elliptic Curve Cryptosystem", Proceedings of the 2009 International Workshop on Information Security and Application, Nov-2009.