Elliptic Curve Cryptography based Security Framework for Internet of Things and Cloud Computing

DAISY PREMILA BAI T, ALBERT RABARA S, VIMAL JERALD M
Department of Computer Science
St. Joseph's College, Bharathidasan University
Tiruchirappalli, Tamil Nadu
INDIA
daisypremila@gmail.com, a_rabara@yahoo.com, vimaljerald@gmail.com

Abstract: - Internet of Things (IoT) and Cloud Computing paradigm is a next wave in the era of computing and it has been identified as one of the emerging technologies in the field of Computer Science and Information Technology. It has been understood from the review reports that integration of IoT and Cloud Computing is in its infantile phase and it has not been extended to all application domains due to its inadequate security architecture. Hence, in this paper a novel Elliptic Curve Cryptography based security framework for Internet of Things and Cloud Computing is proposed. This is a secured and adoptable one for the public to access diversified smart applications and services distributed in the cloud, anywhere, anytime, any device and any network irrespective of the underlying technologies in a smart environment. The cloud services are integrated and connected through a novel IP/MPLS (Internet Protocol/ Multiprotocol Label Switching) core. Elliptic Curve Cryptography (ECC) is used to ensure complete protection against the security risks such as confidentiality, integrity, privacy and authentication. This model eliminates ambiguity and ensures security with enhanced performance and realizes the vision of one intelligent smart card for any applications and transactions. The security strengths of various public key cryptosystems are analysed and ensured ECC is one of the best cryptosystems for internet of things and cloud.

Key-Words: - IoT, cloud, ECC, IP/MPLS core, security, smart environment

1 Introduction

Internet of Things (IoT) and Cloud Computing play a vital role in the field of Information Technology [1]. Internet of things is not a single technology, it is the concept in which many of the new things are getting networked and connected anytime, anyplace, with anything and anyone ideally using any path or network and any service in a heterogeneous environment [2]. European Research Cluster on the Internet of Things (IERC) states that "Internet of Things is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes and virtual personalities and use intelligent interface and are seamlessly integrated into the information network"[3]. In a nutshell, IoT is characterized by the real world of smart objects with limited storage and processing power [4].

In contrast, Cloud Computing is characterized by virtual world with unlimited capability in terms of storage and processing power. According to National Institute of Standard and Technology (NIST), "Cloud Computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or cloud provider interaction" [5]. Cloud computing allows computer users to conveniently rent access to fully featured applications, software development and deployment environments and computing infrastructure assets such as network-accessible data storage and processing with its salient features: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [6].

Though the IoT and Cloud Computing have emerged as independent technologies, merging these two have augmented the field of future networks. Internet of Things is enhanced by the unlimited capabilities and resources of cloud to compensate its technological constraints such as storage and processing. On the other hand, cloud has extended its scope to the real world through IoT in a more dynamic and distributed way to deliver new applications and services in a real time scenario at large scale. Consequently, the integration of IoT and Cloud, the complementary technologies enhance the smart environment to reach the heights of availing any services and applications anywhere, anytime, any firm and any device irrespective of any underlying technology [7].

Since, the integration of IoT and Cloud in its developmental stage, it has not been implemented in all the fields due to its inadequate security architecture. The review of literature articulates the state of the art in this field with its diversified application domains in creating the smart environment and the challenges in deploying this new scenario to all the fields [8]. The significant challenges to be resolved with the existing smart applications are interoperability, security, QoS, load balancing, mobility, IPv6 deployment, data management solution and acceptability of IoT and Cloud applications by users and citizens [9]. Several research works have been carried out to address these issues faced in creating the smart environment and to extend the same for all application domains, but so far no proposed work seems to be integrated and secured. Hence, in this paper a novel Elliptic Curve Cryptography based security framework for Internet of Things and Cloud Computing is proposed.

Elliptic curve cryptography is a public key cryptosystem developed by Neil Kobiltz and Victor Miller in 19th century [10] [11]. It is like RSA public key cryptography. The security strength of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP) [12]. ECC adopts scalar multiplication, which includes point doubling and adding operation which is computationally more efficient than RSA exponentiation. The complexity of ECC puts the attacker in difficulty to understand the ECC and to break the security key. The security level given by RSA with 1024 bit key can be achieved with 160 bit key by ECC. Hence it is well suited for resource constraint devices like smart cards, mobile devices, etc. [13].

This paper is organized as follows. Section 2 briefs the review of the literature. Section 3 describes the proposed work with different aspects such as Internet of Things and Cloud model and the security requirements. Section 4 presents the ECC based security framework and security analysis. Section 5 concludes the paper.

2 Review of Literature

Researchers have proposed various platforms and architectures to substantiate the new paradigm 'Internet of Things and Cloud' and have explained how the Internet of Things and Cloud Computing can work together and complement each other as it has the capability to integrate seamlessly the virtual world of information technology with the real world of things [14] [15] [16] [17]. The features that attract the users, service consumers and providers are the storage, computation, communication, real time access, scalability, reliability, availability, reduced deployment costs, ease of access and ease of use [18] [19] [20].

There are number of integrated CloudIoT architectures and frameworks exist to support applications such as transport, healthcare, smart city, video surveillance, smart mobility, smart metering, smart Grid, etc. [21] [22][23][24]. Though the integration phenomena create more technical advantages and business opportunities in many fields, there are equally larger threats from the attackers. Because the information is not ciphered and the privacy of the information is not ensured and also the senders and the receivers are not authenticated via secure connections [25] [26] [27].

Elliptic curve cryptography is a newer a newer approach to public key cryptography based on algebraic structure of elliptic curves over finite fields and considered as a efficient technique with lower key size for the user and hard exponential time challenge for the attacker to break into the system. In ECC a 160 bit key provides the same security as RSA with 1024 bit key. It requires only lower computation and less memory space. The advantage of the ECC is the absence of the sub exponential time algorithms and uses less key size and provides more security.

ECC is widely used in many fields. It is used in devices which has less storage memory especially popularly employed in smart cards. Smart cards are being used as a bank cards, electronic tickets, personal identification cards, etc. Most of the manufacturing companies are producing smart card that make use of elliptic curve digital signature algorithms. ECC is used in wireless communication and in devices with low computing power and resources such as mobile devices. For implement ECC, constrained devices have been considered to be the most suitable platform. Smaller key size results in faster execution which is beneficial to systems where real time performance is a critical factor. It is also not an easy task to choose appropriate elliptic curve [28]. ECC standardization is crucial for achieving practical and efficient implementation. National Institute of Standards and Technology (NIST) provides specification for ECC which are considered safe for the use in cryptographic application [29].

Consequently, the review of literature puts forward the need for developing a security architecture for Internet of Things and Cloud Computing. Since IoT encompasses smart objects which are considered to be resource constrained devices, ECC could be the best public key cryptosystem. Hence, in this paper a novel ECC based security framework for internet of things and cloud computing is proposed.

3 Internet of Things and Cloud Model

Internet of Things and Cloud model is envisaged to offer secure smart services and applications anywhere, anytime, any firm, any device and any network independent of any underlying technologies with one IoT enabled Intelligent Smart Card (ISC). ISC eases the secure access of diversified applications and services distributed in a cloud environment with one Unique Identification (UID) number per citizen through the intelligent systems. The intelligent system processes the data at smart gateway and then uploads the necessary data to the cloud through IP/MPLS core network. This system adopts elliptic curve cryptography to ensure authentication, confidentiality, privacy and integrity. The functional components of the proposed model is depicted in Fig.1.

Internet of Things and Cloud model consists of four key components, namely intelligent system, security gateway, IP/MPLS core and integrated cloud IoT platform. The intelligent system comprises of an IoT enabled Intelligent Smart Card (ISC), Smart Reader, Near Field Communication (NFC) enabled Mobile Device and Smart Gateway. The proposed Intelligent Smart Card is an IoT enabled active card conforms to the ISO/IEC standard which consists of RFID tag, biometric template, image template and Unique Identification Number (UID) as special features. UID is a 20 digit alpha numeric number which includes country name, state name, place of birth, date of birth, sex, father's initial and five digit number. The last defined five digit number will be the PIN number (accompanied with the abbreviation of the service provider, for example – SJCXXXXX) for any authentication process for availing any applications. This helps the user to use the 'easy to remember PIN' for all applications which overcomes the problem of forgetting or losing the PIN numbers. The biometric fingerprint and facial image are stored on ISC in an encrypted form helps the card holder to have their biometric information on their hands always to ensure the protection of the personal data.

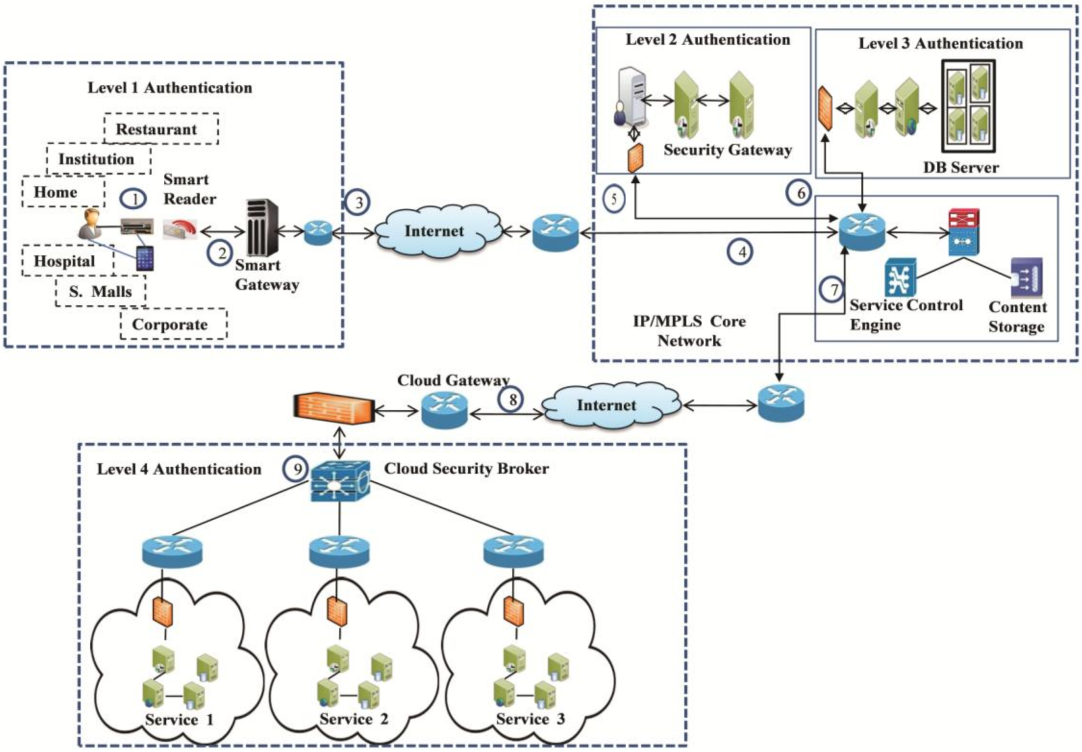

Fig.1. Internet of Things and Cloud Model

RFID tag in the ISC is capable of transmitting data to a RFID reader from the distance of 100 feet and the data are transferred to the smart gateway through any one of the available networks such as WiFi, ethernet, etc. Smart gateway is very compatible and adaptable for both IPv4 and IPv6. It is responsible for protocol conversion which make the user feel comfortable to avail any applications and services from anywhere at any time independent of underlying networks. It collects the data, stores the data temporarily, performs preprocessing, filters the data, reconstructs the data into a more useful form and uploads only the necessary data to the cloud through IP/MPLS core.

IP/MPLS core is the backbone network for the proposed architecture which bridges the cloud platform and IoT enabled intelligent systems. It provides secure and fast routing of the packets from source to destination by adopting packet switching technology. It transmits data with the assurance of high reliability, availability, security and quality of service. The Class of Service (CoS) concept defines traffic priorities for each application. User profiles and service policies are registered in the Service Control Engine (SCE) and they are stored in the DataBase (DB) content storage. Once the user is authenticated and authorized the SCE provides the access and redirects the request to the respective applications. The cloud security broker receives the service request and assigns the cloud services followed by service level authentication. Since the different services of the cloud providers are interconnected interoperability is achieved easily with no single point of failure. The security gateway adopts multi-factor authentication to ensure end-to-end security. The sequence diagram of the internet of Things and Cloud model is depicted in Fig.2.

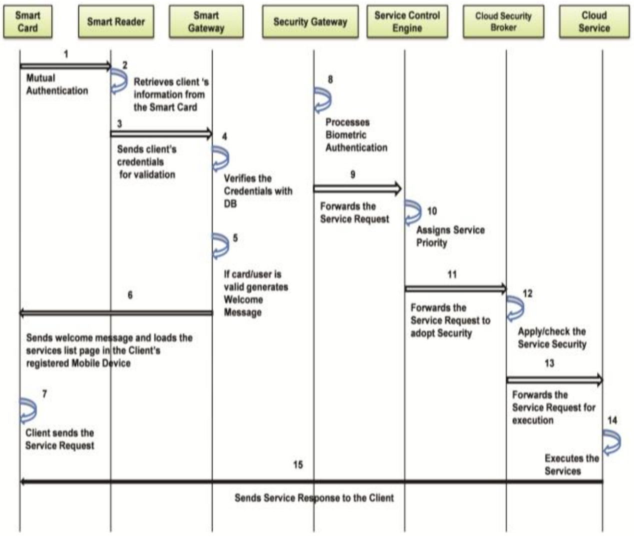
Smart Card
Smart Reader
Smart Gateway
Security Gateway
Service Control Engine
Cloud Security Broker
Cloud Service
1
Mutual Authentication
2
Retrieves client 's information from the Smart Card
3
Sends client's credentials for validation
4
Verifies the Credentials with DB
5
If card/user is valid generates Welcome Message
6
Sends welcome message and loads the services list page in the Client's registered Mobile Device
7
Client sends the Service Request
8
Processes Biometric Authentication
9
Forwards the Service Request
10
Assigns Service Priority
11
Forwards the Service Request to adopt Security
12
Apply/check the Service Security
13
Forwards the Service Request for execution
14
Executes the Services
15
Sends Service Response to the Client

Fig.2. Sequence Diagram

3.1 Security Requirements

The security requirements of the Internet of Things and Cloud model can be defined in terms of mutual authentication, confidentiality, integrity and availability. Mutual Authentication is one of the important aspects in the proposed model where ISC and Reader are RFID based. Mutual authentication of RFID tag in the ISC and the RFID reader is very crucial and critical to ensure the identity of the communication devices involved in communication. Confidentiality is one of the major concerns since the involvement of smart objects in the IoT environment are more and there is no physical path to transmit the data, rather it uses the air interface. Ensuring that the information is hidden from unauthorized access is more important. Integrity also is a challenge to ensure that the information is protected from unauthorized change and the information is available to the authorized party when it requires. To strengthen the security requirements of the internet of things and cloud model elliptic curve cryptosystems is adopted.

4 ECC based Security Framework

The proposed ECC security framework for internet of things and cloud model adopts multifactor authentication. The authentication scheme consists of seven phases, namely initialization phase, registration phase, mutual authentication phase, re-registration phase, user authentication phase, mobile device authentication phase and service level authentication phase. The various notations used for the authentication scheme are presented in Table 1.

Table 1 Notations and Descriptions

Notations	Description
p	large prime number $>2^{160}$
GF(p)	A Finite Field (Galois field)
Ep(a,b)	Elliptic Curve over Fp
G	Generator Point
U	Client
S	Server
UID	Identity of the ISC
SID	Identity of the Server
PID	Pseudo identity of the ISC
Us	Client's secret key
Ss	Server's master secret key
Ns	Random number chosen by the server
Ps	Public key of the server
Pus	Public key of the ISC
Pur	Public key of the reader
Eed	Indicates the presence of ECC algorithm

4.1. System Initialization Phase

The server at the Key distribution and registration center ‘S’ generates the following system parameters:

1. S chooses a non singular elliptic curve $Ep(a,b)$ over the finite field $GF(p)$ where ‘p’ is greater than 2160. It then selects a generator point ‘G’ on the elliptic curve $Ep(a,b)$ and a prime factor ‘N’ which is the largest prime number where $NG=0$ and $N<p$.
2. S randomly chooses a master secret key Ss which is 160 bit in length where $Ss < N$ and $Ss \in Ep(a,b)$ and computes its public key $Ps = SsG$.
3. S announces the public parameters G and Ps on the authenticated public domain.

The public parameters are write protected. Only the authorized server S can update the information in the public domain. The information can be read from the public domain by anyone but no one can change any information. Hence the integrity of data is achieved.

4.2. Registration Phase

To avail the services from any application domain, client ‘U’ should register at the server S with UID and MACID of the ISC which represented by B, IMEI of the clients mobile device denoted by C, biometric finger print and facial image of the client are denoted by E and D . The steps involved in this phase are as follows:

1. U has UID, B, C, D, E and selects a random secret key $Us < N$ which is 160 bit in length.
2. U computes $BUs = H(B\|Us)$, $CUS = H(C\|US)$, $DUs = H(D\|Us)$, $EUs = H(E\|Us)$ and sends the registration request to the server via secure channel. Reg = {UID, BUs, CUs, DUs, EUs}
3. Server receiving the registration request from the client, S chooses a random number Ns and computes the secret token for the client as $Ut = H(SID \|UID \|Ss \|Ns)$
4. S computes
   $aA = Ut \oplus H(BUs\|CUs\|DUs\|EUs\|SID)$ and
   $bA = H(Ut \|BUs\|CUs\|DUs\|EUs \|UID)$.
5. S stores the information {aA,bA, H, Eed, Ep(a,b),p} in an encrypted form on the ISC.
6. S stores the information $PID = H(Ss \|UID)$ and Ns in to client verification table T which contains SID, secret random number Ns along with the status = 0. Status will indicate whether the client is active, inactive, login or logoff. The status may be active and login, active and logoff and inactive.
7. Client computes $cA = H(UID\|B\|C\|D\|E)\oplus Us$ and stores it on the memory of the ISC. ISC contains the information {aA, bA, cA, H, Eed, Ep(a,b),p}

In this registration phase server does not directly store UID in the client’s verification table rather S stores the pseudo identity $PID = H(Ss \|UID)$. Hence it is not possible to compute UID from PID without knowing the server’s secret key Ss and it preserves the privacy of the client.

4.3. Mutual Authentication between ISC and Reader

In the proposed model, ISC is an IoT enabled contactless smart card which has to be authenticated with the RFID reader. This phase illustrates the mutual authentication between ISC and the reader by performing three way handshake negotiation between ISC and the RFID reader. Prior to the mutual authentication the server in the registration center S prelolads the necessary data to the ISC and the reader.

1. The public key of the ISC is Pus =H(ISC MACID). It converts MACID of ISC into 160 bit integer. ISC calculates the reader’s public key Pur = H(R MACID)
2. ISC generates two 160 bit integer x and y where x is the temporary session key.
3. ISC generates two cipher texts C1 and C2. $C1 = y\ (Ps+PurG)$ and $C2 = x\oplus H(y)$.
4. ISC sends the request to the reader by sending the two cipeher texts including its MACID in an encrypted form which is encrypted with the reader’s public key to protect its identity. Only the reader can decrypt it.
5. The reader receives the request in the encrypted form and decrypts the message using its private key Prr.
6. Reader recovers the session key x by calculating $x = H(e(Prr, C1)) \oplus C2$ and saves it.
7. Reader generates two random 160 bit integer u and v where v is the primary session key used for encryption. Reader generates two ciphertexts C3 and C4. $C3 = u(\ Ps+ PusG)$ and $C4 = v\oplus H(u)$. The reader sends C3, C4 including C1 and C2 in an encrypted form to the ISC for verification.

ISC receives the message and decrypts the same with its private key. The tag checks C1 and C2. If the values are same authentication process will be further proceeded otherwise it will be aborted. ISC sends the value of C3 and C4 in an encrypted form to the reader for verification. If the values are same the communication will be established else failure notification will be sent.

Both ISC and the reader have mutually authenticated. For every new session both ISC and reader will generate fresh random values for y and v in order to enhance the session robustness. For effective and secure communication, the authenticated messages are transported to the smart gateway of the proposed model in an encrypted form. It prevents an adversary to perform malicious activities and enhances confidentiality.

4.4. User Authentication

Once the mutual authentication between ISC and RFID reader is carried out, the next factor is to validate whether the user is the legal holder of the ISC and the registered mobile device. The user is identified as an authenticated user with the UID number obtained from the ISC. When UID is sent to the smart gateway, it gets the information from the closest server and checks whether it is a valid UID number. If it is recognized as the valid UID number, then the intelligent system instructs the user to do the biometric authentication using ISC where system on card process takes place. If the fingerprint template stored on the UAISC matches, it checks for the facial image of the UAISC holder with the image captured through the CCTV. If all the three factors match, the user is identified as the legal user of the card holder who becomes an authenticated user to avail any services. To avail any services, users' registered mobile device is used and it need to be authenticated.

4.5. Device Authentication

The mobile device is authenticated using X.509v3 digital certificate for secure communication over the internet followed by unique identifiable picture. The mobile device sends the client certificate to the server. The server gets the client certificate from the CA and verifies it with the client's public key. It is also verified for the validity period and validated. If the certificate is valid, then the device is considered to be authenticated. The authentication is further strengthened with the graphical password by matching the identifiable pictures stored in the mobile device and the server in the registration center. If the picture matches, the secured connection is established between the device and the server and the welcome message is displayed on the mobile device followed by the list of services, since then it is feasible for the user to avail any services over the mobile. Yet it recommends that the service level authentication to be carried out to ensure both the service requester as well as the service provider to be the legal entities.

4.6. Service Level Authentication

Once the user and device authentication is over, user selects or requests for the service. The user interface asks the customer to enter the PIN number for the particular service or request. This is sent to the server in an encrypted form. User interface decrypts this key with the server's public key. If the decryption is successful, then the service will be provided to the customer. Else the client is asked to redo the same for three times. If the login fails for three attempts, the service is blocked. To ensure that the service provider is the authorized party, the cloud security broker matches the already stored credentials such as the digital signature. If the credentials are matching, the secure delivery of the service is initiated which ensures the availability of the service for the legitimate user. Fake service providers are blocked to offer their services which ensures the service consumers that the service provided is reliable.

4.7. ECC based Encryption and Decryption

The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP). In the notation Q=kP, P and Q belong to Ep(a,b) and k is less than p i.e. "k<p". In this if k and P are given it is easy to calculate. But if P and Q are given it is relatively hard to determine k, if k is sufficiently large. k is the discrete logarithm of Q to the base P. This is the discrete logarithm problem for ECC. Due to the complexity of of DLP ECC is hard to break. The main operation involved in ECC is point multiplication.

An elliptic curve E is described as y2=x3+ax+b. The highest degree of this equation is 3. In order to perform higher order encryption and decryption the equation should satisfy the standards proposed by NIST. In the proposed model ECC encrypts the plain text (M) into ciphertext (C) and vice versa by using the finite set of points in the elliptic curve over GF(p). The Weierstrass equation y2=x3+ax+b is used with modulo p to generate the points on the elliptic curve. The elliptic curve domain parameters are p, a, b, G, n, h, r where 'p' is a prime number, 'a' and 'b' are coefficients, 'G' is a generator point, 'N' is the cryptographic prime factor, 'h' is the cofactor and 'r' is the random integer less than 'N'. According to NIST the prime p should be greater than 2^{160}. For illustration, the proposed system uses the finite field elliptic curve with modulo 307. The coefficients 'a' and 'b' are assigned '1'. Hence the equation is y2=x3+x+1 mod 307. The elliptic curve domain parameters over Fp are validated and the chosen elliptic curve satisfies the following criteria and ensures greater security.

1. 4a3+27b2 ≠ 0 (mod p)
2. yG2=xG2+axG+b (mod p)
3. ‘n’ is a prime number
4. h ≤ 4
5. nG=0

The equation given is capable of generating 296 points. The points are generated with the following algorithm defined anew.

4.7.1 Algorithm to generate points on EC

```
Algorithm to generate points
{
Select a EC with modulo p (y2=x3+ax+b mod p)
Assign values for a and b, the coefficients of the equation.
Compute the equation Y2=X3+aX+b mod p.
        {
        For x=0 to (p-1)
        S=X3+aX+b mod p
        For d=0 to (p+1)/2
                {
                T = d2 mod P
                If T=S
                Y1 = d and Y2 = p-d
                Else d = d+1
                }
                X=X+1
        }
        (X,Y1), (X,Y2)
}
```

N=301 where when N is multiplied by the point generator it should produce zero and the generator point is capable of reproducing all the points generated with the defined curve. The chosen point generator is (7,257). The total number of points generated are 296. Only 100 out of 296 points over the proposed elliptic curve (Ep (a, b)) are given in Fig.3.

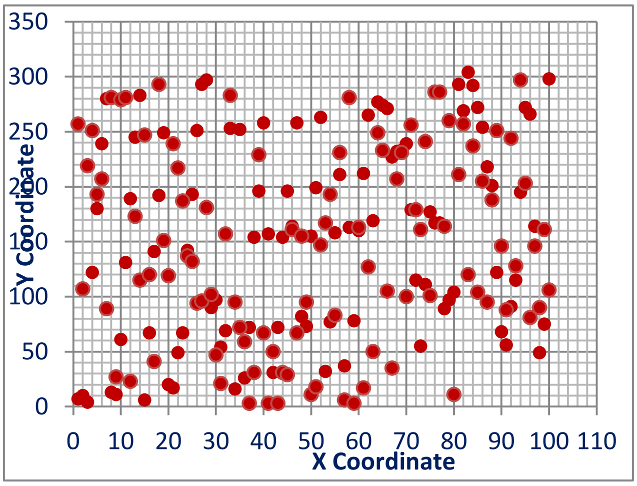

Fig.3. Generated points over the elliptic curve E ($y^2=x^3+x+1$ mod 307)

From the above generated points, eighty points are randomly chosen and the characters are assigned to those points to make the message encryption and decryption more flexible. The sample aggignment is given in Table 2.

Table 2 Character assignment to the EC points

(7,257) A	(10,107) a	(4,219) B	(67,120) b	(239,207) C
(280,89) c	(13,281) D	(11,27) d	(61,279) E	(131,281) e
(189,23) F	(245,173) f	(283,115) G	(6,247) g	(180,193) H
(141,41) h	(192,293) I	(241,151) i	(20,119) J	(17,239) j
(54,21) K	(69,157) k	(253,283) L	(16,95) l	(252,72) M
(26,59) m	(72,3) N	(154,31) n	(196,229) O	(258,67) o
(56,88) P	(91,244) p	(115,128) Q	(195,297) q	(272,203) R
(266,81) r	(164,146) S	(49,90) s	(75,161) T	(298,106) t
(179,256) U	(115, 179) u	(111,241) V	(55,61) v	(177,101) W
(167,286) w	(89,164) X	(97,260) x	(104,11) Y	(293,211) y
(67,187) Z	(292,237) z	(157,3) 0	(201,188) 1	(122,251) 2
(68,146) 3	(304,120) 4	(212,17) 5	(265,127) 6	(193,132) 7
(199,18) 8	(272,104) 9	(254,205) !	(218,95) @	(277,249) #
(274,233) $	(271,105) %	(227,35) ^	(232,207) &	(239,100) *
(49,217) Space	(269,257) ?	(142,137) \	(269,50) `	(251,94) ~
(293,96) /	(297,181) (	(90,102))	(97,47) -	(122,251) +

The plain text (M) is encoded into a point P(M) from the finite set of points generated in the elliptic curve Ep (a, b). When the points are generated, selecting a generator point ‘G’ is the important factor, where G ∈ Ep (a, b). The generator point and the Ep(a, b) will be made public. The generator point chosen is (7, 257). Sender and receiver can select a private key (Pr) and calculate the public key Pu = Pr x G. The simple method of encryption and decryption is given below.

To encrypt the message

1. The sender chooses a random integer ‘r’.
2. Calculates ciphertext point using receiver’s Public Key.
3. C= [(r.G), (M+r. Pur)]

To decrypt the message

1. Receceiver multiplies the first point (r.G) with the private key (Prr).

2. Adds this result to the second point of the ciphertext pair.
3. M = (M+rPur)-(Prr(r.G))=(M+rPrrG) - (Prr(r.G))

To do this cryptography point addition, point doubling and point multiplication are employed. To make encryption and decryption more feasible both sender and the receiver should know and agree upon the table defined with the chosen elliptic curve. Since the ECC is based on discrete lograthim problem, for an intruder to crack or steal the message is not possible. They should know the random integer generated ‘r’ by the sender and the private key of the receiver. The cracker should find the multiplier that creates the ciphertext ‘C’ from the generator point ‘G’. It is rather difficult when ‘r’ and ‘p’ in GF(p) are large.

4.8 Security Analysis

During the initialization phase, since the master key Ss is owned only by the Key distribution and registration center, it is difficult for an adversary to generate the correct private key for the reader even the adversary could copy all the valid parameters from ISC. The parameters and the information received cannot be modified or changed. This preserves the integrity of the data. At registration phase, the server S hashes UID with Ss and stores this pseudo identity of the ISC. Hence it is not possible to compute UID from PID without knowing the server’s secret key Ss. It preserves the privacy of the client. At the mutual authentication phase, the communicating devices authenticate mutually and generate fresh session key which enables the session robustness. Since the authenticated messages are transmitted to the smart gateway in an encrypted form confidentiality is achieved.

4.8.1 Comparison of Public Key Cryptosystems

The performance of ECC depends on the efficient computation of scalar multiplication. ECC can use small size key and offer the same level of security as the other public key cryptographic algorithms do with large size keys. Table 3 presents the key size ratio and cost ratio of ECC and RSA.

Table 3 Key Size Ratio and Cost Ratio for ECC and RSA

ECC key size (bits)	RSA key Size(bits)	Key size ratio	Cost Ratio
160	1024	1:7	1:3
224	2048	1:10	1:6
256	3072	1:12	1:10
384	7680	1:20	1:32
521	15360	1:30	1:64

The table values prove that ECC can provide same security level of RSA with shorter key length. The advantage of ECC over RSA is very obvious.

5 Conclusion

The proposed Elliptic Curve Cryptography based Security framework for Internet of Things and Cloud Computing is a unique one to avail any applications and any services irrespective of any underlying technologies anywhere, anytime with one ISC. Implementing this architecture will help every citizen to have only one ISC for any applications in a smart environment. ISC can connect people and enable automatic machine to machine communication. The message encryption and the multifactor authentication ensure unique authentication, integrity, confidentiality and privacy of the users. This ensures that the users and the service providers can adopt this system with its salient features of ease of use and security. The overall simulation of this architecture and real time implementation are in the progress of this research. Certainly, the proposed architecture eliminates ambiguity and enhances security.

References:

[1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Future Generation Computer Systems, Vol.29, 2013, pp. 1645-1660.

[2] O. Vermesan and P. Friess, Internet of Things from Research and Innovation to Market Deployment, River Publishers Series in Communications, Aalborg, 2014.

[3] O. Vermesan and P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers Series in Communications, Aalborg, 2013.

[4] R. Roman, P. Najera and J. Lopez, Securing the Internet of Things, IEEE Computer, Vol.44, 2011, pp. 51-58.

[5] L. Badger T. Grance, R.P. Corner and J. Voas, DRAFT Cloud Computing Synopsis and

Recommendations, National Institute of Standards and Technology, 2011, pp. 84.

[6] R. Buyya, J. Broberg and A. Goscinski, Cloud Computing Principles and Paradigms, WILEY, 2011.

[7] C. Atkins, K. Koanagi, T. Tsuchiya, T. Miyosawa, H. Hirose and H. Sawano, A Cloud Service for End-User Participation Concerning the Internet of Things, Proceeding of IEEE Conference on Signal-Image Technology and Internet-Based Systems (SITIS), IEEE, 2013, pp. 273-278.

[8] P. P. Pereira, J. Eliasson, R. Kyusakov, J. Delsing, A. Raayatinezhad, and M. Johansson, Enabling Cloud Connectivity for Mobile Internet of Things Applications" Proceedings of IEEE Symposium on Service Oriented System Engineering (SOSE), IEEE, 2013, pp. 518-526.

[9] S. Aguzzi, D. Bradshaw, M. Canning, M. Cansfield, P. Carter, G. Cattaneo, S. Gusmeroli, G. Micheletti, D. Rotondi and R. Stevens, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination. Final Report, European Commission, SMART 2013/0037, 2013.

[10] N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, Vol.49, pp. 203-209, 1987.

[11] V.S. Miller, Use of Elliptic Curves in Cryptography, Advances in Cryptology – CRYPTO'85, Lecture Notes in Computer Science, Springer Verlag, Vol.128,1985, pp. 417-426,

[12] Moncef Amara and Amar Siad, Elliptic Curve Cryptography and its Applications, 7th International Workshop on Systems, Signal Processing and thir Applications (WOSSPA), IEEE, 2011, pp. 247-250.

[13] Sandeep S. Kumar, Elliptc Curve Cryptography for Constrained Devices, PhD Thesis, Ruhur University Bochum, 2006.

[14] K. D. Chang, C. Y. Chen, J. L. Chen, H. C. Chao, Internet of Things and Cloud Computing for Future Internet, Communications in Computer and Information Science, Vol.223, 2011, pp. 1-10.

[15] B. B. P. Rao, P. Saluia, N. Sharma, A. Mittal and S. V. Sharma, Cloud Computing for Internet of Things & Sensing Based Applications, Proceedings of the 6th International Conference on Sensing Technology (ICST), IEEE, 2012, pp. 374-380.

[16] C. Dores, L.P. Reis and N.V. Lopes, Internet of Things and Cloud Computing, Proceedings of the IEEE Iberian Conference on Information Systems and Technologies (CISTI), IEEE, 2014, pp. 1-4.

[17] J. Cubo, A. Nieto and E. Pimentel, A Cloud-Based Internet of Things Platform for Ambient Assisted Living, SENSORS, 2014, pp. 14070-14105.

[18] Enabling Connected Smart Cities For A Better Tomorrow, Elitecore Wi-Fi Service Management Platform (SMP), 2015, http://www.elitecore.com/downloads/datasheets/wifioffload/Elitecore-Smart-City-Solution.pdf.

[19] C. Dobre and F. Xhafa, Intelligent Services for Big Data Science, Future Generation Computer Systems, 2014, Vol.37, pp. 267–281.

[20] G. Suciu, A. Vulpe, S.Halunga, O. Fratu, G.Todoran and V.Suciu, Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things, Control Systems and Computer Science (CSCS), IEEE, 2013, pp.513-518.

[21] J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, H. Jin and L. T. Yang, CloudThings: A Common Architecture for Integrating the Internet of Things with Cloud Computing, Computer Supported Cooperative Work in Design (CSCWD), IEEE, 2013, pp. 651-657.

[22] Y. Benazzouz, C. Munilla, O. Gunalp, M. Gallissot and L. Gurgen, Sharing user IoT Devices in the Cloud, World Forum on Internet of Things (WF-IoT), IEEE, 2014, pp. 373-374.

[23] G.C. Fox, S. Kamburugamuve and R. D. Hartman, Architecture and Measured Characteristics of a Cloud Based Internet of Things, Collaboration Technologies and Systems (CTS), IEEE, 2012, pp. 6-12.

[24] A. Botta, W. Donato, V. Persico and A. Pescap, On the Integration of Cloud Computing and Internet of Things, Future Internet of Things and Cloud (FiCloud), IEEE, 2014, pp. 23-30.

[25] D. Evans, The Internet of Things How the Next Evolution of the Internet Is Changing Everything, White Paper, Cisco, 2011.

[26] M. Aazam, P.P. Hung and E.N. Huh, Smart Gateway based Communication for Cloud of Things", Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), IEEE, 2014, pp. 1-6.

[27] M. Aazam, I. Khan, A.A. Alsaffar and E. N. Huh, Cloud of Things: Integrating Internet of Things and Cloud Computing and the issues involved", Proceedings of the 11th

International Bhurban Conf. Applied Sciences & Technology (IBCAST), IEEE, 2014, pp. 414-419.

[28] Ankita Soni and Nisheeth Saxena, Elliptic Curve Cryptography; An Efficient Approach for Encryption and Decryption of a Data Sequence, International Journal of Science and Research, Vol.2, No.5, 2013.

[29] Mohsen Bafandehkar, Sharifah Md Yasin, Ramlan Mahmod, Zurina Mohd Hanapi, Comparison of ECC and RSA Algorithm in Resource Constraint Devices, Proceedings of the International Conference on IT Convergence and Security (ICITCS), IEEE, 2013, pp. 1-3.