ECC based Security Architecture for IoT Cloud Integrated Smart Applications

T.Daisy Premila Bai
Assistant Professor, Department of Computer Science
Holy Cross College, Tiruchirappalli – 620002, India.

Abstract
IoT Cloud integrated smart applications are growing rapidly to make everything smart. Researchers all over the world contribute enormous for the realm of smartness with the maxim of anytime anywhere paradigm. This growing technology is at the risk of security requirements such as authentication, confidentiality, integrity and non-repudiation. Hence in this paper ECC based Security Architecture for IoT Cloud Integrated Smart Applications is presented. The proposed architecture adopts smart card to avail applications anywhere anytime with multilevel security mechanisms. This paper focuses on card level security which is considered to be the major element in securing the entirety of the proposed work. The experimental results prove that the card level security employed is more secure and unique.

Keywords: Internet of Things, Cloud Computing, Smart Card, Security, Elliptic Curve Cryptography

1. INTRODUCTION
Internet of Things (IoT) and Cloud Computing, play a vital role in the era of digital world. [1]. Though the Cloud and IoT have emerged as independent technologies, these two technologies complements in the field of Next Generation Networks. Internet of Things can be enhanced by the unlimited capabilities and resources of Cloud to compensate its technological constraints such as storage and processing. On the other hand, Cloud can extend 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 [2]. IoT based smart objects and cloud integration for storage is a novel conceptual framework which leads to a large number of smart applications. In this context researchers have identified the challenges of IoT and Cloud integration as security and privacy, heterogeneity, reliability and performance. Security and privacy are considered to be the major challenges [3].

IoT and Cloud integration will pave the way to help the users with the rise of empowered and embedded technology with Radio Frequency Identification Technology (RFID). This integrated technology further opens up a new domain of research for the design of smart cards with new functionalities. The portability of smart cards enables their extensive adoption by people worldwide for different applications such as mobile communications, banking and financial services, passport, identity cards, transportation, health care services, education, remote working, etc. [4]. The existing smart cards have been issued by different service providers for varied applications and they are service provider oriented. The existing service oriented transaction cards are not considered to be a smart one. Moreover, every card has its unique Personal Identification Number (PIN). It is very difficult for a common man to remember all the PINs and to carry all the cards. Hence, there is an impelling force from the public to design a Multi-Application Smart Card to access any Smart Services and applications Anywhere at Anytime in the Smart Environment [5].

Integrating a single smart card for multiple applications will certainly acquaint with limitations such as security, interoperability and reliability issues [6]. Security is considered to be one of the major concerns. The various smart card security issues are credential leakage attack, denial of service attacks, forgery attacks [7], mutual authentication, replay attacks, parallel session attacks, reflection attacks, smart card loss attacks, user anonymity [Mishra et al., 2014], offline password guessing attacks, stolen verifier attacks, modification attacks, server spoofing attacks, forward secrecy and insider attack [9].

To mitigate the security issues and to enhance the security features of smart card, the researchers believe that the integration of smart cards with biometrics and elliptic curve cryptographic algorithms will deliver a number of significant benefits to organizations and all sectors which require secure identification system. Researchers all over the world put on efforts to design a Smart Card integrating the intelligence, security and IoT to make use of all the services required by a common man [10]. This smart card may be independent of service provider but cater to the needs of all types of services of the common public which are IoT Cloud integrated. Hence in this paper ECC based Security Architecture for IoT Cloud Integrated Smart Applications using smart card is proposed.

2. SECURITY ARCHITECTURE
The proposed ECC based Security Architecture for IoT Cloud Integrated Smart Applications is designed with end-to-end strong multilevel security using Smart Card such as mutual authentication, confidentiality, integrity and non-repudiation. The mutual authentication of the proposed architecture is to ensure the identity of the Smart Card (SC) and the Smart Reader (SR). Due care and importance is given to ensure confidentiality while accessing smart objects through the smart card. It is also important to ensure that the information
transmitted between Smart Card (SC) and the Smart Reader (SR) is protected from unauthorized access to maintain Integrity and Non-Repudiation. The security requirements of the proposed architecture are augmented by adopting different security mechanisms with the incorporation of Digital Signature, Digital Certificate, One Time Password (OTP), Biometric templates and Elliptic Curve Cryptosystems and Advanced Encryption Standard (AES). Figure 1 depicts the proposed Security Architecture.

In the proposed architecture, the service requester who wishes to access the services through the proposed system, registers at Global Secure Management System (GSMS) with the required user credentials. The Global Secure Management System (GSMS) verifies the user information, generates Unique Identification (UID) Number, creates Biometric Templates for the users, places them on the Smart Card along with the required information and issues the Smart Card to the users. The service providers who offer the services through the proposed system should register themselves in the Global Secure Management System (GSMS) through the website by sending their credentials.

The user enters the service portal with the Smart Card. The Smart Reader activates the Smart Card and performs mutual authentication. Then the Smart Reader reads the Unique Identification (UID) Number from the Smart Card and sends the Unique Identification (UID) Number to the Global Secure Management System (GSMS) for validation through Smart Gateway. If Unique Identification (UID) Number is valid, user is authenticated with biometric match on card process at Smart Gateway. The ‘Success Message’ of user authentication is sent to the Security Gateway.

When the user is authenticated, Global Secure Management System (GSMS) sends the Verification Code to the registered Mobile Device followed by the ‘Welcome Message’. The user activates the ‘Welcome Message’ by entering the Verification Code. When the ‘Mobile Apps’ is activated, list of registered services are loaded on to the users’ Mobile Device. User can choose the respective service and make the Service Request. The Service Request is forwarded to the Security Gateway through Intelligent Smart Gateway and IP/MPLS core. Security Gateway verifies the credentials of the user and the service providers and forwards the service request to the corresponding service provider in cloud platform. Security Gateway receives the service response from the service provider and sends the service response to the user’s mobile device in a secure manner followed by One Time Password (OTP) verification. This process is applicable for all the services since the Unique Identification (UID) Number of the registered users are linked with Service Identification (SID) Number of the registered

![Fig.1 IoT Cloud Integrated Security Architecture](image-url)
service. In this way, one Smart Card (UAISC) with one Unique Identification (UID) Number for all applications and transactions will be realized with the proposed architecture.

This paper proposes strong security for the proposed architecture in various levels namely Card level Security and Architectural Security. This paper discusses the Card Level Security. Card Level Security involves Unique Identification (UID) number generation, Biometric Template creation, Digital Signature Creation and Verification and Issuance of the Digital Certificate.

3. CARD LEVEL SECURITY

The security requirements of the proposed Smart Card (SC) are Privacy, Confidentiality, Integrity and Authentication. This includes secure UID generation, Biometric Template creation, Digital Signature creation and verification and issuance of the Digital Certificate. UID and Biometric templates are digitally signed and stored on the Smart Card (SC) to ensure the privacy of the users and the confidentiality and integrity of the information. Digital Certificate is also stored on the Smart Card (SC) obtained from Certificate Authority (CA) for authentication.

### 3.1. Secure UID Generation

Unique Identification (UID) number generated and discussed in this paper is novel and unique. An Algorithm known as ‘uidgen’ is developed and executed. UID is a twenty digit unique number having four fields namely Country Code (U_Cc), Date of Birth (U_Dob), Security Code (U_Sec) and Card Number (U_Cn). Country Code occupies the first four digits, Date of Birth reserves the next eight digits that is from fifth to twelfth position, Security Code takes the position of thirteenth and fourteenth digits and finally the fifteenth to twentieth digits are reserved for Card Number.

The actual data obtained from the users for the generation of Unique Identification (UID) Number is converted through various security methods and hence the number is a generated one with proposed algorithm ‘uidgen’ in this paper to enhance strong security. The converted Unique Identification (UID) Number is printed on the Smart Card (SC). The Security Code is the key factor to bridge the number printed and stored on the Smart Card (UAISC) and to determine the validity of the Unique Identification (UID) Number. Figure 2 depicts the sample UID to be printed on Smart Card.

![Sample UID to be printed on Smart Card](image)

**Fig.2** Sample UID to be printed on Smart Card
To ensure strong security, the generated UID is converted into 16 byte hexadecimal number and populated in to 16 byte (128 bit) block size using padding bits. These bits of UID are encrypted using Advanced Encryption Standard (AES) with Elliptic Curve Cryptography (ECC) as per the standard of NIST. Figure 3a presents UID in 16 byte block size with equivalent hexadecimal values (10 bytes) and padding bits (6 bytes). The padding bits are appended at the end of the message. Figure 3b presents UID in binary form with padding bits appended.

3.2. Biometric Template Creation

The proposed Smart Card (SC) uses three Biometric Identifiers namely fingerprint, iris and face. Sensors and Camera are used to capture the images and Fingerprint Extractor, Iris Extractor and Face Extractor are used to extract the images. The extracted images are encrypted and digitally signed using Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) and stored on the Smart Card (SC).

3.3. Digital Signature Creation and Verification

The digital signature is an unforgeable piece of data that asserts the sender and provides a higher degree of security and cannot be repudiated. The proposed architecture uses Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signature creation and verification. For digital signature creation and verification of the Smart Card (SC), key pair generation is a prerequisite. The Secure User Registration System (SURS) at Global Secure Management System (GSMS) incorporates Elliptic Curve Cryptography (ECC) and selects the Elliptic Curve $E_p(a,b)$ where ‘$p$’ is greater than 160 and a prime number. Secure User Registration System (SURS) selects another prime number $q$ where ($q < p-1$), chooses the private key ‘$d$’ an integer. Secure User Registration System (SURS) chooses a point on the curve ‘$e1$’ and calculates a point ‘$e2$’ on the curve where $e2=d*e1$. Public Key of the Smart Card ‘$Pus$’ is $(a,b,p,q,e1,e2)$ and the private key ‘$Pur$’ is ‘$d$’.

During the process of Digital Signature Creation, Smart Card chooses a secret random number ‘$r$’, between 1 and $q-1$, creates a point $p(u,v)$, calculates two signatures ‘$S1$’ and ‘$S2$’ and sends the encrypted message ‘$M$’ along with the encrypted signatures $S1$ and $S2$ to the Intelligent Smart Reader.

$$\begin{align*}
P(u,v) &= r * e1 \\
S1 &= u \mod q \\
S2 &= (h(M) + d * S1) r^{-1} \mod q \\
M &= UID/ Biometric Template / MACID
\end{align*}$$

Digital Signature verification process at the Intelligent Smart Reader involves the decryption of the message and the signatures received from the Smart Card, creation of two intermediate results ‘$A$’ and ‘$B$’ and construction of a point $T(x, y)$.

$$\begin{align*}
A &= h(M) S2^{-1} \mod q \\
B &= S2^{-1} S1 \mod q \\
T(x, y) &= A * e1(x, y) + B * e2(x, y)
\end{align*}$$

Then the reader checks the ‘$x$’ with $S1$. If equals the authentication of the Smart Card and the integrity and confidentiality of the message in the Smart Card are ensured.

3.4. Issuance of Digital Certificate

Initially, Secure User Registration System (SURS) of Global Secure Management System (GSMS) requests the Certificate Authority (CA) to issue the Digital Certificate (DC) for Smart Card users. The Digital Certificates are stored on the Smart Card to authenticate the Smart Card users. The issuance of Digital Certificate is depicted in Figure 4.
i. The Secure User Registration System (SURS) of Global Secure Management System (GSMS) submits the Digital Certificate (DC) request to the Registration Authority (RA) for the issuance of Digital Certificate along with the required information such UID, name, gender, DoB and public key of the users.

ii. Registration Authority (RA) forwards the Digital Certificate (DC) application and its information after verification to the Certificate Authority (CA).

iii. Certificate Authority (CA) stores the received information from Registration Authority (RA) in its repository for future reference.

iv. Certificate Authority (CA) signs the certificate with its public key and sends it to Registration Authority (RA).

v. Registration Authority (RA) sends the same to Secure User Registration System (SURS) of Global Secure Management System (GSMS) to store the Digital Certificate in its repository.

vi. Global Secure Management System (GSMS) sends the Digital Certificate (DC) to UAISC Personalisation System (UPS) to write it on the Smart Card.

This end-to-end security are carefully designed and established in this paper and incorporated in the proposed Smart Card (SC).

4. EXPERIMENTAL SETUP AND PERFORMANCE ANALYSIS

The experimental setup has been created to test the performance of the proposed architecture in a lab setup. The performance of the proposed architecture is carried out with regard to ping response time and priority based response time with varied applications.

4.1 Performance Analysis on User Authentication with Smart Card

User authentication is carried out at Smart Gateway Server and analyzed with MatchOnCard process using MegaMatcherOnCard SDK 3.5. It offers matching-on-card technology that stores a person's fingerprint, iris and face templates on a smart card and performs template matching in a microprocessor embedded in the card, instead of matching biometric information on a PC processor. The MatchOnCard method ensures the privacy of the users since the personal biometric information is not transferred to an external computer.

The MegaMatcher extractor has been used to extract the biometric identifier and MegaMatcher matching engine is used to match the live template with the already stored biometric identifier in Smart Card. The biometric identifiers used are fingerprint, face and iris. The comparative study has been made with six users and the average time was observed. For Fingerprint verification the time taken is less than 63.4 milliseconds, for Face less than 42.2 milliseconds and for Iris less than 32.7 milliseconds. Figure 5 depicts the average time taken to perform the user authentication.

![User Authentication using Smart Card](image)

Fig. 5. User Authentication using Smart Card

The results prove that the time taken to perform user authentication using the biometric MatchOnCard process is very less. It takes about only 138.46 milliseconds to execute the verification process of biometric templates including image capturing, extracting, matching, encryption and decryption. It is very much secure and adaptable. Since the extracted features of the users are always kept in the Smart Card, it is highly secured and privacy of the personal information of the users are preserved.

4.2 Priority Based Response Time

There are 500 requesters requesting for various services through smart card in the proposed architecture such as 100 for health care, 100 for transportation, 100 for corporates, 100 for restaurant booking and 100 for banking. Assuming each
requester’s data is about 3 kbps, the total bandwidth allocated is 1 Megabit. When the request reaches the control engine, it classifies the services and process the data according to the priority. Higher priority services are served without any delay. Low priority services are queued and will be processed accordingly.

According to the graph, requests for the health care service has no delay, banking has processed 97% of the request leaving only 3% to be in queue, transportation has processed 95% of the requests leaving the 5% to be in queue, Restaurant has processed 93% request and leaving only 7% to be in queue and corporate have processed only 91% leaving 9% in queue.

Figure 6 depicts the priority based response time obtained through the proposed architecture and Table 1 presents the priority based response time for various requests.

### Table 1: Priority Based Response Time for various Requests

<table>
<thead>
<tr>
<th>Services</th>
<th>No. of users</th>
<th>Packet Drops (%)</th>
<th>Bandwidth Utilized (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health care</td>
<td>100</td>
<td>0</td>
<td>0.292968750</td>
</tr>
<tr>
<td>Banking</td>
<td>100</td>
<td>3</td>
<td>0.284179688</td>
</tr>
<tr>
<td>Transportation</td>
<td>100</td>
<td>5</td>
<td>0.205078125</td>
</tr>
<tr>
<td>Restaurant</td>
<td>100</td>
<td>7</td>
<td>0.146484375</td>
</tr>
<tr>
<td>Corporate</td>
<td>100</td>
<td>9</td>
<td>0.958007813</td>
</tr>
</tbody>
</table>

**Fig. 6: Priority based Response Time**

The results show that the system prioritizes the services and process the requests accordingly, with less packet drops.

### 5. CONCLUSION

The proposed ECC based Security Architecture for IoT Cloud Integrated Smart Applications using smart card is very much secure to avail smart applications anytime, anywhere. The results prove, with all the security mechanisms incorporated at card level in the proposed architecture, the response time for varied applications is less and highly secured. The future work is to develop the architectural level security mechanism for IoT Cloud integrated smart application architecture.

**REFERENCES**


