Multilevel Authentication for Secured IoT Cloud Integration Platform

Dr. T. Daisy Premila Bai
Department of Computer Science, Holy Cross College, Tiruchirappalli, Tamil Nadu, India
daisypremila@gmail.com

Abstract**—** Anywhere Anytime paradigm is achieved with the integration of IoT and Cloud Computing. The integration of these technologies have paved a way for multiple applications to be smart in nature. 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. Hence in this paper Multilevel Authentication for Secured IoT Cloud Integration Platform is proposed with the incorporation smart card and IP/MPLS core switch. This paper discusses the various authentication phases to ensure end to end security. The performance results prove that the proposed multilevel authentication for secured IoT Cloud Integration platform is more secure and feasible to accesses any smart applications securely with one smart card.

Keywords**—** *IoT; Cloud; Security; Authentication; ECC; Smart Card*

I. INTRODUCTION

The World Wide Web has almost become synonymous with the Internet itself in the mindset of every individual [1]. Billions of people around the world rely on the Internet for performing business operations and various tasks [2] Consequently, the Internet infrastructure retains its vital role as global backbone for worldwide information sharing and diffusion, interconnecting physical objects with computing and communication capabilities across a wide range of services and technologies [3]. Hence a novel concept Internet of Things (IoT) arises in which the virtual world of Information Technology integrates seamlessly with the real world of things enabling anytime, anywhere connectivity [4]. The large-scale implementation of IoT devices promises to transform many aspects of the human life. Thus the emergence of smart home, smart cities, smart transaction, smart game, Smart agriculture, etc. [5], [6]. In this scenario, IoT is considered as a part of the Future Internet and will comprise billions of intelligent communicating 'things'. Though IoT is emerging as a novel technology in Next Generation Internet, researchers put on efforts worldwide to integrate the objects with sensors in the cloud-based environment [7]. Cloud Computing allows computer users to conveniently rent access to fully featured applications, to software development and deployment environments, and to computing infrastructure assets such as network-accessible data storage and processing with its salient features of on-demand self-service, broad network access, resource pooling, rapid elasticity and measured Service [8].

Though the Cloud and IoT have emerged as independent technologies, 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 [9].

IoT based smart objects and cloud integration for storage is a novel conceptual framework which leads to a large number of smart applications. The various applications that are made available through the adoption of the Cloud and IoT paradigm are health care, environmental monitoring, smart city, smart logistics, smart home and smart metering, smart energy and smart grid, etc. These applications ensure that integrating IoT and Cloud, the complementary technologies will enhance the Smart World to reach the heights of availing different services and applications anywhere, anytime, any firm and any device irrespective of any underlying technology. 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 [10]. Hence this paper presents the overview of the architecture for IoT Cloud integration with the adoption of smart card and IP/MPLS core switch and elaborates the multilevel authentication employed to achieve end to end security in IoT cloud Integration platform.

II. REVIEW OF LITERATURE

The review of the literature with regard to the integration of Cloud and IoT (CloudIoT) and highlighting the complementarity and the need for their integration was presented by Botta et al. [11]. The authors have summarized the issues solved and the advantages obtained by adopting this paradigm in various aspects such as storage, computation, communication, real time access, scalability, reliability, availability, reduced deployment costs, ease of access and ease of use. Finally, presenting the applications like healthcare, smart city, video surveillance, etc., which are made possible through CloudIoT paradigm, the authors have pointed out the challenges such as the need for standards, new protocols, energy efficient sensing, complex datamining and security mechanisms that need more attention in order to make integrated cloud and internet of things paradigm more conducive and implemented in real time scenario.

Dores et al. [12] have discussed the state of the art technologies such as Next Generation Networks (NGN), Internet of Things (IoT), Wireless Sensor Networks (WSN), Body Sensor Networks (BSN) and Cloud Computing and have evoked the need for the integration of the technologies in making the future internet a reality. The authors have also quoted that the integration of the mobility of the cloud systems and the diversity of IoT will make the day to day life easier. This platform has the ability to register network devices, and the ability to store, update and exchange information. The information is not ciphered and the privacy of the information is not ensured and also the senders and receivers are not authenticated via secure connections. The authors have also performed a Quality of Service (QoS) test in terms of delay and jitter and have suggested that more research work is needed to enhance QoS associated with the security requirements.

Hung et al. [13] have proposed an architecture for Smart Gateway based communication for Cloud of Things (CoT) to filter the unnecessary data and to enhance the efficient utilization of the power. The smart gateway is presented in a layered architecture consisting of seven layers. Describing the functionalities of the smart gateway, the authors have mentioned that the potential future work is required to develop the special type of storage for the data generated by a specific IoT and the development of applications with strong security solutions.

Aazam et al. [14] have coined the term ‘Cloud of Things’ (CoT) for IoT and Cloud Computing Integration. The authors have briefed the concept and the functionalities of IoT layers and Cloud Computing and have shared the necessity of integrating these two paradigms for the effective utilization of the resources and availing the services anytime, anyplace with any device. This integration phenomena creates more business opportunities and equally larger threats from the attackers. The authors have asked the researchers to design a smart gateway which has the extra functionality to do a little processing, before sending the data to the cloud and to develop security mechanisms for IoT and Cloud platform.

Benazzouz et al. [15] have proposed an architecture for Cloud and IoT (ClouT) centric social device network which provides a virtual execution environment and avails access to the IoT devices, by integrating multiple heterogeneous devices using heterogeneous data and protocols. This model provides new business properties for application developers that can reuse information provided by the users. However, the authors suggest the researchers to develop adequate and secured business models which will enable the citizens to get involved in the revenue sharing for providing access to their devices.

Cubo et al. [16] have presented a novel cloud based IoT platform, named DEEP (DPWS (Devices Profile for Web Services) enabled devices platform) to manage the integration and behavior-aware orchestration of heterogeneous devices as services, stored and accessed via the cloud. The authors have validated the implemented platform in a real scenario related to a specific AAL application, concentrating on the usability, scalability, elasticity, latency and the cost. They have demonstrated that the cloud solution eases the management of these systems, allowing simplified user access and effectively handling demanded elasticity. They did insist that the aspect of security is one of the main concerns and it has to be addressed and mitigated.

Zhou et al. [17] have proposed the CloudThings architecture, a Cloud-based Internet of Things platform which accommodates CloudThings Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) for accelerating IoT application, development, and management. They have presented the state of the art for the cloud based IoT and Use Case study for the Things-enabled Smart Home scenario with ‘things’ features and the ‘things’ application characteristics to insist the need for integrated computing, data storage, heterogeneous hardware infrastructure management and other issues such as interoperability, use of IT resources, privacy and security which will enhance the CloudThings architecture to be implemented in real life scenario. The authors have said that this may be a viable approach to facilitate ‘things’ application development which can be extended to many more application domain with the specific emphasis on secure data transmission. It is not yet implemented in real time scenario.

Rao et al. [18] have explained how the Internet of Things and the 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. They have proposed a prototype model for providing sensing as a service on the scientific cloud using a few applications like augmented reality, agriculture and environment monitoring. The authors have suggested that the researchers need to develop mechanisms which are required to mitigate the practical implementation challenges. The security requirements are not yet addressed which are very much essential to implement the proposal.

The review of literature on the recent trends and issues of the integration of IoT and Cloud Computing paradigm envisages the feasibility of constructing security mechanisms. The major challenges in implementing this scenario are the security risks such as authenticity, confidentiality, integrity and privacy. Security risks can be mitigated with the adoption of Elliptic Curve Cryptography (ECC). Hence, in this paper multilevel authentication for IoT Cloud integration platform is discussed.

III. PROPOSED ARCHITECTURE

The proposed Architecture for Internet of Things and Cloud Computing integration is envisaged to avail secure smart services and applications anywhere, anytime with one Smart Card with an end to end security. Smart Card facilitates the secure access of diversified applications and services distributed in a smart environment over the proposed Global Secure Management System (GSMS) with one Unique Identification (UID) Number per citizen through the proposed IoT enabled intelligent systems. For all the transactions this architecture processes the data through a Smart Gateway and then uploads the necessary data in the Cloud through Internet Protocol/ Multiprotocol Label Switching (IP/MPLS). The proposed architecture is depicted in Fig.1.

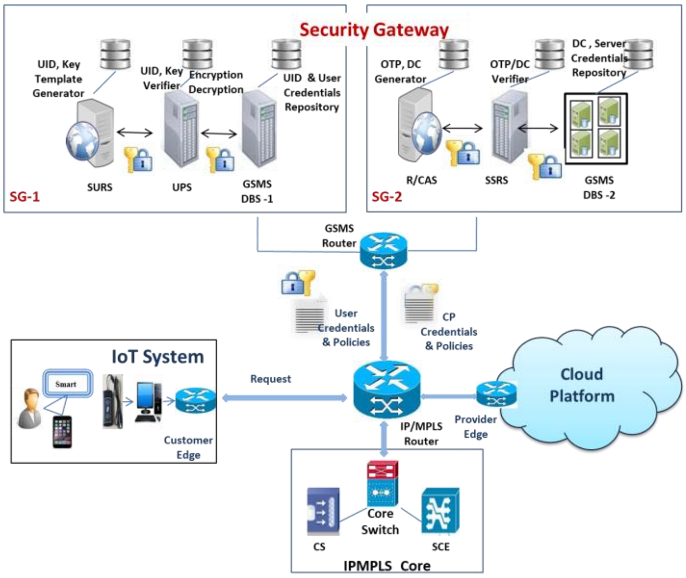


Fig.1 IoT and Cloud Integration Platform

The smart services and applications are deployed in the cloud based environment. The services and the service providers are integrated and connected through a novel IP\MPLS core system wherein the authenticated and registered users and the service providers can access and provide the services through the IoT enabled intelligent system. Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) security are incorporated in the design to ensure complete protection against the security risks. This is a novel This is a novel secure architecture eliminates ambiguity, ensures security and realizes the vision of "one intelligent smart card for any applications and transactions. Multilevel Authentication is adopted to ensure end to end security for the proposed architecture. It consists of eight phases namely Registration Phase, Mutual Authentication between Smart Card and Intelligent Smart Reader, Card Authentication, User Authentication, Mobile Device Authentication, Service Authentication, Secure Service Transmission between Smart Gateway and Security Gateway and Secure Service Transmission between Security Gateway and Service Provider. The functional components diagram of the proposed architecture is depicted in Fig.2.

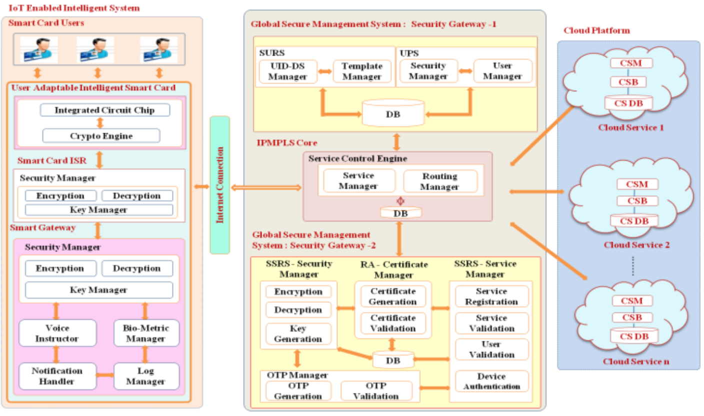


Fig.2 Functional Components Diagram

A. *Registration Phase*

In the registration phase, the information of the users and their mobile devices, Service Providers and their services are to be registered in the Global Secure Management System (GSMS) of the architecture. The Biometric Templates of the users such as finger print, iris and face of the users are also to be registered and stored on the Smart Card. Storing these Biometric Templates on the Smart Card and performing MatchOnCard process preserves the privacy of the users. Secure User Registration System (SURS) of Global Secure Management System (GSMS) verifies the user credentials, generates Unique Identification (UID) Number and key pairs that are required for Digital Signature Creation of the Smart Card users, obtains Digital Certificate and issues the Smart Card to the users. The information elicited from the users and the service providers are stored in the Global Secure Management System Database in an encrypted form using Elliptic Curve Cryptography (ECC). The key pairs used for encryption and decryption are also generated during registration. The Secure User Registration System (SURS) at Global Secure Management System (GSMS) chooses a non-singular Elliptic Curve Ep (a, b) over the finite field GF(p) where 'p' is a prime number and greater than 2^160. It then selects a generator point 'G' on the Elliptic Curve Ep(a, b) as e1 where e1=(x1,y1) and a prime factor 'N' which is the largest prime number where NG=0 and N<p. Secure User Registration System (SURS) randomly chooses a private key Prs where Prs < N and computes e2 = Prs.e1 where e2 ∈ Ep(a, b) and computes its public key 'Pus' as Ep (a, b), e1, e2.

The Global Secure Management System (GSMS) sends public parameters of the Smart Card 'pus', the public key and 'G', the generator point to the authenticated public domain. The public domains are the registered Service Providers registered in the Global Secure Management System (GSMS) to provide service to the registered users. 'Prs', the private key is written on to the Smart Card. Only the registered public domains will have the necessary features to authenticate the Smart Card and provide services.

B. *Mutual Authentication*

In the proposed architecture, the Smart Card is designed as an IoT enabled Smart Card which is to be mutually authenticated with the Smart Reader to ensure its identity and authenticity, when the Smart Card users, using the Smart Card to access the registered services. The information used to perform mutual authentication is the MAC ID of both the Smart Card and the Intelligent Smart Reader. They are hashed into 160-bit integer and stored as CH (hashed MACID of the Smart Card) and RH (hashed MACID of the Intelligent Smart Reader) in the Smart Card and the Smart Reader respectively. As soon as the Smart Card receives the signal from the Smart Reader through RF interface, Smart Card sends the request to the Smart Reader by sending the CH in an encrypted form followed by two cipher texts C1 and C2. Cipher texts are created with a 160-bit integer 'r' the secret random number.

$$C1 = \quad u \bmod q \qquad (1)$$

$$C2 = \quad (CH + d * C1)\ r\ \text{-1mod}\ q \qquad (2)$$

‘q’ is a prime number where (q<p-1) and ‘u’ is the ‘x’ coordinate of a point p(u,v), randomly chosen on the Elliptic Curve Ep(a, b). When the Smart Reader receives the request in the encrypted form, it constructs a point on the Elliptic Curve as T(x,y) by calculating two intermediate results ‘A’ and ‘B’.

$$A = CH*C2-1 \bmod q \tag{3}$$
$$B = C2-1\ C1 \bmod q \tag{4}$$
$$T(x,y) = (A*e1) + (B*e2) \tag{5}$$

If ‘x’ coordinate of the point constructed by Smart Card equals C1 mod q, the Smart Reader calculates two cipher texts C3 and C4 by using its private key ‘f’ and secret random number ‘e’.

$$C3 = x \bmod q \tag{6}$$
$$C4 = (RH + f * C3)\ e\ -1 \bmod q \tag{7}$$

Then Smart Reader sends C3, C4 including C1 and C2 in an encrypted form to the Smart Card for verification. Smart Card receives the message from Smart Reader and decrypts the same with its private key. If C1 and C2 are the same sent by the Smart Card , the authentication process will be further proceeded otherwise it will be aborted. Smart Card sends the value of C3 and C4 in an encrypted form to the Smart Reader for verification. The Smart Reader decrypts the received values C3 and C4 and checks whether it is same as the Smart Reader sent to the Smart Card. If both the values are equal, the authentication is ensured and the communication will be established between the Smart Card and the Smart Reader else communication will be aborted. For every new session both the Smart Card and the Smart Reader will generate new secret random numbers ‘r’ and ‘e’ to enhance the session robustness. For effective and secure communication, the authenticated messages are transmitted to the Smart Gateway in an encrypted form. It prevents an adversary to perform malicious activities and enhances confidentiality.

C. *Card Authentication*

Once the mutual authentication between Smart Card and the Smart Reader is carried out, the next step is to validate Unique Identification (UID) number and to authenticate the Smart Card with the Digital Certificate. The Smart Reader reads the UID from the Smart Card. UID is hashed with SHA 1 algorithm and digitally signed with Elliptic Curve Digital Signature Algorithm (ECDSA). This Digital Signature is appended with the encrypted UID using Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC). It is then sent to the Secure User Registration System (SURS) of Global Secure Management System (GSMS) through Smart Gateway to check the validity of UID with the Global Secure Management System Database. The UID manager of Secure User Registration System (SURS) splits the received message as signed and encrypted UID. UID manager decrypts the UID with the dynamic session key of Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) and hashes with SHA-1 to get the UID digest. The generated UID digest is compared with UID digest in Global Secure Management System Database (GSMS DB). If matches, Global Secure Management System (GSMS) sends the ‘Valid UID’ message and the respective user credentials to the Smart Gateway. Otherwise, Global Secure Management System (GSMS) sends the ‘Invalid UID’ message to the Smart Gateway. The Smart Card is also to be authenticated with the Digital Certificate. The Digital Certificate of the UAISC is retrieved from the Smart Card by the registered Near Field Communication (NFC) enabled mobile device and the request for verification will be sent to the Certificate Authority. The Certificate Authority will verify it with the public key of Smart Card received from the Global Secure Management System (GSMS). If the Certificate is valid, then the Smart Card is considered to be authenticated.

D. *User Authentication*

Once the Unique Identification (UID) number and the Smart Card is validated and authenticated, the voice instructor at the Smart Gateway instructs the user to perform the Biometric Authentication. Three Biometric Templates namely fingerprint, iris and face are used for user authentication. The live templates of the users are created and encrypted using the Mega Matcher Extractor installed at the Smart Gateway. The Digital Signature is also generated for the live template followed by hashing with SHA-1. Multimodal Biometric Matching Engine on the Smart Card executes the matching process by matching the encrypted templates stored on the Smart Card and verifying the Digital Signature with the live encrypted and signed template. If there is a match, the success message of user authentication is sent to the Security Gateway, else the process will be terminated after three attempts.

E. *Device Authentication*

Device Authentication is also to be ensured followed by user authentication. Security Gateway, after receiving the success message of user authentication, sends the encrypted Verification Code to the user’s registered mobile device followed by the ‘Welcome Message’. The user activates the ‘Mobile Apps’ designed for this system by entering the Verification Code. The Code Manager of Secure Service Registration System (SSRS) at Global Secure Management System (GSMS) receives the Verification Code, decrypts it and matches with the verification code sent. If there is a match, then the device is authenticated and the ‘Mobile Apps’ is activated and the list of services are loaded on to the user’s mobile device. The user can choose the service and make a service request. If there exists a mismatch with the verification code, communication will be terminated.

F. *Service Authentication*

Service Authentication is performed followed by User Authentication and Device Authentication. The user makes the service request followed by Card, User and Device Authentication. The One Time Password (OTP) Manager of Secure Service Registration System (SSRS) at Global Secure Management System (GSMS) sends the user interface with UID and asks the user to enter the One Time Password (OTP) sent to the registered mobile device of the user for the particular service or request. The user sends the encrypted OTP to the Global Secure Management System (GSMS). OTP Manager decrypts the OTP with ECC. If the decryption is successful, service will be provided to the user. Else the service is blocked after three attempts. To ensure that the Service Provider is the authorized one, the Cloud Security Broker matches the already stored credentials of the service provider such as Service Identification Number and digital signature with the Global Secure Management System (GSMS). If the credentials are verified, the secure delivery of the services are initiated.

G. Secure Service Transmission between Smart Gateway and Security Gateway

The proposed architecture establishes connection between the Smart Gateway and the Security Gateway after the successful mutual authentication between them with the exchange of X.509v3 Digital Certificate via Transport Layer Security (TLS) Protocol. The Smart Gateway requests a connection with the Security Gateway through the IP/MPLS plug-in. In response, the Security Gateway sends its public key using an ECC based signed server-side certificate X.503v3. The Smart Gateway checks the authenticity of the certificate's issuer from the list of root certificates from trusted CAs listed through the Web Browser. If the signature on the Security Gateway's Certificate matches, then the Security Gateway can be trusted. The session keys are securely exchanged between the Smart Gateway and the Security Gateway. The Smart Gateway can communicate securely over this channel.

The Smart Gateway sends its public key certificate through the IP/MPLS plug-in to the Security Gateway. The Security Gateway attempts to match the signature on the certificate received from Smart Gateway with the CA using the Security Gateway's certificate store. If there is no match for the signature, an SSL error code is generated and returned to the Smart Gateway. If there is a match for the signature, then the Smart Gateway can be treated as trusted. Session keys are securely negotiated between the Smart Gateway and the Security Gateway. Then the secure communication channel is established between the mutually authenticated Smart Gateway and Security Gateway.

The Smart Gateway trusting the Security Gateway sends the encrypted and signed Unique Identification (UID) number received from the Smart Card to the Security Gateway for validation. Security Gateway trusting the Smart Gateway, receives the request, processes the request by decrypting the UID and comparing the UID in Global Secure Management System (GSMS) and sends the 'Welcome Message' with the registered list of services to the user's mobile device through Smart Gateway.

H. Card Authentication

The secure communication is established between the Security Gateway and the Service Provider after the successful mutual authentication with the exchange of X.509v3 Digital Certificate via Transport Layer Security (TLS) Protocol. After establishing secure communication between the Security Gateway and the Service Provider Security Gateway sends the service request in an encrypted form to the Cloud Platform through IP/MPLS core. The Service Engine at IPMPLS decrypts the service request, analyses the service, sets the priority and directs to the Service Provider in the Cloud Platform in an encrypted form. The Cloud Service Manager (CSM) directs the request to the Cloud Security Broker (CSB). The Cloud Security Broker (CSB) decrypts the request and checks the user credentials and the service providers' credentials at Global Secure Management System (GSMS). If both are valid and authenticated, the user interface with Unique Identification (UID) Number and One Time Password (OTP) is sent to the mobile device of the service requester through the Security Gateway in an encrypted form.

The interface decrypts OTP with the server's public key and if it is successful, the service will be provided to the service requester, otherwise the requested service will be blocked after three attempts.

To ensure that the Service Provider is the authorized party, the Cloud Security Broker (CSB) matches the already stored credentials such as the Service Identification (SID) Number and Digital Signature. If the credentials are same, the service request is processed and sent to the Service Requester's Mobile Device through the Smart Gateway. Nonregistered service providers will be blocked.

These procedures ensure and guarantee the end to end security for the proposed architecture with the adoption of Elliptic Curve Cryptography (ECC). The interface diagram of multilevel authentication for the proposed architecture is depicted in Fig.3.

IV. PERFORMANCE ANALYSIS

The multilevel authentication employed for the IoT Cloud Integration Platform is experimented in the lab environment. Mutual Authentication between Smart Card and the Smart Card Reader, User Authentication, Device Authentication and Service Authentication are performed to ensure the end to end security. The performance analysis on System Throughput and Hit Ratio guarantee that the proposed architecture works efficiently with the enhanced performance. The experimental setup involves hardware and software requirements to analyze the performance. Fig.4 depicts the experimental test bed established to study the performance.

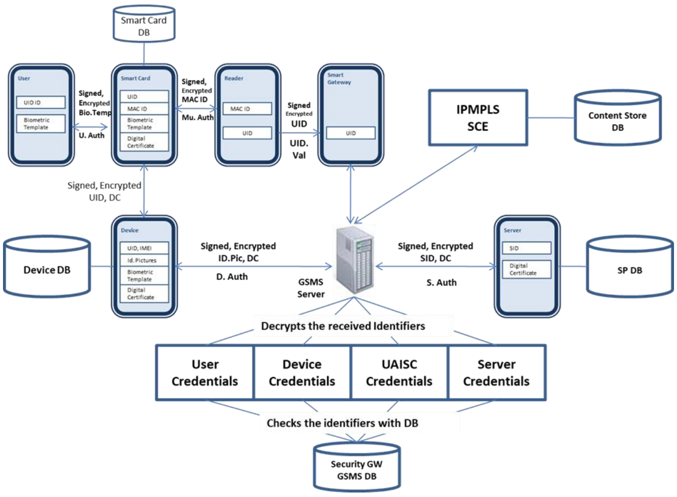


Fig.3 Interface diagram of Multilevel Authentication

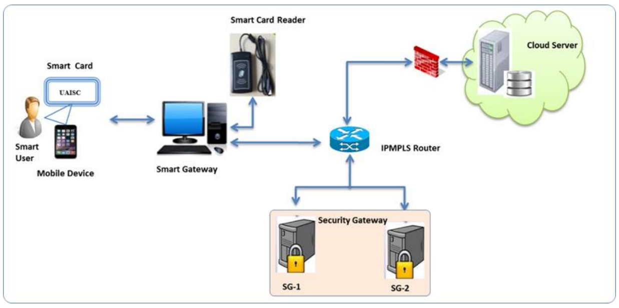


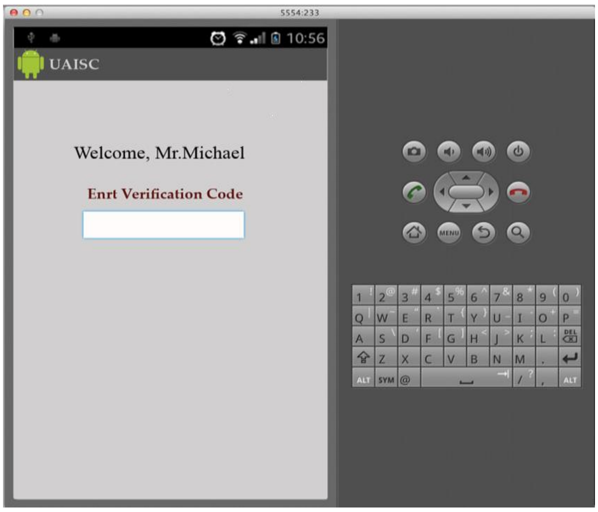
Fig.4 Experimental Test Bed

A. *Performance analysis on Device Authentication*

The user’s Mobile Device is authenticated with the Verification Code sent by the Security Gateway Server after the successful user authentication performed at the Smart Gateway through the User Interface. When the mobile user sends the verification code to the Security Gateway, the security gateway verifies the received Verification Code and activates the ‘Mobile App’ in the Mobile Device. Fig. 5 depicts the User Interface used to perform Device Authentication.

B. *Performance Analysis on Service Authentication*

After the successful device authentication, the proposed security architecture initiates service authentication followed by the service request received by the user. The Cloud Server checks the user as well as service provider’s credentials such as Service Identification (SID) Number and Digital Certificate in Security Gateway Server and sends the One Time Password (OTP) to the User’s Mobile Device in an encrypted form. The user sends the encrypted OTP to the Security Gateway Server. Security Gateway Server decrypts the OTP and does the matching process. The time taken by the Security Gateway Server to do the service authentication for one user is depicted in Fig. 6. The results prove that the time taken to authenticate the service for one user is relatively less. Even for fifty service requesters, the proposed system takes around only 125 milliseconds.



Welcome, Mr.Michael

Enrt Verification Code

Fig. 5 User Interface to perform Device Authentication

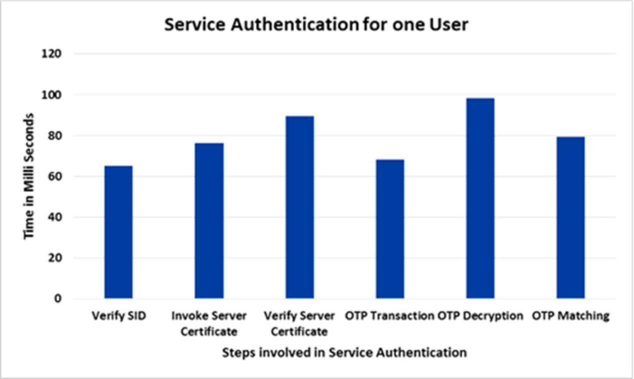


Fig. 6 Service Authentication for one User

C. *System Throughput*

The performance test is carried out to calculate the system throughput. It represents the amount of the work the proposed system does at a given time. To analyze the system throughput IXIA generator is used. Fig.7 depicts the Overall System Throughput of the proposed model. Sample tests have been done with 600 service requesters, requesting for the service in the proposed system.

The system throughput increases gradually as the number of requesters increase. At one point, the system has reached the saturation point due to various factors and the throughput declines. However, the proposed system provides responses to the service requests with a reasonable response time.

D. *Hit Ratio*

The number of hits made on the Security Gateway Server by the Smart Card Service Requesters during each second of the load is observed using the Load Runner Tool. Fig.8 shows the sample output screen shot for the load on the Security Gateway Server by creating 10 Smart Card Service Requesters. This graph is used for determining the number of service requesters on the proposed system at any given amount of time.

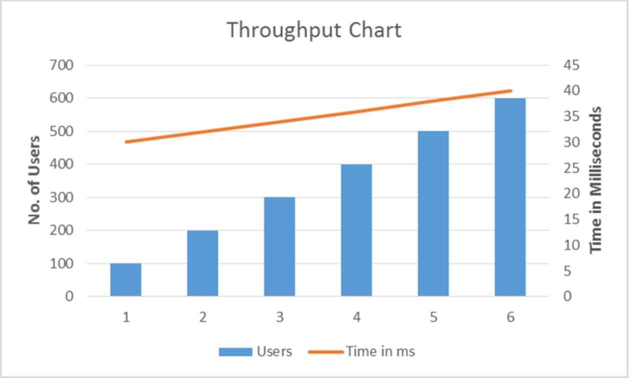


Fig. 7 Overall System Throughput

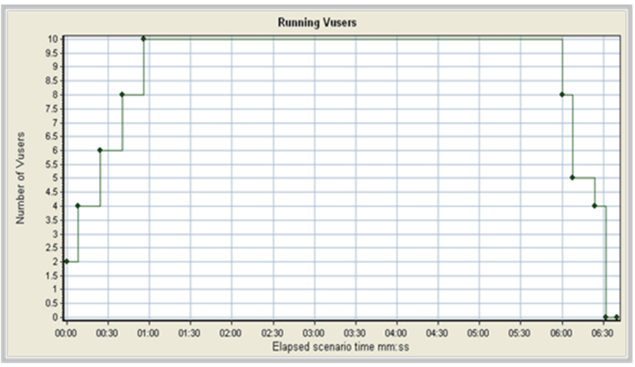


Fig. 8 Sample Screen shot for 10 Users

V. CONCLUSION

The proposed multilevel authentication for IoT Cloud Integration platform enhances security with Elliptic Curve Cryptography (ECC) and Advanced Standard Encryption (AES). This ensures that the proposed research work is highly secured and enhance the security requirements such as authentication, confidentiality, privacy and integrity. This guarantees that the users and the service providers can adopt this proposed architecture to avail and provide services with its salient features of ease of use and end to end security. The future work is to redesign the proposed architecture with IPv6 compatibility to access applications and services anywhere and anytime.

REFERENCES

[1] Ibrahim Mashal, Osama Alsaryrah, Tein-Yaw Chung, Cheng-Zen Yang, Wen-Hsing Kuo, Dharma P Agrawal, “Choices for Interaction with Things on Internet and underlying Issues”, Ad Hoc Networks, ELSEVIER, pp. 1-22, 2015.

[2] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, “Internet of Things: Vision, Applications and Research Challenges”, Adhoc Networks, ELSEVIER, pp. 1497-1516, 2012.

[3] Luigi Atzori, Antonio Iera, Giacomo Morabito, “The Internet of Things: A Survey”, Computer Networks, Vol. 54, pp. 2787-2805, 2010

[4] Michele Zorzi, Alexander Gluhak, Sebastian Lange and Alessandro Bassi, “From Today’s INTRAnet of Things to a Future INTERnet of Things: A Wireless and Mobility Related View”, Wireless Communication, IEEE, Vol. 17, pp. 44-51, 2010.

[5] Shancang Li, Li Da Xu and Shanshan Zhao, “Internet of Things - A Survey”, Information Systems Frontiers, Springer, Vol. 17, pp. 243-259, 2014.

[6] Antonio J Jara, Latif Ladid and Antonio Skarmeta, “The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities”, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 4, pp. 97-118, 2014.

[7] Gyanendra Prasad Joshi and Sung Won Kim, “Survey, Nomenclature and Comparison of Reader Anti-Collision Protocols in RFID”, IETE Technical Review, 2013.

[8] Rajkumar Buyya, James Broberg and Andrzei Goscinski, “Cloud Computing Principles and Paradigms”, pp. 3-5, WILEY Publications, 2011.

[9] Alessio Botta, Walter de Donato, Valerio Persico, Antonio Pescape, “On the Integration of Cloud Computing and Internet of Things”, International Conference on Future Internet of Things and Cloud, IEEE, pp. 23-30, 2014.

[10] Walter de Donato, Alessio Botta, Valerio Persico, Antonio Pescape, “Integration of Cloud Computing and Internet of Things: A survey”, Future Generation Computer Systems, ELSEVIER, Vol. 56, pp. 684-700, 2016.

[11] Walter de Donato, Alessio Botta, Valerio Persico, Antonio Pescape, “Integration of Cloud Computing and Internet of Things: A survey”, Future Generation Computer Systems, ELSEVIER, Vol. 56, pp. 684-700, 2016.

[12] Carlos Dores, Luis Paulo Reis, Nuno Vasco Lopes, “Internet of Things and Cloud Computing”, 9th Iberian Conference on Information Systems and Technologies (CISTI), IEEE,pp. 1-4, 2014.

[13] Pham Phuoc Hung, Mohammad Aazam, Eui-Nam Huh, “Smart Gateway Based Communication for Cloud of Things”, Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, IEEE, pp. 1-4, 2014.

[14] Mohammad Aazam, Imran Khan, Aymen Abdullah Alsaffar and Eui-Nam Huh, “Cloud of Things: Integrating Internet of Things and Cloud Computing and the Issues Involved”, 11th International Bhurban Conference on Applied Sciences and Technology (IBCAST), IEEE, pp. 414-419, 2014.

[15] Yazid Benazzouz, Christophe Munilla, Ozan Günalp, Mathieu Gallissot and Levent Gurgen, “Sharing User IoT Devices in the Cloud”, IEEE World Forum on Internet of Things (WF-IoT), pp. 37-374, 2014.

[16] Javier Cubo, Adrian Nieto and Ernesto Pimentel, “A Cloud-Based Internet of Things Platform for Ambient Assisted Living”, SENSORS, pp.14070-14105, 2014.

[17] Jiehan Zhou, Teemu Leppänen, Erkki Harjula, Mika Ylianttila, Timo Ojala, Chen Yu, Hai Jin, Laurence Tianruo Yang, “CloudThings: a Common Architecture for Integrating the