AN ADAPTABLE SECURE SMART CARD ARCHITECTURE FOR INTERNET OF THINGS AND CLOUD COMPUTING

T Daisy Premila Bai[1], S Albert Rabara[2], A Vimal Jerald[3]

[1,2,3]*Department of Computer Science St. Joseph's College, Tiruchirapalli – 620 002, India*
daisypremila@gmail.com,a_rabara@yahoo.com,vimalgerald@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 literature that integration of IoT and cloud computing is in its infantile phase, that has not been extended to all application domains due to its inadequate security architecture. Hence, in this paper a novel adaptable secure smart card architecture for internet of things and cloud computing is proposed. This is a unique architecture adoptable for the public to have a secure access over 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 with one IoT enabled User Adaptable Intelligent Smart Card (UAISC) through mobile devices. The cloud services are integrated and connected through an IP/MPLS (Internet Protocol / Multi-Protocol Label Switching) core System. Elliptic Curve Cryptography (ECC) is used to ensure complete protection against the security risks such as confidentiality, integrity, privacy and unique authentication. This model eliminates ambiguity, ensures security with enhanced performance and realizes the vision of "one secure smart card for any applications and transactions". The performance of the proposed architecture is tested by establishing a test bed in a simulated environment and the results are reported.

Keywords: *Internet of Things (IoT), Cloud Computing, Smart Card, Security, Elliptic Curve Cryptography (ECC)*

----------***----------

1 INTRODUCTION

Internet of Things (IoT) and Cloud Computing play a vital role in the field of Information Technology [1]. The vision of the IoT is to enable things to be connected anytime, anyplace, with anything and anyone ideally using any path or network and any service in heterogeneous environment [2]. European Research Cluster on the Internet of Things 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 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, 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 [6].

Though the cloud and IoT have emerged as independent technology, merging these two technologies creates renaissance in the field of future networks and in building smart environment. 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 [7]. Consequently, integrating IoT and Cloud, the complementary technologies will enhance the smart world to reach the heights of availing any services and applications anytime, anywhere irrespective of any underlying technology.

'Anytime, anywhere' paradigm gains its momentum in the world of ever increasing use of the Web with the development of emerging technologies in particular mobile devices and smart card systems [8]. Mobile devices and smart cards, the portable devices could complement each other to realize the vision of 'Anytime, anywhere' prototype in the smart machine era in the history of IT arena and in the world of internet of things. In this state of affairs smart cards are considered to be the smart solutions to avail any applications and any services since the smart cards could be easily interfaced with the mobile devices and the card readers.

Existing smart cards are the most secure devices widely used and adopted in many application domains like telecommunications industry, banking industry, health care services, audiovisual industry, transportation, access control, identification, authentication, pocket gaming, e-commerce, remote working, remote banking, etc. with the adoption of the various smart card standards and specifications [9]. The major drawback is that for each application, a user should have an individual smart card. This will undoubtedly fill the wallet of the users with many numbers of cards and leaving them with the difficulty of remembering the personal identification number (PIN) for each application.

Researchers all over the world put on efforts in designing the multiapplication smart card to satisfy the needs of the common public. But no prominent design has been authenticated so far. The existing smart cards in use are intra domain dependent where a card issued for one particular concern has the ability to avail various services and applications provided by the same but not the inter domain services due to security concerns. In addition smart cards have only limited storage and processing capacity. This could be surmounted only with the adoption of cloud technology where it has unlimited storage and processing power.

Hence, in this paper an Adaptable Secure Smart Card Architecture for Internet of Things and Cloud Computing is proposed. Section II presents the review of literature, Section III describes in detail the proposed architecture, Section IV briefs the security algorithms developed for the proposed architecture, Section V presents the experimental study and the performance results and Section VI presents the summary of the proposed architecture with future research direction.

2. REVIEW OF LITERATURE

The review is done with regard to various aspects of smart card technology, IoT and cloud integration, mobile technology and Elliptic Curve Cryptography.

2.1 Overview of Smart Card

Keith et al., [10] have presented an introduction to smart cards and RFIDs and have discussed the various kinds of smart cards such as contact and contactless smart cards/RFIDs and the range of smart card devices from simple ID tag/card, memory tag/card, secure memory/tag card and secure microcontroller ID tag. Enumerating the applications of these devices the authors have provoked to develop a smart card architecture which will replace the multiple smart cards used for different application into one card. Akram et al., [11] have explored the evolution of smart card platforms from a single application platform to a feature-rich multiapplication platforms and have suggested to design a robust architecture for multiapplication smart card which will mitigate the security issues. Kamrul [12] has presented a case study on effective use of smart cards in Sweden and have suggested to design a multifunctional smart card by which people can get more benefits in their daily life.

2.2 Smart Card Applications

Damein et al., [13] have enumerated the most significant domains that are currently using mono application smart cards as telecommunication industry, banking industry, healthcare field, audiovisual industry, identification industry, transportation industry, access control industry and pocket gaming. Sun et al.,[14] have proposed a new model to estimate passenger activity time between boarding/alighting using smart card. Pasquet et al., [15] have designed an interoperable and up-gradable e-student smartcard environment. Long et al., [16] have proposed a health smart card to protect the pregnant women from potential adverse events caused by improper prescription. Though there are several applications adopt smart card, in all cases the authors have recommended to propose a strong security mechanism. Moreover, there is a breakthrough to design multiapplication smart card which will reduce the weight of the wallet in filling with smart cards for each application.

2.3 IoT Enabled Smart Card

Steinberg et al., [17] have developed a novel miniaturized RFID tag photometer for Optical Chemical Analysis Applications. Chen et al., [18] have proposed a passive electron tag for smart card which completes RF communications under CPU control in relatively less time with less energy. Williamson et al., [19] have proposed active tags to make smart cards more secure. Mayes et al., [20] have given the overview of MIFARE Classic which adopts contactless smart cards. The authors have alarmed the need to strengthen the security requirements for there is a possibility of losing data from the card and other threats.

2.4 Smart Card Security

Marimuthu et al., [21] have proposed a secure remote user mutual authentication scheme using smart cards to achieve security requirements which is limited only to password. Lu et al., [22] have proposed an efficient biometrics-based user authentication scheme for remote access using smart cards adopting SHA-256, to implement the one-way hash function and the random-number generator. Wynat et al., [23] have proposed an efficient implementation of palm print verification for smart-cards and suggest to merge different biometrics in order to improve system security. The study reveals that multimodal biometric authentication could be more efficient for multiapplication smart card environment.

2.5 IoT and Cloud Integration

Carols et al., [24] have introduced a platform ‘Skynet’ an open source for the development of IoT Cloud integration in order to store, update and exchange information. Prahlada et al., [25] have proposed Center for Development of Advanced Computing (CDAC) Scientific Cloud (CSC) for IoT to provide on demand access to the resources and to store the data in the cloud. Mohamed et al., [26] have

briefed the necessity of integrating IoT and Cloud which has the effective utilization of the resources and availing the services anytime, anyplace with any device. The limitation is that IoT cloud integration requires strong security mechanism.

2.6 Mobile Technology

Gartner [27] says, "By 2020, the average affluent household will contain several hundred smart objects, including LED light bulbs, toys, smart cards, to name but a few. These domestic smart objects will be a part of the Internet of Things, and most will be able to communicate in some way with an app on a smart phone or tablet which will perform many functions including acting as remote controls, displaying and analyzing information and updating object firmware". To make this scenario more effective and even useful for higher end applications in the smart environment, IoT enabled smart cards can be interfaced with the mobile devices.

2.7 Elliptic Curve Cryptography

Ankita et al., [28] have said that ECC is widely used in devices which has less storage memory especially popularly employed in smart cards. Moncef et al., [29] have said that ECC is computationally more efficient than RSA. 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.

The review of the literature reveals that there exists no one smart card to avail multiapplications and services in real time. But there are proposals to design multiapplication cards for higher end applications with security features. The detailed study on the smart card technology and the integration of IoT and cloud computing paradigm envisages the feasibility of constructing IoT enabled multiapplication smart card. Though the smart card has the limited storage and the processing capabilities, it can securely leverage cloud environment for better processing and data storage and communicate to the real world through the mobile devices. 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 ECC. Hence, in this paper a novel and unique Adaptable Secure Smart Card Architecture for Internet of Things and Cloud Computing is proposed.

3. PROPOSED ARCHITECTURE

The proposed Adaptable Secure Smart Card Architecture for Internet of Things and Cloud Computing is envisaged to avail secure smart services and applications anywhere, anytime with one IoT enabled User Adaptable Intelligent Smart Card (UAISC) in a secured manner. UAISC facilitates the secure access of diversified applications and services distributed in a smart environment over the proposed Global Secure Management Systems (GSMS) with one Unique Identification (UID) number per citizen through the proposed IoT enabled intelligent systems. The proposed IoT enabled intelligent system processes the data at smart gateway and then uploads the necessary data to the cloud through IP/MPLS core network. The core network enables all heterogeneous devices to communicate with one another via TCP/IP and the cloud platform collects the information from the core network via HTTPs REST and stores the same in the cloud datacenters. The smart services and applications are deployed in the cloud environment. They 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 with the support of IoT enabled intelligent system. This is a novel, intelligent and secure architecture to access diversified applications and services distributed in the smart environment through an IoT enabled intelligent system with an adequate security using one UAISC per individual.

Elliptic Curve Cryptography (ECC) algorithm is incorporated in the design to ensure complete protection against the security risks such as confidentiality, integrity, privacy and unique authentication. This model eliminates ambiguity, ensures security with enhanced performance and realizes the vision of "one intelligent smart card for any applications and transactions". The proposed architecture is depicted in Figure 1. The functional components of the proposed architecture are explained subsequently. The architecture is composed of four key components namely IoT enabled Intelligent System, IP/MPLS Core, Security Gateway and Cloud Platform. IoT enabled Intelligent System is comprised of an User Adaptable Intelligent Smart Card (UAISC), Intelligent smart reader, mobile device and Intelligent smart gateway.

The User Adaptable Intelligent Smart Card (UAISC) proposed in this paper is an IoT enabled active card which conforms to the ISO/IEC 14443 standard. It contains an integrated circuit chip (ICC) to provide computational power which allows information to be accessed via contactless readers. It is presented in a four level layered structure. The various layers are physical layer, network layer, security layer and application layer. Figure 2 depicts the proposed layout of the UAISC.

The major UAISC components are hardware components and data elements. The hardware components include 32 Bit CPU, 16 KB RAM, 400 KBROM, 500 KB EEPROM, Radio Frequency Interface, RFID tag, antenna, microprocessor, serial communication port and random number generator. UAISC has the special feature of physical address namely MAC ID which conforms to the IEEE 802 standard format of MAC-48 address form. The proposed UAISC adopts RFID tag specially designed to resist the loss and stolen smart card attack. Cryptoengine enable the UAISC to be more intelligent and secure. UAISC is uniquely identified with 20 digit unique identification number which is generated using newly defined algorithm '*secureuidgen*'.

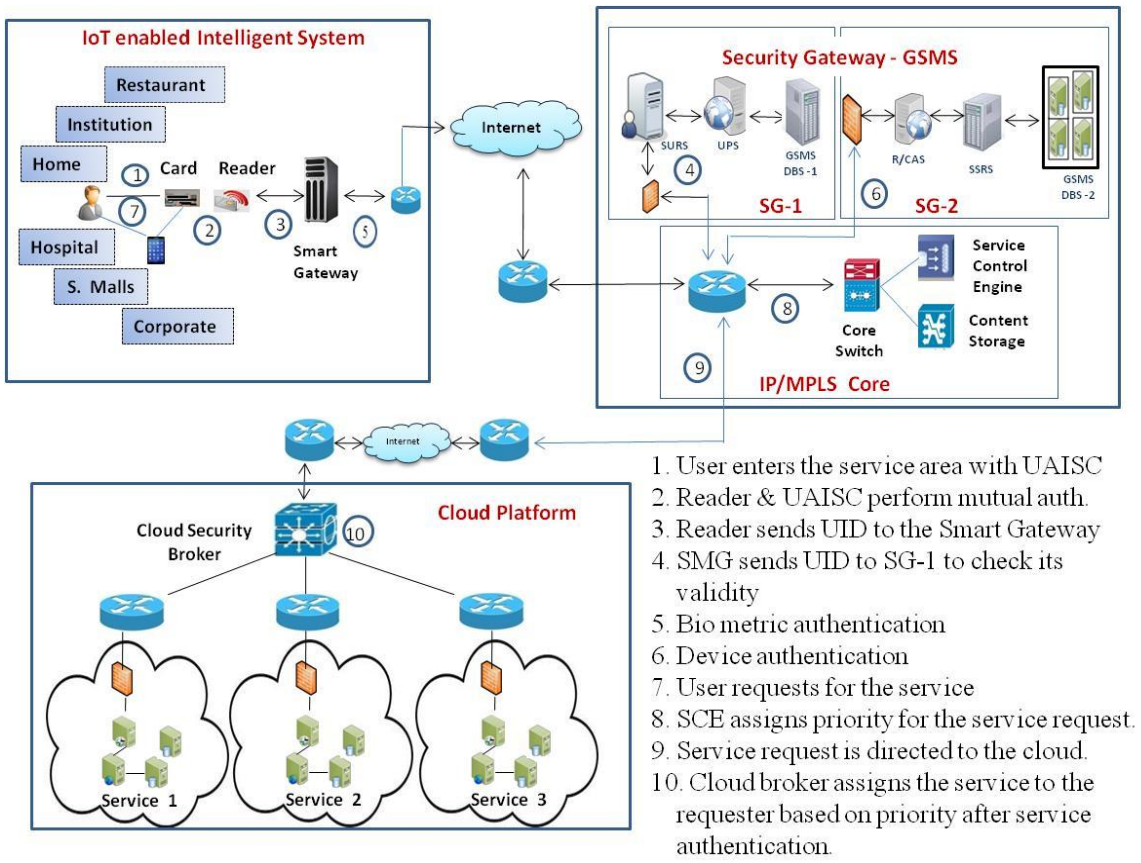

Fig-1: Proposed Architecture

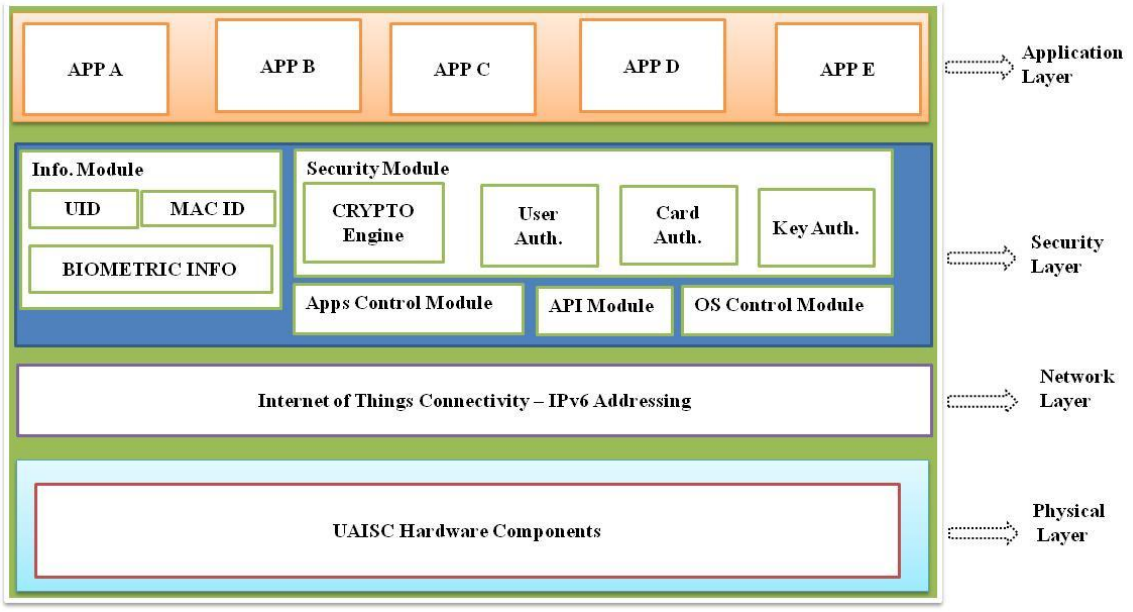

Fig-2: UAISC Layout

The UID is unique and it will not be exhausted even with the population of quintillion people. This UAISC can be the employee ID, student ID, Bank ID, Patient ID, Transport ID, etc. Hence, one user adaptable intelligent smart card (UAISC) can be used to avail any applications and perform financial transactions with one UID. This facilitates the entire system to be unique and secure in nature. The intelligent smart reader is an RFID reader and acts as interface between the UAISC and the intelligent smart gateway and establishes connection between them. No direct interaction between server and UAISC is established, which reduces the UAISC's resource requirements in terms of performance and power supply. The reader device acts as a secure entity.

The smart gateway is the heart of the proposed architecture which plays a vital role in enabling the IoT enabled intelligent system to communicate with the Global System Management Server (GSMS) database of the security gateway for validating the UID of the UAISC. The smart gateway keeps track of all communications initiated by the UAISC, collects the data, stores the data temporarily, performs pre-processing, filters the data, reconstructs the data into a more useful form and uploads only the necessary data to the cloud through core IP-MPLS network.

IP/MPLS core acts as a 'plug-in' in the proposed architecture for IoT enabled intelligent systems, cloud platform and security gateway. It provides secure and fast routing of the packets from source to destination and vice versa in a smart environment which is heterogeneous, based on the shortest path labels independent of any underlying networks by adopting packet switching technology. Service control engine of the IPMPLS switch sets the priority for the services and the information pertained to the services are stored in the content storage database.

Cloud platform is envisioned to be one of the best solutions for the proposed architecture in terms of storage and availing and provisioning of services anywhere anytime. It is assumed that all the services and transactions to be accessed and performed through the proposed architecture are deployed in the cloud environment to substantiate and realize the vision of the proposed architecture. Cloud Manager (CM) and Cloud Security Broker (CBS) play a major role in identifying and directing the services to the users in a secure way through GSMS.

The security gateway designed is named as Global Secure Management Systems (GSMS) which is segregated as Security Gateway-1 ((SG-1) and Security Gateway-2 (SG-2). User credentials such as UID, biometric template and key pairs are generated and encrypted at Secure User Registration System (SURS) of SG-1. SG-2 comprises of Secure Service Registration System (SSRS) which registers the services of service provider in a secure way and it is mainly concerned with the secure generation of OTP, verification and management of service providers' credentials such as SID. Registration Authority System (RAS) and Certificate Authority System (CAS) are the part of the SG-2 to issue the digital certificate for both users and the service providers. GSMS DB-1 and GSMS DB-2 securely stores and manages the data in GSMS. GSMS is global and neutral in nature. The users, devices and the service providers must be securely registered and authenticated in GSMS in order to establish a secure connection between the users and the service providers.

3.1 Security Framework of the Proposed Architecture

The research proposes strong security for the proposed architecture in two levels: Card level and architectural level. These two levels of security are substantiated with multilevel authentication for the proposed architecture. The security framework for the proposed architecture is depicted in figure 3.

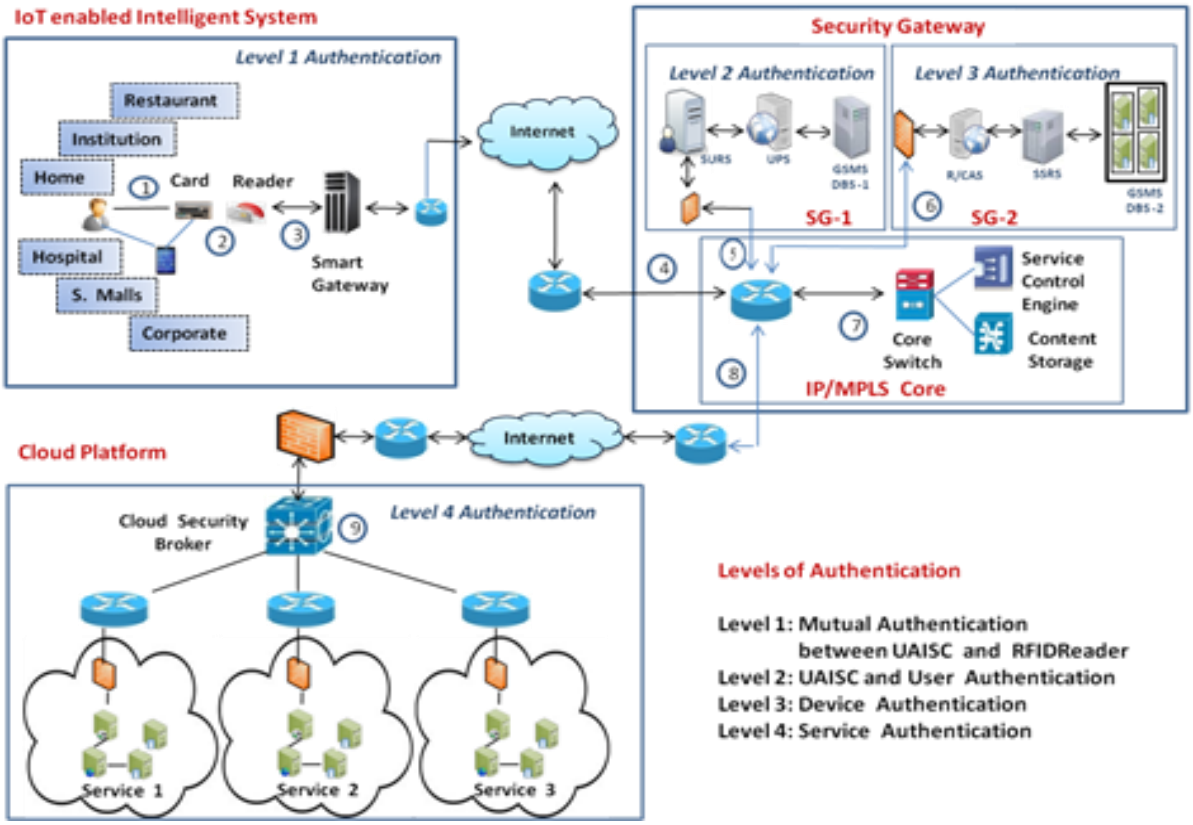

Fig-3: Security Framework

Card Level Security (UAISC): The security requirements of the proposed UAISC are privacy, confidentiality, Integrity and authentication. To make the security requirements of the UAISC more feasible and adoptive, card level security involves secure UID generation, Biometric template creation, digital signature creation and verification and digital certificate. UID and Biometric template are digitally signed and stored on the UAISC to ensure the privacy of the users and the confidentiality and integrity of the information. Digital certificate is also stored on the UAISC obtained from CAS for authentication.

Architectural Level Security: In the architectural level, the proposed security architecture adopts multifactor authentication which consists of seven phases namely initialization, registration, mutual authentication, UAISC authentication, user authentication, device authentication and service authentication. Mutual Authentication takes place between the card and the reader to ensure the authenticity of the UAISC and the RID reader by binding its MAC-ID. UAISC is authenticated with the UID stored on the GSMS SG-1. User is authenticated with digitally signed UID and biometric templates stored on the UAISC. Mobile device is authenticated with the digital certificate and identifiable pictures stored on the mobile device during registration at SG-1. Service level authentication is obtained with digital certificate and OTP generated at SG-2.

3.2 Secure Transmission Between Service Requester And Service Provider

To avail the services with the proposed architecture, the service requester (SR) goes to the smart service premises with the registered UAISC (SC) and the mobile device. The RFID Reader (RR) recognizing the arrival of SC, it powers up and awakens the RFID tag of SC. Then the SC and the RR performs mutual authentication by binding its MACID. When both SC and RR are mutually authenticated, the UID is captured from the SC by the RR and it is validated with the UID stored in the GSMS data base. If it is valid, the information about the user is displayed on the digital board at the entrance of the service premises through smart gateway (SMG) and the SR is instructed to do the biometric authentication. The biometric authentication is carried out with match on card process, since the users' biometric identifiers are stored in the UAISC. If the service requester is identified as legitimate user, device authentication is done with digital certificate and identifiable pictures.

If the user and the device authentication are valid with the respective UID of the SC, welcome message is sent to the mobile device followed by displaying the list of services. The SR chooses the required service and submits the request. The SR's request is encrypted, digitally signed and transmitted to the respective server in the Cloud Platform (CP) via IP/MPLS core after assigning service priority for the service requested, by Service Control engine. The Cloud Manager (CM) sends the service request to Cloud Security Broker (CSB). CSB receives the command form the CM, checks for the availability of the services at the service providers (SP) site and invokes the SP to offer the service demanded. Prior to provisioning the services, the CSB checks the SR credentials, SP credentials and security profile in GSMS.

If SR is found to be valid for the service requested and the SP is authenticated with digital certificate, the service provisioning process will be initiated. To initiate the response from the server side, the server at the service provider's site displays the user interface and sends an OTP to the registered mobile device. The user interface requests the user to enter the OTP. OTP is digitally signed and encrypted with UID and transmitted to the server. Server receiving the encrypted OTP, decrypts the same and checks for its credibility. If it matches, the server processes the request and sends the response to the requester. The service is available to the user. If SP is found to be fake, it will be blocked and the message 'Service Unavailable' will be sent to the mobile device of the SR, by which the SR is provided only with the guaranteed services in the smart environment.

4. SECURITY ALGORITHMS

The various security algorithms constructed to make the proposed system more secure are Secure UID Generation algorithm, Secure GSMS Initialization algorithm, Secure Registration algorithm, Mutual Authentication algorithm, User Authentication algorithm, Device Authentication algorithm, Service Authentication algorithm, algorithm for Secure Communication between the requester and the service provider, point generation algorithm and encryption and decryption algorithm. The proposed security algorithms are tested and the performance study has been carried out and presented.

5. EXPERIMENTAL STUDY AND PERFORMANCE ANALYSIS

The main objective of the experimental study is to test the functionality of the proposed architecture and to measure the time taken with respect to biometric on card matching, user authentication, device authentication, UAISC authentication, UID validation, service authentication, system throughput, hit ratio and request response time in terms of encryption and decryption using Elliptic Curve Cryptography (ECC) and message signing using ECDSA. The performance of the proposed architecture with the above mentioned criteria is carried out in a lab environment. The simulated results obtained are tabulated and graphically presented.

5.1 Experimental Setup

The experimental setup has been established for the proposed architecture by creating a Test Bed in a lab environment. The experimental setup involves hardware and software requirements to analyze the performance of the proposed architecture.

Hardware Requirements: The test bed of the proposed system consists of the security components of the UAISC, intelligent smart reader, Mobile device, smart gateway,

security gateway, IPMPLS core and cloud platform. Servers of varied configuration are used as smart gateway server, security gateway server and cloud servers.

Software Requirements: The software requirements of the proposed architecture are virtual smart card emulator, megamatcher software development tool kit, bouncy castle package, Elliptic Curve Cryptography package and IXIA generator.

5.2 Performance Analysis

The performance of the proposed architecture is carried out with regard to latency analysis, ping response time, priority based response time, M2M testing and system throughput.

Latency Analysis: Latency is the amount of time taken to transmit all the data from source to destination. The latency is measured by varying the packet size from 1250 bytes to 10000 bytes. Figure 4 represents the latency value derived. The latency result proves that it significantly takes less time.

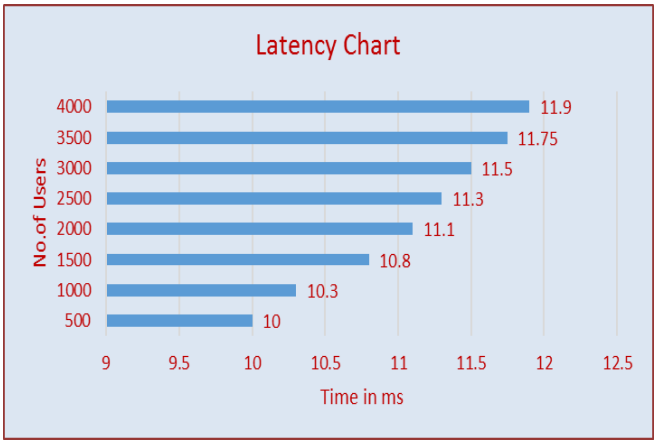

Fig-4: Latency Graph

Ping Response Time: To analyse the ping response time for the proposed system, the sample data set for the requesters ranges from 500 to 4000 were taken with the increase of 500 requesters assuming each requester's data is about 3 kbps and providing the bandwidth about 12 mbps. Figure 5 presents the ping response time graph.

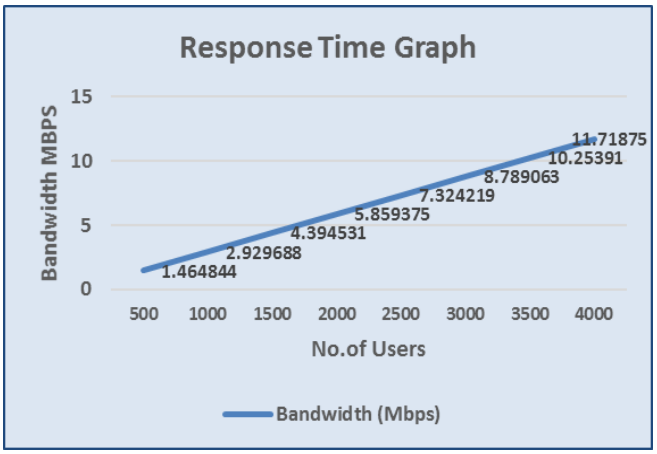

Fig-5: Ping Response Time

The results show that there is only minimal delay which is just 10 seconds even for the 4000 requests, which proves the efficiency of the proposed system in processing the requests faster with no drops of the packets.

M2M Testing: M2M testing refers to the technology that allows Machine to Machine (M2M) communication. Testing is done by customizing networks to support traffic generated from smart gateway (SMG) to Security Gateway (SG), SG to Cloud Security broker (CSB) and from CSB to mobile device (MD). M2M analysis for the proposed architecture is studied by sending 64 bytes size packets between SMG to SG, SG to CSB and CSB to MD. The Reachability Convergence is measured independently for users ranging from 100 to 500 with the increase of 100. Figure 6 indicates the output observed.

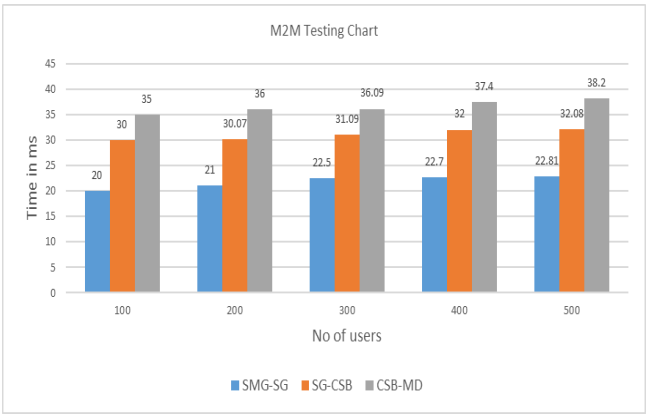

Fig-6: M2M Test Result Graph

It is observed from figure 8 that the convergence of packets from SMG-SG, SG-CSB and CSB-MD gradually increase with the increase of the users in relatively less time.

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. Figure 7 depicts the overall system throughput.

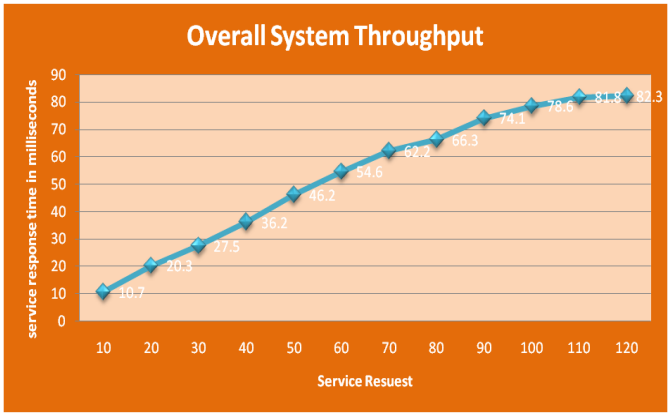

Fig-7: Overall System Throughput

The system throughput is analyzed for different loads on the server with 10 to 100 service requests. Sample tests have been done with 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110 and 120 service requesters, requesting for the service in the

proposed system. The system throughput increases gradually up to 10 requests and keeps rapidly increasing till 120. At one point, the system has reached the saturation point due to various factors and the throughput declines. However, the result proves that the proposed system provides responses to the service requests with a reasonable response time.

Comparison of Public Key Cryptosystems: The comparison of public key cryptosystems has been carried out with bouncy castle package. 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. Figure 8 presents the comparative graph for ECC and RSA.

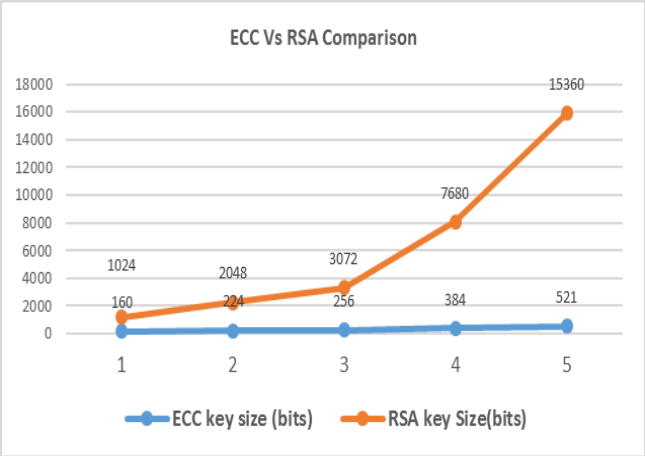

Fig-8: ECC vs. RSA

The overall performance analysis of the proposed system proves that the proposed system is very efficient in processing the request in relatively less time.

6. CONCLUSION

The proposed Adaptable Secure Smart Card Architecture for Internet of Things and Cloud Computing realizes the vision of the future networks to avail any applications and any services irrespective of any underlying technologies anywhere, anytime with one User Adaptable Intelligent Smart Card (UAISC). This UAISC is unique and the users can carry one smart card for any applications and transactions in a smart environment. By implementing this architecture, the UAISC can be used to avail on premise and off premise applications with one Unique Identification Number (UID), connect people and enable automatic machine to machine communication. This system eliminates ambiguity and enhances security.

The simulated results prove the performance of the proposed system. This guarantees that the users and the service providers can adopt this system with its salient features of ease of use and security. The future work is to design the quality of service framework for the proposed architecture.

REFERENCES

[1]. Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems, Vol. 29, pp. 1645–1660, Elsevier, 2013.

[2]. Dr. Ovidi Vermesan, Dr. Peter Friess, "Internet of Things from Research and Innovation to Market Deployment", River Publishers. Aalborg, Denmark, 2013.

[3]. IEEE – SA, "Enabling Consumer Connectivity through Consensus Builiding", 2012. online at http://standardsinsight.com/ieee-company-detail/consensus-building.

[4]. Rodrigo Roman, Pablo Najera, and Javier Lopez, "Securing the Internet of Things", IEEE Computer Society, Vol.44, pp.51-58, IEEE, 2011.

[5]. Lee Badger, Tim Grance, Robert Patt-Corner Jeff Voas, "Draft Cloud Computing Synopsis and Recommendations", NIST, 2011.

[6]. Rajkumar Buyya, James Broberg, Andrzei Goscinski, "Cloud Computing Principles and Paradigms", WILEY Publications, 2011.

[7]. Atkins, C., "A Cloud Service for End-User Participation Concerning the Internet of Things", SITIS, pp. 273-278, IEEE, 2013.

[8]. Raghu Das, "NFC-Enabled Phones and Contactless Smart Cards 2008–2018", Card Technology Today, 2008.

[9]. Xu JunWu, Xie Fang, "Developing Smart Card Application with PC/SC", Internet Computing and Information Services, pp. 286 – 289, IEEE, 2011.

[10]. Keith Mayes and Konstantinos Markantonakis, "An Introduction to Smart Cards and FRIDs", Secure Smart Embedded Devices, Platforms and Applications, Springer Science, New York, pp. 3-25, 2014.

[11]. R. N. Akram and Konstantinos Markantonakis, "Rethinking the Smart Card Technology", HAS 2014, LNCS 8533, pp.221-232, Springer International Publishing Switzerland, 2014.

[12]. Md. Kamrul Islam, "Effective Use of Smart Cards – A Case Study of Smart Cards in Sweden", UMEA University, 2012.

[13]. Damien Sauveron, "Multiapplication Smart Card: Towards an Open Smart Card?", Information Security Technical Report 14, pp. 70-78, ELSEVIER, 2009.

[14]. Lijun Sun, Alejandro Tirachini, Kay W. Axhausen, Alexander Erath and Der-Horng Lee, "Models of Bus Boarding and Alighting Dynamics", Transportation Research Part A 69, pp.447-460, Elsevier, 2014.

[15]. Marc Pasquet, Ndiaga Faye and Sylvie Gerbaix, "Multi-service Card for Students using JavaCard Global Platform and IAS specifications The access control use case", CTS, pp. 185-190, IEEE, 2013.

[16]. An-Jim Long, Polun Chang, "The effect of using the health smart card vs. CPOE reminder system on the prescribing practices of non-obstetric physicians during outpatient visits for pregnant women in Taiwan, international Journal of Medical Informatics 81, pp. 605–611, Elsevier, 2012.

[17]. Matthew D. Steinberg, PetarKassal, BiserkaTkalcec, IvanaMurkovic Steinberg, "Miniaturised Wireless Smart Tag for Optical Chemical Analysis Applications" Talanta 118, pp.375–381, Elsevier, 2014.
[18]. Kuilin Chen, Dongyan Zhao, Haifeng Zhang, Yubo Wang and Liang Liu, "13.56 MHz Passive Electron Tag for Smart Card Application with High-Security", IEEE, 2013.
[19]. Avery Williamson Sr., Li-Shiang Tsay, Ibraheem A. Kateeb, Larry Burton, "Solutions for RFID Smart Tagged Card Security Vulnerabilities", AASRI Procedia 4, pp.282 – 287, Elsevier, 2013.
[20]. Keith E. Mayes and Carlos Cid, The MIFARE Classic Story", Information Security Technical Report 15, pp.8-12, ELSEVIER, 2010.
[21]. Marimuthu Karuppiah and R. Saravanan, "A Secure Remote User Mutual Authentication Scheme using Smart Cards", Journal of Information Security and Applications 19, pp. 282-294, ELSEVIER, 2014.
[22]. Jian-Zhu Lu, Ting Chen, Jipeng Zhou, Jinjin Yang, and Junhui Jiang, "An Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards", CISP, pp.1643-1648, IEEE, 2013.
[23]. Rafael Soares Wyant, Nadia Nedjah, and Luiza de Macedo Mourelle, "Efficient Biometric Palm-Print Matching on Smart Cards", ICCSA 2014, Part VI, LNCS 8584, pp. 236–247, 2014. Springer International Publishing Switzerland 2014.
[24]. Carlos Dores, Luis Paulo Reis, Nuno Vasco Lopes, "Internet of Things and Cloud Computing", Portugal, 2014.
[25]. Prahlada Rao B. Payal Saluja, Neetu Sharma, Ankit Mittal, Shivay Veer Sharma, "Cloud Computing for Internet of Things & Sensing Based Applications", Sixth International Conference on Sensing Technology (ICST), IEEE, 2012.
[26]. Mohammad Aazam, Imran Khan, Aymen Abdullah Alsaffar, Eui-Nam Huh, "Cloud of Things: Integrating Internet of Things and Cloud Computing and the Issues Involved", Proceedings of the 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST), Islamabad, Pakistan, IEEE, 2014.
[27]. Gartner Identifies Top 10 Mobile Technologies and Capabilities for 2015 and 2016. Egham, UK, 2014. http://www.gartner.com/newsroom/id/2669915.
[28]. Ankita, S., Nisheeth, S., "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]. Moncef, A., Amar, S., "Elliptic Curve Cryptography and its Applications", Proceedings IEEE International Workshop on Systems, Signal Processing and their Applications (WOSSPA), 9^{th} -11^{th} May, Algeria, pp: 247-250, 2011.