International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 14813-14828

http://www.ripublication.com

An Architecture For Secure Mobile Database Transaction For Corporate Environment

D. Sathiya, T. Daisy Premila Bai, J. Ronald Martin, S. Albert Rabara

Dept. of Computer Science,
St. Joseph's College (Autonomous),
Tiruchirappalli- 620 002, India
dsathya25@gmail.com, daisypremila@gmail.com,
martinronald.007@gmail.com, a_rabara@yahoo.com

Abstract

The frequent use of mobile devices to access the sensitive data of the corporate environment envisages a new challenge in maintaining an adequate level of information security and the managers of the corporate world are faced with decision making problem in providing restricted access to the personnel of the corporate. In this scenario ensuring the protection of the sensitive data of the corporate while accessing through mobile device is one of the main concerns in recent days in the field of information and communication technology. There are several efforts have been taken by the researchers to propose an unified secure architecture to access the corporate data through mobile devices. Yet there is no significant work found to be more secure and reliable. Hence, in this paper a novel architecture for secure mobile database transaction for corporate environment has been proposed. The main feature is both the mobile and corporate database include ECC based hardware cryptographic coprocessor to enhance secure data transaction. The performance of the proposed architecture is tested in a simulated environment and the results are presented.

Key words: Mobile database, Elliptic Curve Cryptography, Database security, Cryptographic Co-Processor.

1. Introduction

Greater flexibility and technological agility of the recent developments in information and communication technology eliminates the need of the desktops and enhances the employees to access its customer relationship management (CRM) application on their mobile devices and enables the users to transform their operating models and customer propositions [1]. This unique feature has drawn the attention of corporates

around the world to widely integrate mobility into their workforce support and business applications which will increase the accessibility of the corporate data through mobile devices. Hence, corporates in a broad cross section deploy an increasingly wide range of mobile devices and technologies, enabling the employees to perform essential tasks better that drive revenue and deliver value to customers [2].

It also impells a growing number of corporates to encourage their employees to bring their own mobile devices to work to experience the new era of the "always connected" which certainly presents a myriad opportunities for instant information sharing and transactions in the corporate sectors [3]. Consequently the corporate personnel use mobile devices, to connect to the corporate networks via WiFi, UMTS, etc., to have uninterrupted access to corporate databases and information which enhances the working process and decision making [4].

As the adoption of mobile device-based application accelerates and corporates become more dependent on these computing assets, their operational readiness, defined by availability and performance, have a growing impact on the bottom line. The scale of mobile device proliferation within a corporate environment for data transaction are morphing into a mixed device pool comprised of thousands of enterprise and consumer-grade devices used on a daily basis by a large, diverse, and often geographically dispersed workforce. Organizations that leverage mobility to boost productivity enhances the customer experience and improves transaction performance with increasingly complex mobile device environment [5].

The mobile devices which play a vital role in accessing information system not only getting smarter in their computing capabilities, but are also evolving from lower-generation network connectivity (2G) to higher-generation network connectivity (3G, 3.5G, and 4G or LTE). This faster network connectivity, combined with higher bandwidth and intelligent networks attracts the corporate personnel for the wide adoption of advanced mobile devices to access data anywhere and any time irrespective of any underlying technology [6].

Corporates with mobility initiative have the highest grade sensitive information and they are faced with managing complex deployments, standardizing across regions, maintaining consistent processes and proactively identifying and solving problems [7]. The managers of the corporate world today face with a problem of enforcing restricted data access to ensure secure data transaction. It is considered to be a great challenge of accessing sensitive corporate information through mobile devices and it entails the competitive pressure to deploy new mobile technologies faster while simultaneously minimizing risk during the data transaction [8].

The state of the art survey presents that the researchers have carried out an sample amount of work in proposing a secure data transaction while accessing corporate information through mobile devices. None of the efforts seem to be more effective and efficient.

Hence, in this paper a novel architecture for secure mobile database transaction for corporate environment has been proposed. The main feature is both the mobile and corporate database include ECC based hardware cryptographic coprocessor to enhance secure transaction between mobile devices and corporate servers. This paper is organized as follows: Section 2 provides a survey of related

research. Section 3 presents the proposed architecture. Section 4 illustrates the experimental setup and performance analysis are explained in section 5. Section 6 concludes the paper.

2. Review of Literature

Seth et al. [9] have proposed a model for Android application to process and display summarized corporate data which will help the corporate managers in the decision making process. The various components of this model include a web application to input data, database to store information in the central server, an application programming interface that takes requests from the Android application and gives the results back and an Android application to process and display the results. This model helps to analyse data quickly and able to make faster decisions. It also provides flexibility for the corporate personnel to access the corporate data on the move and to have up-to-date information on their Android device wherever they find themselves with an active data connection. This model does not guarantee secure data transaction. The future work of the authors is to incorporate artificial intelligence techniques for data mining and integrate security mechanisms for secure transactions.

Blaz et al. [10] have done a survey on mobile devices and corporate data security. They have said that in the era of mobile penetration, ensuring the protection of corporate data is one of the main concerns. They have also dealt in detail the mobile usage in a corporate environment and have given its statistics. They did narrate about the blended threats sent to the mobile devices which cause significant danger to individuals and corporates. It has the ability to unlawfully acquire restricted information of the corporate and can profit from this. Enumerating the security risks and safe usage of mobile devices, they did present the current security solution available today to minimize the risk of accessing the corporate data through the mobile devices. They did describe that the current safety measures only can protect the mobile devices and software and have pointed out that there is no system which could enable the corporate to monitor the information system and have secure transferring of information through the mobile devices.

Erez Shmueli et al. [11] have analyzed and compared five traditional architectures for database encryption and showed that existing architectures have the capability to provide secure transaction in a low level, affecting the performance of the entire system. The authours have proposed a new architecture, in which the encryption module is placed inside the database management software (DBMS) and a dedicated technique is used to encrypt each database value together with its coordinates. These properties allow to achieve a high level of data security while offering enhanced performance and total transparency to the application layer. The authors have evaluated the performance of the various architectures, both analytically and through extensive experimentation. The results exhibit that the suggested architecture outperforms the others in more realistic scenarios, where only a part of the database content is stored in the database cache. The authors have only given the benefits of using crypto operations and it has not been implemented and not validated how secure is the data transaction in real time.

Britto et al. [12] proposed a system model and protocol for Mobile Payment Consortia System (MPCS) which performs end to end secure payment transactions using SMS services through mobile devices. MPCS supports the security properties such as party authentication, message confidentiality, message integrity, authorization, availability, and non-repudiation. The authors have explained the workflow of the proposed system in terms of communication protocols. There are five entities involved in this proposed scheme which includes Mobile Client (MC), Mobile Payment Consortia Server (MPCS), Student Bank Server (SBS), Institution Bank Server (IBS), Institution Server (IS). The sub-entities to the SBS and IS are Authentication Server for Bank (ASB), Authentication Server for Institution (ASI). The security protocols used in this model with symmetric key cryptography techniques reduces the complexities of computation and the payment process and also reduces the transactional cost for both the students and the educational institutions. The authorssuggest that this framework can be adopted for any systems to have secure data transaction.

Narendiran [13] has proposed a security framework architecture to carry out mobile banking transactions. This framework enables the developers to access the sensitive data and provides a solution for securing sensitive data access over the wireless network with a Mobile Information Device Profile (MIDP) enabled device. This helps the users to access the banks and performs secure transactions anytime, anywhere through their mobile devices with two security levels namely device authentication and user authentication. The banking services are enhanced with this proposed architecture. The author has said that the research area is still young and new challenges may evolve with the advancements of sophisticated mobile technologies. The author has suggested that the mobile device is one of the best solutions to have a secure access over sensitive information, irrespective of where they are physically located.

Fan Mingyu et al. [14] presented a general design of cryptographic co-processor, which can select different algorithms through programming, and perform crypto operations such as key management, data encryption, and decryption, implemented in FPGA. In this proposed design, the Algorithm Library Memory on board holds all selectable crypto algorithms and the controller receives the instructions via PCI bus and programs the FPGA to perform the algorithm selected by the user. The system controller instructs the co-processor to perform either encryption or decryption and the processed data is sent back to the host via PCI bus. This proposed design has been verified by the testing system. The authors have recommended that the further work is still needed since it faces several issues like processing speed, reconfigurability and the security of the coprocessor itself to secure transactions of data with high performance.

Steffen et al. [15] have proposed a design of a low power asynchronous elliptic curve cryptography coprocessor to reduce the power consumption with limited area overhead and to reduce the risks of the side channel attacks occur in a networking environment by hardening cryptocores. They have provided the theoretical base of this cryptographic technique, the description of the design flow and the case study. To demonstrate the benefits of the design flow, they have generated

two versions of the ECC processor: one with the square unit written in VHDL and optimized with Synopsys Design Compiler and the other one is without manual optimizations which was completely specified and synthesized with Balsa. To evaluate the work presented, they have created a layout and compared this with a synchronous implementation and the results show that it has achieved the goal of reducing the power consumption and the further work is needed with respect to the side channel attacks in order to enhance secure transaction.

The review of the literature has revealed that there exist a few secure architectures and framework to access information through mobile devices and to mitigate the security issues arise during mobile transactions. Yet there is no such proposal has been implemented with the use of cryptographic coprocessor to have a secure data access through mobile devices with higher performance. In this paper, a novel architecture has been proposed for secure mobile database transaction for corporate environment which integrates ECC based hardware cryptographic coprocessor in both mobile and corporate databases.

3. Proposed Architecture

The proposed architecture is a Hardware based Cryptographic Co-Processor (CCP) which can be implemented on Mobile Platforms and corporate servers. This architecture enables the Mobile Application to perform hardware based crypto algorithms for encryption/decryption operations targeting towards accessing secure corporate databases/applications. The proposed CCP is a standalone coprocessor capable of providing hardware acceleration in order to relieve the system from the computational burden associated with the various cryptographic functions. Figure 1 depicts the proposed architecture.

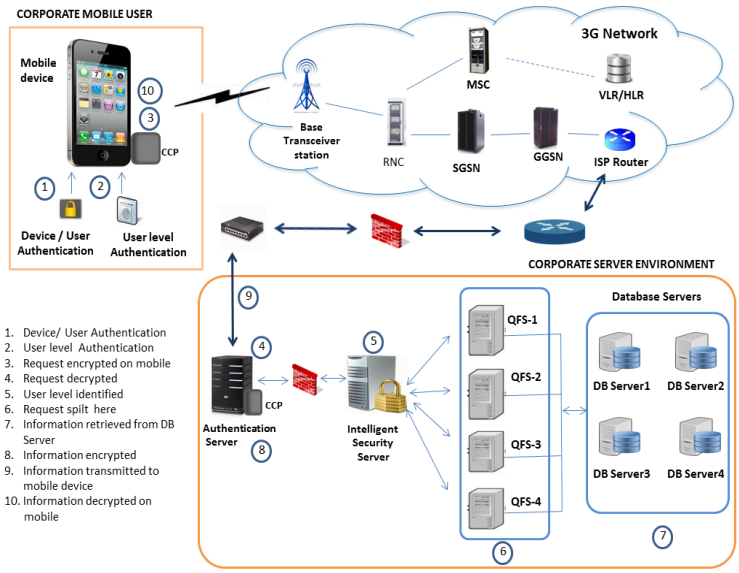

Figure.1 Secure Mobile Database Transaction for Corporate Environment

3.1 Components and Overall Functionalities of Proposed System

The proposed architecture consists of Mobile Client (MC) Device which has a CCP enabled processor and the Corporate Server (CS) which also has a CCP enabled server processor.The mobile device contains the client application which helps to establish the secure connectivity with the corporate servers through 3G network connection and to access the employee data such as salary details, personal details, emails and other sensitive services. Additionally, the client application enables configuration of security settings to protect the organizational data on the user's device. This will accept the authentication request and sends the same to the authentication server for processing. After the three levels of authentication process such as device authentication, user authentication and server authentication, the mobile client interface generates the user's request and sends it to the corporate server. Finally, the corresponding information is loaded on the mobile device from the corporate server.

The Corporate server includes Authentication Server (AS), Intelligent Security Server (ISS), Query Filtering Servers 1-4 (QFS) and Database Servers 1-n (DBS). Figure 2 depicts the flow diagram of the proposed architecture. The functionalities of the proposed architecture are presented below.

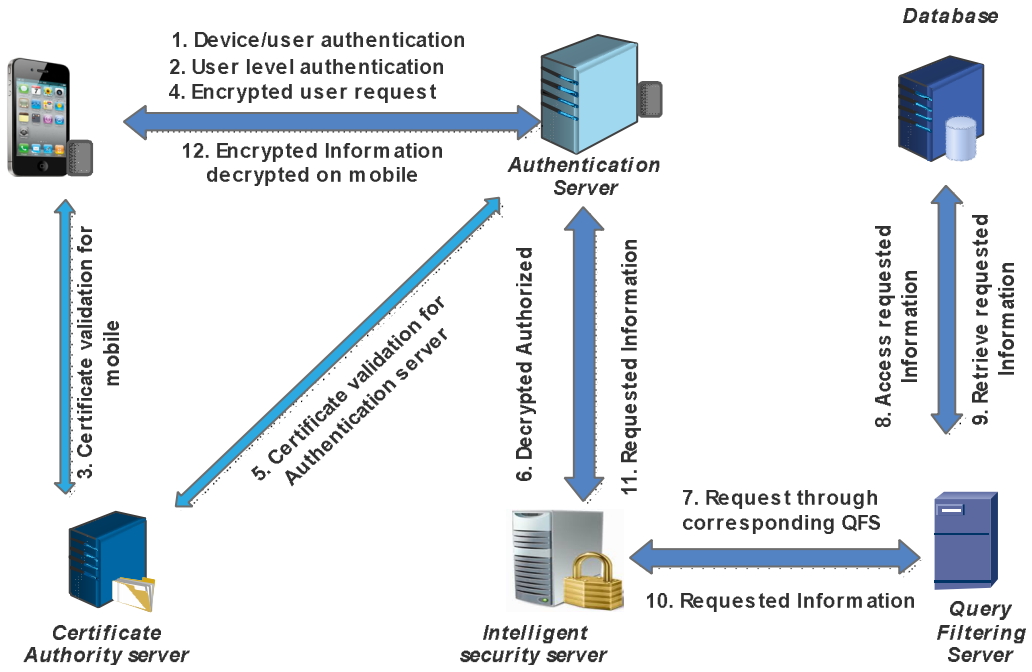

Figure 2: Flow Diagram of the Proposed Architecture

3.2. Employee Registration Process with Corporate Server

In any corporates, the Human Resource (HR) department collects employee's personal information and creates an employee database. The HR administrator permits the employees who need to have access to the database with the criteria that

the employee should have already registered and confirmed registration with a User Id and password. The User Id and password are created by HR administrator and sent to the employee's already registered email. The Authentication Server generates a unique mobile client application using the MACID of the registered employee's mobile device and will be transferred to the registered mobile number of the employee for the activation process.

3.3. Activation Process

During the time of activation, the client application checks the MACID of the mobile device with the registered MAC ID. If MAC ID matches, then the client application ensures the integrity of the employee's device. After the verification of MAC ID, ECC based public and private key pairs are generated. The public key is sent to the corporate server and the private key is encrypted using MAC ID of the mobile device and securely stored in SELinux enabled file system of the mobile device.

Once the registration and activation are over the employee can start to access his/her client application using the credentials which are already sent to the registered email-id of the employee for acquiring the services. Services are provided based on the access rights set for the requester from the corporate server.

3.4. Proposed Corporate Server Components

The proposed corporate environment has authentication server, intelligent security server, query filtering server and database server. The corporate server keeps record of all the registered employees. The authentication of the client is done by the corporate server by verifying the UserId and password.After authentication, the corporate server is connected to the employee database for retrieving the details such as name, role, accessibility options, etc. and sends the employee's profile to the Authentication Server. The information flow on the network is secured by encrypting and decrypting the message using elliptical curve cryptography implemented in CCP.

3.4.1. Authentication Server

Authentication Server authenticates the user with three levels of authentication and determines whether a privilege may be granted to a particular user or not in order to keep the information more confidential from non-participants. Once the user is authenticated this server permits the clients to access the corporate database system after the three levels of authentication. If not with the three subsequent attempts the access will be denied. The algorithms developed for various levels of authentication are given below.

3.4.2. Intelligent Security and Query Filtering Server

The Intelligent Security Server (ISS) provides an intelligent gateway to access the corporate database server through query filtering server (QFS). The ISS receives the user's request through the authentication server and verifies the requested data with his/her access control policy. Then the QFS server provides an indexing path for queries obtained from the intelligent server, and processes the query. If the database access is necessary for the given query, then the query filtering server accesses the

particular database which is pertained to it. Otherwise, the query filtering server itself processes the query and sends the response to the client.

3.4.2.1 Proposed Access Control Policy for Query Filtering Server

There are four levels of access control policy defined for the proposed system which will be processed through four types of QFS namely QFS1, QFS2, QFS3 and QFS4. Information in the corporate serves are categorized as top secret information, secret information, confidential information and employee details. The top secret information will be transmitted through Query Filter server 1, the secret information will be transmitted through the QFS2, the confidential information will be transmitted through the QFS3 and the employee details will be transmitted through the QFS4.

3.4.3. Database Server

Database Server (DDS) is one of the main servers in the proposed corporate environment. This server holds the information about the personnel information, login credentials, employee departments and their role in the corporate information system etc. This server allows the user to access the requested information which will be ultimately sent to the user through the authentication server which encrypts the accessed data using ECC algorithm that resides in CCP. The mobile device receiving the encrypted request, decrypts it using the ECC algorithm. The decrypted information is displayed on the mobile devices through the mobile Apps.

3.5 System architecture of Hardware implementation for CCP

In the proposed architecture, Hardware based Cryptographic Co-Processor driver is implemented on employee's mobile device to encrypt/decrypt the employee data. The CCP driver is made up of two sub modules: (1) ccp module (ccp.ko) provides low level interface to the CCP HW. (2) ccp-crypto module (ccp-crypto.ko) provides the Linux crypto API interface to the CCP. The Linux Crypto API is a Linux in-kernel infrastructure that offers cryptography to all other subsystems. It provides a single API for accessing different ciphers and digests.

CCP HW is the lowest layer, and ccp.ko implements the interface to communicate to the CCP HW. The CCP module is responsible for initializing the CCP hardware, registers to the correct values, sets up the command descriptor as per the requirement of each CCP command and implements an interrupt handler to signal completion/error status from the CCP HW to upper layers. The CCP Crypto module uses the underlying CCP module for communicating the command requests to the CCP HW. It also provides the Linux crypto API interface, thereby providing a standard and uniform interface to the CCP from the employee client application layer. The command requests are in the form of CCP commands created in the memory.

Figure 3 illustrates the Android Crypto acceleration stack and the interfaces available in the user-space and the kernel space which enables crypto acceleration through hardware. The CCP module and the CCP crypto module are implemented to support CCP acceleration in Linux kernel. OpenSSL is an open source library implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols and provides a full-strength general purpose cryptography library.

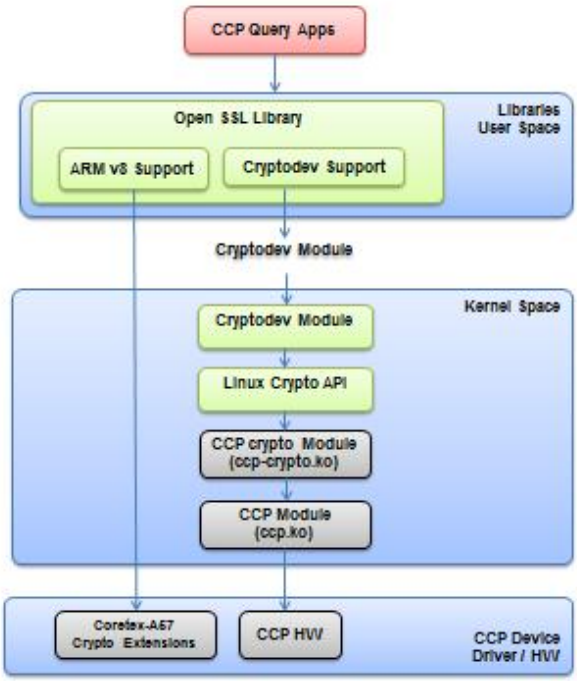

Figure 3. System architecture of Hardware Implementation for CCP

Cryptodev is a device (/dev/crypto) that allows access to Linux kernel cryptographic drivers, thus allowing user space applications to take advantage of hardware accelerators. Cryptodev support is enabled in OpenSSL, which allows OpenSSL to call input/output controls (ioctls) to perform crypto operations. Cryptodev module is an open source Linux kernel mode driver that implements various ioctls thereby allowing communication between OpenSSL and the Linux crypto drivers. Cryptodev module is registered as a misc device with the Linux kernel and exposes /dev/crypto node to the user-space. The ioctls implemented by the Cryptodev module uses the Linux crypto API, to perform a particular crypto operation.

3.6 Interface for Device Authentication

Algorithm DeviceAuthen(MDC, URL)
{
Mobile Device sends Certificate (MDC) to the Corporate Server (CS);
CS obtains CDP from user certificate and retrieves CRL from CDP;
CS examines CRL for the serial number of the MDC;
CS queries CDP for CRL to verify the validity of the MUC;
CRL is returned from CA's CRL database (CDP) to CS;
CS examines the CRL for the validation of the User Certificate;
IF serial number of MDC is not found in new CRL
IF(Sent MDC(Public Key & Validity) = CRL MDC(Public Key & Validity))

```
{
Client device is authenticated;
CS sends X.509v3 based server certificate to the mobile Device;
Mobile Device initiates communication with CA Server;
Mobile Device sends serial number of server's certificate and requests
the server certificate status from OCSP Server;
OCSP server returns the status for requested server certificate;
IF (OCSP response = 'Success')
The Corporate Server is identified and authenticated;
ELSE IF(OCSP response = 'NotSuccess')
Invalid Server Certificate;
}
ELSE
Invalid Device Certificate (MDC);
Exit( );
}
```

3.7 Interface for Client and Client/Server (CS) Authentication

```
Algorithm CSAuthen(UserId, Password)
{
//Client side
GET UserId and Password;//Mobile user enters UserId and password;
MD = hashing (UserId& Password) using SHA1 algorithm;
EMD = encrypt(MD using secret key);
CSAuthenDS = sign(EMD using client's private key);
Send CSAuthenDS to the Corporate Server;
//CorporateServer side
Find and validates MSISDN of the user request from the user profile;
IF MSISDN is valid then
{
Extract the user's public key, UserId, password from the CSDB
with respect to the MSCSDN;
CSAuthen = de-sign(CSAuthenDS using client's public key);
MD = decrypt(CSAuthen using secret key);
IF (CSDB:UserId and Password = MD:UserId and Password)
{
Client and Corporate Server are authenticated;
CS sends Welcoming Message to the Mobile device;
}
ELSE
Send error message for invalid UserId and Password;
}
ELSE
Access Denied;
}
```

4. Experimental Setup

The proposed architecture for Hardware based Secure Mobile Corporate Database System is tested with the sample test bed. The hardware requirement at client side is a CCP enabled mobile phone and at the server environment it requires Authentication Server (AS), Intelligent Securtiy Server (ISS), Query Filtering Server(QFS) and Distributed Database Server(DDS) which are also CCP enabled. The proposed work is examined with an emulator using Android Development tool kit on Samsung Galaxy Grand 2 android enabled device. The sample testbed is depicted in figure 4.

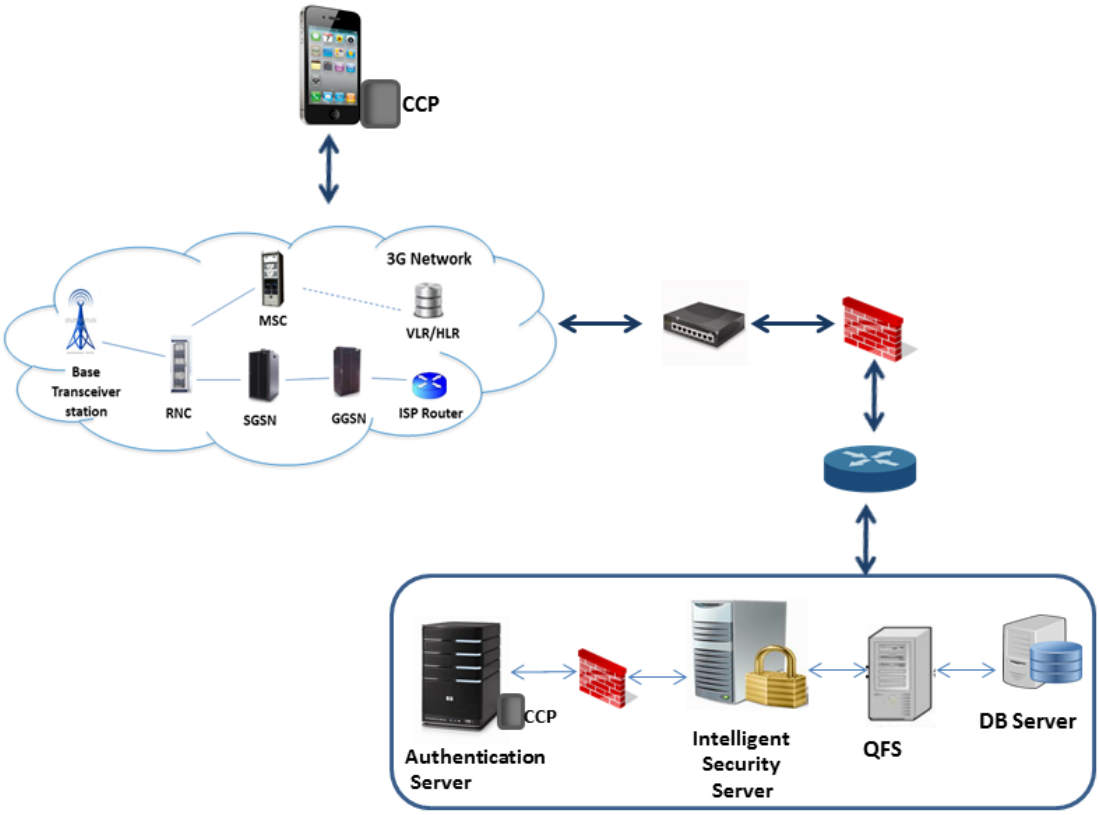

Figure. 4 Test Bed for Secure Mobile Corporate Database System

5. Performance Analysis

The performance of the proposed system is tested with regard to the time taken for device authentication and client server authentication.

5.1. Performance Analysis for Device Authentication

The device authentication verifies the identity of theMobile Client and the corporate authentication server by using ECC based X.509v3. The Mobile Client authentication process involves invoking client certificate, fetching the serial number of the client certificate, establishing communication with Certificate Authority(CA) server, obtaining the Certificate Revocation Lists (CRLs) and finding the revocation status

for the client certificate. To evaluate the server certificate, the client device invokes the server certificate and fetches the serial number of the certificate, initiates Online Certificate Status Protocol(OCSP) connectivity, sends the OCSP request and verify the response of the OCSP from the CA server.

The time taken for the various steps involved in device authentication for both emulator and mobile phone is shown in Table 1 and graphically presented in figure 5.

Table 1: Time taken for Device Authentication

Steps	Description	Emulator (in ms)	MobilePhone (in ms)
1	Invoke the Client certificate and URL	21	29
2	Client certificate verification & Mobile Client authentication	317	375
3	Invoke the server certificate	61	120
4	Fetching the serial number from the server certificate	44	135
5	OCSP Protocol Initiation	62	125
6	Server certificate validation & Server Authentication	438	325

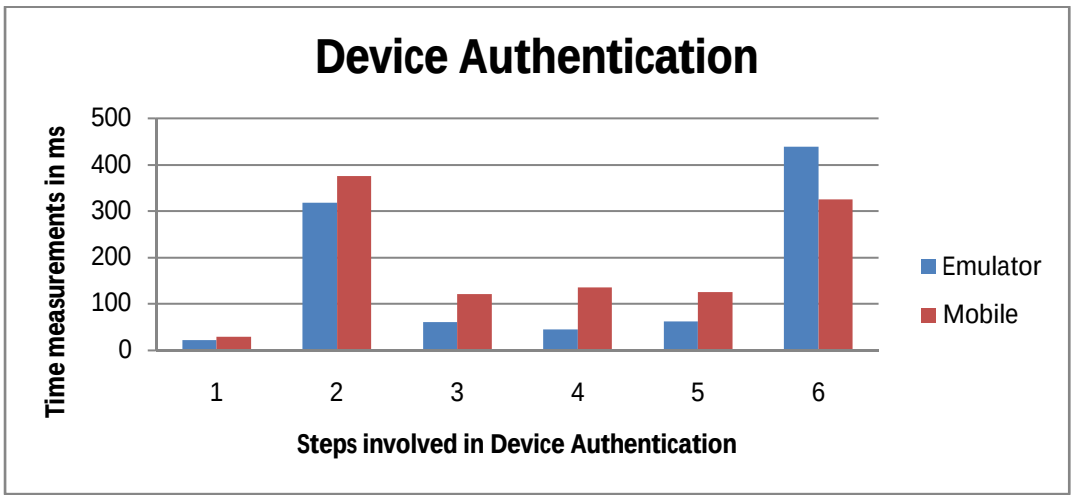

Figure 5: Time taken for Device Authentication

It is observed that the emulator runs on personal computer consumes less time than the mobile phone, because the processor speed and memory of the personal computer are higher than a mobile phone.

5.2 Performance Analysis of Client and Client/Server Authentication

The client authentication process includes secret key generation using user Id and

MAC ID, obtaining the public key from server certificate and decryption of the public key using a secret key. The client/server authentication process includes obtaining the user Id and password from the mobile user, creating a digest for authentication parameters, encrypting the digest using the secret key, signing the final message using client's private key and sending it to the corporate authentication server. These functionalities are done at the client device.

After receiving them, the corporate authentication server follows the reverse process and maps the UserId and password with the database records. If the server gets positive results, then the client receives the message for authentication. If the corporate authentication server decrypts UserId and password successfully, then the server is authenticated to the mobile user.

The time taken for the client authentication process at mobile device is presented in Table 2 and it is graphically presented in figure 6.

Table 2: Time taken for Client Authentication

Steps	Operations	PC (in ms)	Mobile Phone (in ms)
1	Secret Key Generation	25	50
2	Obtain the public key from the Server's Certificate	36	69
3	Decrypt the public key using secret key	25	48

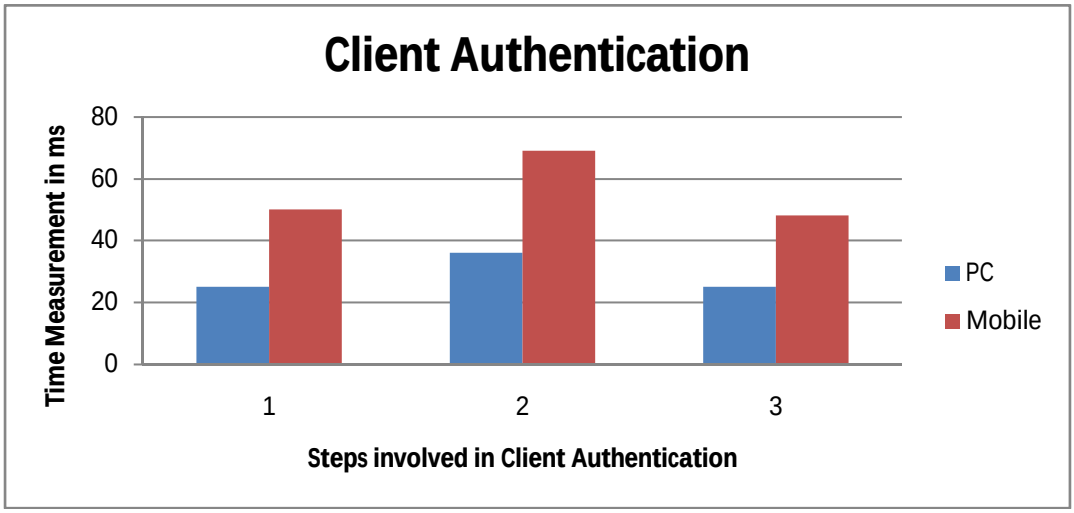

Figure 6: Time taken for Client Authentication

The performance analysis for client /server authentication is done in an emulator using Android Development tool kit on Samsung Galaxy Grand 2 Android

enabled device and the emulator running on the Personal Computer (PC) over Local Area Network (LAN). The time spent for client/server authentication process done is presented in Table 3 and it is diagrammatically presented in figure 7.

Table 3: Time taken for Client/Server Authentication

Steps	Operations	Emulator (in ms)	Mobile Phone (in ms)
1	Hashing the UserId&password	22	34
2	Encrypt hashed UserId&password using secret key	30	44
3	Sign the encrypted hashed message	40	63
4	Encrypt UserId&password using AS's public key	42	78
5	Client authentication Reply	52	71

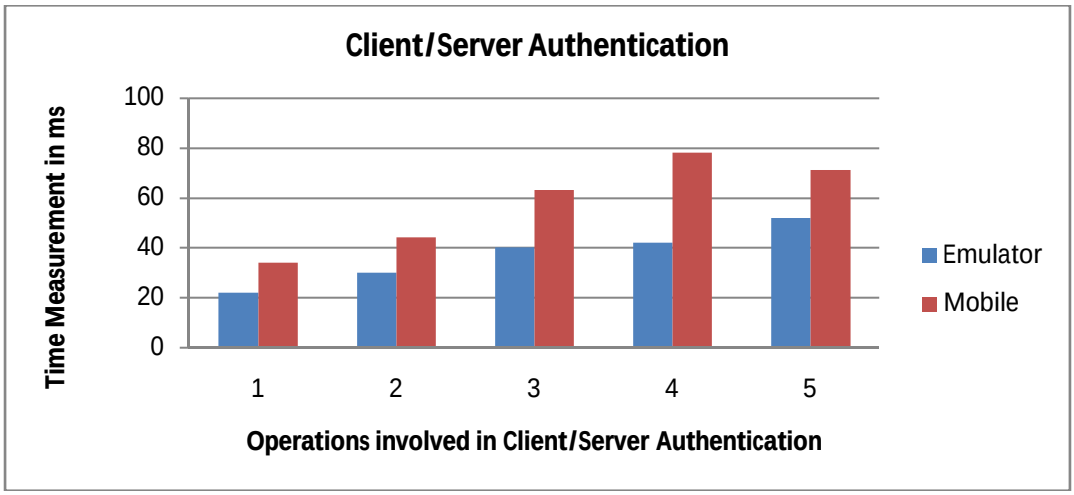

Figure 7: Time Taken for Client/Server Authentication

The results show that the client mobile device consumes more time for encrypting the digest of UserId and password using secret key than the computer. Also, the mobile phone consumes significant time for creating the signature using the client's private key. The significant note here is that the time taken for encrypting the digest of the UserId and password using secret key is less than from encrypting the UserId and password using public key at the mobile device.

From the implementation, it is found that ECC provides equivalent performance and response time in mobile device when compared with the personal computer, although it achieves high level security when compared to symmetric algorithms. Finally, if any corporate system implements more security mechanisms with complex public key encryption algorithm like ECC it then becomes an advantage with a notable impact.

6. Conclusion

The proposed architecture for Secure Mobile Databases for Corporate Environment is a novel approach integrating ECC based hardware Cryptographic Co-Processor to perform secure database transactions while accessing corporate information through mobile devices. It's a new launch of implementing ECC coprocessor at client's mobile device and the corporate server to have a secure access by defining and validating the user credentials and processing the data through QFS at different security levels. The future work is to implement the same in a real time scenario.

References:

[1] "Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged", United States Government Accountability Office, GAO, September 2012. http://www.gao.gov/assets/650/648519.pdf

[2] "Bring your own device: Security and risk considerations for your mobile device program", Insights on governance, risk and compliance, September 2013. http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf

[3] "Mobile security: from risk to revenue, Creating opportunity from challenge", KPMG International Cooperative, 2013. http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/mobile-security-risk-to-revenue/Documents/mobile-security-risk-to-revenue-v2.pdf

[4] "Guidelines for Managing and Securing Mobile Devices in the Enterprise (Draft)", Murugiah Souppaya, Karen Scarfone, National Institute of Standards and Technology, U.S Department of Commerce, NIST Special Publication 800-124 Revision 1 (Draft), July 2012. http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf

[5] "Secure application delivery for a mobile workforce", White Paper, Citrix Systems, 2014. http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/secure-application-delivery-for-a-mobile-workforce.pdf

[6] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014–2019", White Paper, February 3, 2015. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf

[7] "Best Practices for Securing Remote and Mobile Devices", White Paper, BeyondTrust Software, Inc., 2013. http://www.beyondtrust.com/Content/whitepapers/Best-Practices-for-Securing-Remote-and-Mobile-Devices.pdf

[8] "Cisco 2014 Annual Security Report". http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

[9] Fiawoo, S.Y., and Sowah, R.A., 2012, " Design and Development of an Android Application to Process and Display Summarised Corporate Data", IEEE, pp. 86-91.

[10] Blaz Markelj and Igor Bernik, 2012, "Mobile Devices and Corporate Data Security", International Journal of Education and Information Technologies, Issue 1, Volume 6, pp.97-104.

[11] Erez Shmueli, Ronen Vaisenberg, Ehud Gudes and Yuval Elovici, 2014, " Implementing a database encryption solution, design and implementation issues", Volume 44, Computers & security, pp. 33-50.

[12] Kumar, S. B. R., Rabara, S. A., and Martin, J. R., 2009, "A System Model and Protocol for Mobile Payment Consortia System", International Conference on Test and Measurement, IEEE, pp.439-442.

[13] Narendiran, C., 2011, "A New Approach on Secure Mobile Banking using Public Key Infrastructure", International Journal of Computing Technology and Information Security Vol.1, No.1, pp.40-46.

[14] Fan Mingyu, Wang Jinahua, and Wang GuangweI, 2003, "A Design of Hardware Cryptographic CO-Processor", Workshop on Information Assurance United States Military Academy, West Point, NY June, pp.234-236.

[15] Zeidler, S., Goderbauer, M., and Krstic, M., 2013, "Design of a Low-Power Asynchronous Elliptic Curve Cryptography Coprocessor", In Technologiepark 25, 15236 Frankfurt (Oder), Germany, IEEE, pp. 569-572.