A Framework for Secure Mobile Database Transactions using Cryptographic Co-processor

D. Sathiya
Dept. of Computer Science,
St. Joseph's College
(Autonomous),
Tiruchirappalli- 620 002, India

S. Albert Rabara
Dept. of Computer Science,
St. Joseph's College
(Autonomous),
Tiruchirappalli- 620 002,India

J. Ronald Martin
Dept. of Computer Science,
St. Joseph's College
(Autonomous),
Tiruchirappalli- 620 002,India

ABSTRACT
The increase in the adoption of database systems by the Corporates in key data management technology for their day-to-day operations. So, decision-making becomes crucial for the security of data that is managed by these systems. The damage and misuse of data affects not only the single user or application, but it may have disastrous consequences for the entire organization as well. Accessing more secured information through client's mobile device is an important issue. In this paper, a framework for Secure Mobile Database Transactions using the Cryptographic Co-processor (CCP) is proposed. A dedicated coprocessor for encryption and decryption process enables high level security when compared to software based encrypting/decrypting process in corporate environment.

Keywords
Cryptographic Co-processor, Mobile Database, Elliptic Curve Cryptography, Distributed Database, Query optimization.

1. INTRODUCTION
To realize the objectives and to survive in the digital era, the corporates must continually grow and study their competitors to manage information correctly. Indeed, the survival of these corporates may depend on securing this important information. The rapid progress in wireless mobile communication technology and personal communication systems has prompted new security questions. Since open air is used as a communication channel, the content of the communication may be exposed to an eavesdropper, or the system services can be used fraudulently. In order to have reliable and proper security over the wireless communication channel, certain security measures, like confidentiality, authenticity, and untraceability need to be taken care of. To meet today's needs in wireless digital communication; the developed protocols need to be highly secure, requiring low computational overhead and thus low power [1].

Smart phones are an integral part of today's society, especially as technology has made mobile devices into becoming an extension of the workplace, either in an entertainment system, or a banking center, or a favorite store. Anything earlier done on a desktop computer has now been migrated to a smartphone in some form or other. The most serious restrictions on mobile devices can be narrowed to two categories: (1) computational limitations and (2) power limitations. With the advent of technology, mobile devices have always been less powerful than their non-mobile counterparts – an intrinsic quality of the mobile environment. As technology has grown widely, a race has developed between creating more powerful encryption schemes and the ability to crack these powerful encryption schemes by using brutal force – a race where mobile technology will always be on the loser end. Most of these devices are in use all day and security should not be the main cause for draining the battery. For example, a Chief Executive Officer (CEO) sends confidential information throughout the day from his mobile phone, the same phone he uses on as an emergency contact option. The encryption of this information should not prevent him from receiving a phone call about a client who needs his help. To overcome the computational and power limitations, a hardware based cryptographic co-processor is introduced in this proposed architecture.

Cryptographic Co-processor provides a high security, high throughput cryptographic subsystem. In this current technological corporate world, each corporate differ from the others by using unique quality product. To establish their identity, they have to secure their product design information and their raw material information. Elliptic Curve Cryptography (ECC) has been shown to be a promising technique for cryptographic systems [2]. One of the most interesting features of ECC systems is the key length required for secure communication, which is much smaller than RSA system. In [3] it has been shown that a key length of 160-223 bits is necessary to reach the same level of security as an RSA system with a relevant key for security applications, such as SmartCards and Mobile phone. The major part of the sub-operations to encrypt and decrypt data are very specific bit-level operations which consume many instructions when executed on standard processors. For this reason, often special dedicated hardware accelerators are added to the systems to speed-up the computation and to reduce the energy consumed during crypto-operations [4].

The paper is organized as follows. Section 2 provides a survey of related research work. Section 3 presents a framework for proposed Architecture. Section 4 has a sequence diagram for hardware based Cryptography Co-Processor, which includes Hardware system routine and Software system routine. Section 4 concludes the paper.

2. REVIEW OF LITERATURE
Fan Mingyu et. al., [5] presented a design of general purpose crypto co-processor, which is capable of selecting different algorithms through programming, and performing crypto operations such as key management, data encryption, and decryption, which is implemented in FPGA. A testing system is designed to verify the co-processor. Most crypto algorithms work more effectively when they are implemented in hardware than in software. In this paper, reconfigurable architecture is described which gives high performance

hardware implementations with the flexibility of general purpose processors. Processing speed is the first concern for hardware implementation of the algorithm. Hardware implementations usually run at a higher speed than software implementations. But while taking the reconfigurable character of the co-processor into account, the co-processor's processing speed may be lower.

MuthuKumar et al., [6] present Elliptic Curve Cryptography (ECC) co-processor, which is dual-field processor with projective coordinator and they have implemented architecture for scalar multiplication, which is a key operation in elliptic curve cryptography. Elliptic curve cryptography (ECC) provides secure data transaction for personal identity verification, authentication, digital signature, and key management. ECC algorithm has been implemented in software, ASIC and FPGA. Hardware implementation of public key cryptosystems is flexible when compared to software. The software implementation is slow and not safe to store the private key in the computer's memory. The advantage of ASIC implementation is that it is secure and faster than the software, but it is not flexible. The FPGA implementation is suitable for most of the applications, secure and faster. Their proposed processor contains Advanced high performance bus (AHB) interface, input and output buffers, Main controller, EC data selector, ECC modular multiplier, Clock controller, Register File, and Montgomery Unit. The EC Data selector fetches the instructions from the main controller and decoded it to ECC Modular Multiplication Units. The Clock Control Unit used to schedule the cycle is required to perform the scalar multiplications. The ECC Modular Multiplier performs point coordinate conversion, point double, point addition, scalar multiplication, Montgomery pre and post processing, and modular exponentiation. In their processor, the power management scheduler controls the power consumption. When power utilization goes the threshold values, the clock control unit automatically controls the cycles. The coprocessor can be adapted both in the primary field and binary field, and provides a high throughput. The synthesis result shows that their design produces high throughput and power efficiency.

Muthukumar et al., [7] have proposed FPGA architecture of elliptic curve cryptography coprocessor. The coprocessor contains the operation over binary finite fields, point adding, doubling and scalar multiplication on elliptic curve. In their coprocessor, a new type of FPGA-based modular multiplier architecture is proposed. There are numerous advantages of using Field-Programmable Gate-Array (FPGA) technology to implement in hardware the computationally intensive operations are needed for ECC. In particular, performance, cost efficiency, and the ability to easily update the cryptographic algorithm in fielded devices are very attractive for hardware implementations for ECC. The FPGA based architecture of the ECC arithmetic coprocessor is introduced with Verilog HDL. The Verilog description is correctly simulated in ModelSim and the synthesis of the description is finished in Xilinx's integrated software environment. The placing and routing process is finished in Xilinx's XC31000 device. The new design thus can achieve more convenience and flexibility into modular multiplier design over finite field. Moreover, the multiplier can achieve half or quarter of clock cycles consuming in the full bit-serial multiplier (m clock cycles in GF(2111)). Experiment results show that coprocessor designed can achieve high performance. With the coprocessor embedded in, a PCI ECC adapter for data encryption and decryption is implemented.

SeongHan Shin et al., [8] proposed an elliptic curve based AKA (EC-AKA) protocol secure against partition attacks and it is found to be suitable for the following situation: (1) a client, who communicates with many different servers, remembers only one password and has insecure devices (e.g., mobile phones or PDAs); (2) the counterpart servers are not perfectly secure against several attacks (e.g., virus or hacker); (3) neither PKI (Public Key Infrastructures) nor TRM (Tamper Resistance Modules) is available. The EC-AKA protocol achieves more strengthened security properties and efficiency when compared with the existing AKA protocols (employed in the IEEE 802.1x). Elliptic curve cryptographic systems and protocols are ideal for wireless environments where processing power, time and/or communication bandwidth are at a premium. However, the difficulty arises from the fact that the direct elliptic curve analogs of password-based AKA protocols are insecure against a special kind of off-line dictionary attacks, called partition attacks.

The EC-AKA protocol is suitable for the situation in that it is secure against leakage of stored secrets from a client and a server, and it is more efficient than the existing password based AKA protocols. The authenticity of the EC-AKA protocol is based on password and an additional stored secret which might seem to be similar to that of EAP-FAST. However, the obvious distinction between the two protocols is that the EC-AKA protocol remains secure even if the stored secret on client's side is leaked out to an attacker. The EC-AKA protocol achieves more strengthened security and efficiency where the authenticity is based on the client's relatively short password and an additional secret stored on insecure mobile devices.

Elliptic Curve Cryptosystem (ECC) based remote authentication scheme has been used for mobile devices. For instance, Yang and Change proposed an ID-based remote mutual authentication with key agreement scheme for mobile devices on Elliptic Curve Cryptosystem in 2009. However, their scheme is still vulnerable to insider attack and impersonation attack. Therefore, Tien-Ho Chen [8] proposed an advanced ECC ID-Based remote mutual authentication scheme for mobile devices to solve the issues. Furthermore, they analyzed their scheme to show that this scheme is more secure to authenticate users and remote servers for mobile devices. The computation cost is higher than Yang and Chang's scheme.

Erez Shmueli et al., [9] analyze and compare five traditional architectures for database encryption. They show that existing architectures may provide a high level of security, but have a significant impact on performance and impose major changes to the application layer, and provide high performance, but have a significant impact on performance and impose major changes to the application layer, or may be transparent to the application layer and may provide high performance, but will have several fundamental security weaknesses. The new architecture proposed is based on placing the encryption module inside the database management software (DBMS), just above the database cache, and using a dedicated technique to encrypt each database value together with its coordinates. These two properties allow this new architecture to achieve a high level of data security while offering enhanced performance and total transparency to the application layer. The performance of the various architectures is evaluated both analytically and through extensive experimentation. The performance evaluation results demonstrate that in more realistic scenarios, i.e., where only a part of the database content is stored in the database cache, the suggested

architecture outperforms the others. Here, they used a software implementation of AES with the Cipher-Block Chaining (CBC) mode. The software implementation with a dedicated hardware for cryptographic operations may reduce the time spent for cryptographic calculations and consequently may contribute to the superiority of the above cache architecture.

In this paper, a framework for Secure Mobile Database Transactions using Cryptographic Co-processor is proposed with dedicated coprocessor for encryption and decryption process. The CPP provides high level security compared to software based encrypting/decrypting process in corporate environment.

3. FRAMEWORK FOR PROPOSED APPROACH

A framework is a logical structure that classifies and organizes the components and artifacts of the system. A comprehensive framework has a consistent naming of the components and elements of the framework, all terms of the components and elements fully defined, and has a consistent and expressive set of graphical representations for each component and element. The proposed framework for mobile based corporate information system provides well-defined and coherent components and artifacts of the system. In addition to that, it also provides the necessary technical infrastructure such as acquiring information, connectivity, communication and security to facilitate the corporate information sharing and acts as an intermediary between the employees and the corporate server. This framework is specifically developed for the corporate users for the registered clients using mobile devices. The framework for secure mobile database transactions using Cryptographic Co-processor is designed according to the software architectural standards that is presented in Figure 1 and illustrated in this section.

3.1 Mobile Client

The Mobile client handles a variety of mobile devices like mobile phones, and PDAs. The different mobile devices have different technical and physical characteristics in terms of performance and its functionality. The modern mobile phones like smart phones provide much of the same functionality that is supported by the desktop computer. This makes them a potentially reliable for mobile transactions in terms of security. There are several components available for the mobile client to carry out the mobile applications.

Designing the user interfaces for mobile based corporate information system applications present a new set of challenges for the interface designers and software developers due to the limitation of mobile devices such as limited screen size, power, memory, battery life and computational capabilities as well as the constraints of wireless networks such as low bandwidth, high latency, and unpredictable availability and stability. The responsibility of User Interface Manager is to acquire and validate data entered by the mobile clients as per business and security logic. Android V4 is the preferred development platform for mobile application systems due to the portability code, the ability to reduce the network traffic since it can process the data locally, and the ability to establish a different security policy on the client device.

The Display Manager maps the display resolution with respect to the transaction interfaces and also handles display issues. The Communication Manager (CM) establishes and manages connectivity with the CDBSE. It allows exchange of information in a secured way between the communicating parties. The CCP manager provides a high level encrypted data for outgoing and incoming information using an ECC algorithm to the communication manager. The CM maintains the account for the source and destination of communication, information about communicators, and the time at which the communication is initiated. Other communication issues such as performance, security and privacy, and litigation are considered by the CM. The mobile client device executes the user's requests, including request in multi-tasking environment, where the task switching mechanism refers to application switching. To respond to the number of the user's requests, the TaskSwitchingManager keeps the information about application switching including the task ID and application ID.

The Synchronization Manager's main responsibilities are sending and receiving the data between the client and CS and with the CDBSE server, authenticating the device with the authentication service, downloading application updates and device management commands. During the data synchronization, the Security Manager is performing authentication, signing the request, certificate management, secret key management and distribution. The DeviceAppManager keeps the information about corporate application Business Logic, validations and alerts, and authentication information. The Backup Manager supports atomic transaction in case of network disconnection. When the network is disconnected, the failed transaction is picked up from the restore point and resumes the data, instead of restarting again.

The mobile user starts to communicate with the corporate server through activating the interface from his mobile device. While activating the interface, the client device is authenticated to the corporate server with a valid PIN. Once the device authentication is completed successfully, the application interface prompts for username and password for client authentication. While activating the user interface, the International Mobile Equipment Identity (IMEI) number of the mobile client device is validated. If the IMEI of the client device is not matched, the user interface will not be enabled in the client device, otherwise, the interface will be displayed. Once the client makes entries, those parameters are encrypted using the Elliptic Curve Cryptography (ECC) and are later sent to the corporate server in a secured way. After that, a third level authentication is performed for level of accessing for clients which is displayed on the user interface for the employees who wants to get information from the corporate server.

3.2 Corporate Database Server Environment (CDBS)

The corporate server mainly consists of four subordinate servers to make the client server interaction effectively. They are ECC enabled Authentication Server (AS), Intelligent Security Server (ISS), Query Filtering Server (QFS) and Distributed Database Management System (DDMS).

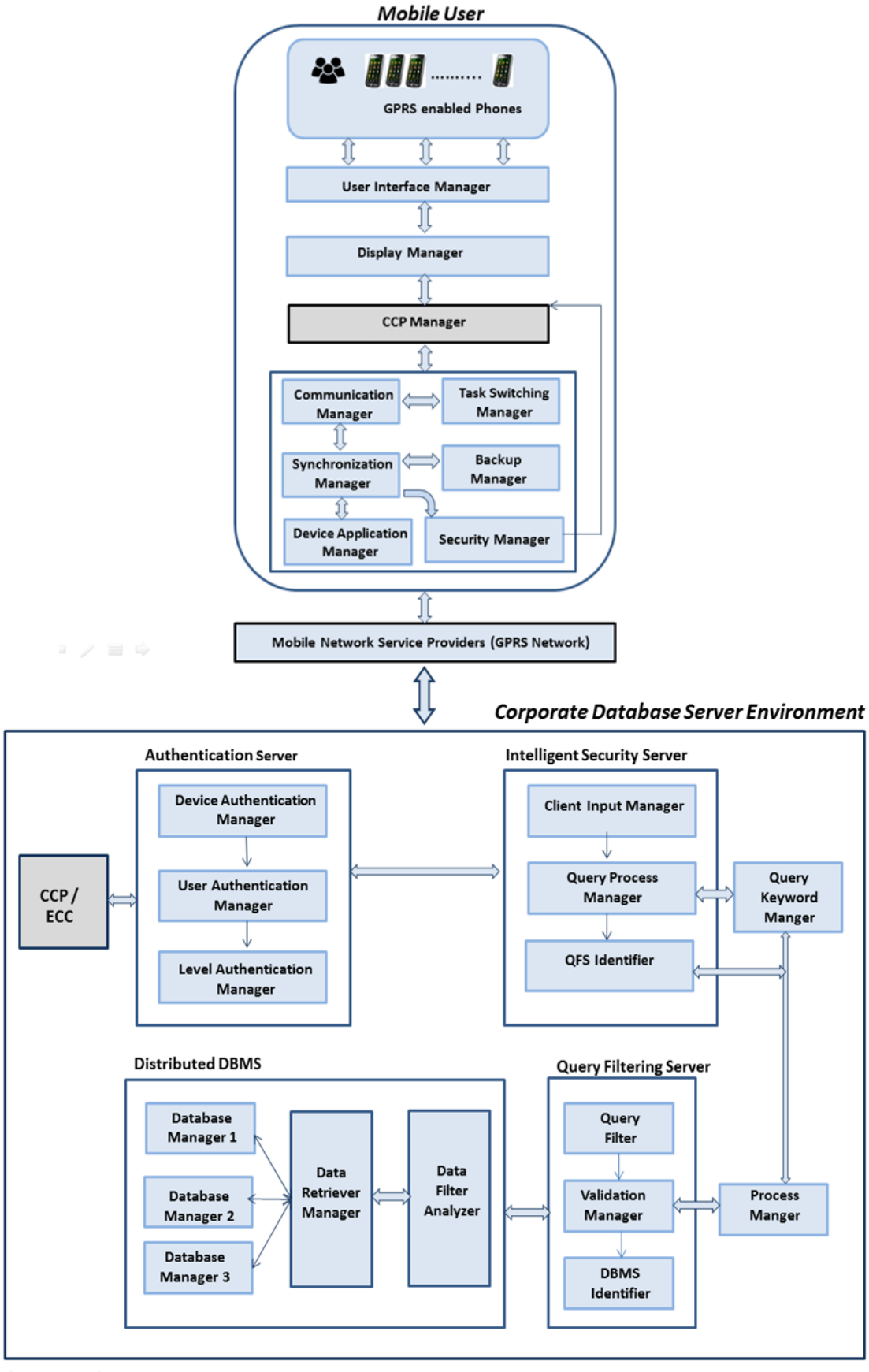

Fig 1: Framework for proposed Architecture

3.2.1 Authentication Server (AS)

The Authentication Server embedded with CCP, will decrypt the request from the user and encrypt the retrieved information from the Distributed DBMS using the ECC algorithm. The Device Authentication Manager is used to validate the device with the help of phone number, IMEI number, and PIN number. User Authentication Manager is used to validate the user by his login credential information like username as EmployeeId and password. The Level Authentication Manager is used to validate the level of access by verifying the designcode, access level code.

3.2.2 Intelligent Security Server (ISS)

In this proposed architecture, the intelligent manager does some important operations such as analyze the importance of user level of authentication and analyzes the importance of query. Based on these combine decision, it will select a particular query filtering server and do the operations. The Client Input Manager will analyze the level of access. The Query Process Manager will analyze the importance of the query. Based upon query QFS identifier will select particular QFS. The query keyword manager will choose the best QFS algorithm.

3.2.3 The query filtering server (QFS)

The query compilation process is responsible to convert such a declarative query into an execution plan. This compilation process includes three steps: query parsing, logical plan selection and physical plan selection, where logic plans represent different algebraic expressions and physical plans are generated from the logical plans by selecting algorithms for each operator and by selecting an order execution for those operators. Given one input query, there are many different logical plans and accordingly more physical planes.

Query optimization is a process to produce a query execution plan which represents an execution strategy for a query. The selected plan is optimal in some metrics, for example, minimum objective cost, maximum performance, maximum fairness among multiple users, which defines the goal of the optimization process. The execution plan chosen depends on the level of information such as top secret, secret, confidential and unclassified. In this proposed approach, there are four QFS. Depends of level of information, the corresponding QFS is chosen to process it and corresponding execution plan is applied to each QFS.

The query filter manager is used to select an appropriate query optimization technique. Validation manager is used to validate user request with his/her access level in the database. QFS Identifier identifies particular data which is located in distributed DB.

3.2.4 Distributed Database server (DDS)

Data Filer Manager selects data from database by indexing method. Depending on query filter manager, Data retriever Manager retrieves query from the database. Database Manager controls both the data filter manager and data retriever manager.

4. IMPLEMENTATION TECHNIQUE OF CCP IN HARDWARE AND SOFTWARE

4.1 Hardware System Routine Implementation for CCP

The system routines for implementation of the cryptographic co-processor are shown in Figure 2. A CCP driver module contains the init request to initialize the access for the CCP hardware. This request is passed to PCI driver for accessing the hardware through the bus drivers which are responsible for the data transfer between the application and the hardware.

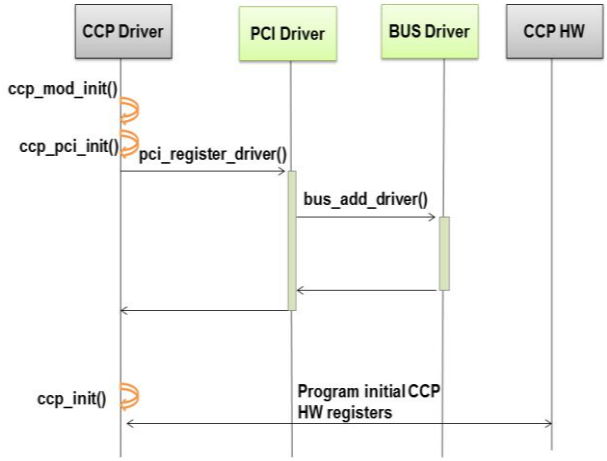

Fig 2: Hardware System routine implementation for CCP

CCP Driver enables CCP chip with OS. PCI Driver is used to introduce CCP hardware to the driver software. BUS Driver is used to transfer data or control between different components. The first initialization request enables the coprocessor in CCP driver. The next PCI initialization is to indicate operating system. The next request is to make use of BUS driver which transfer data or control. The next request is to access hardware. Finally, the replay comes to report that the CCP is ready for process [10] [11].

4.2 Software System Routine Implementations for CCP

The crypto API implementation is shown in Figure 3. It contains an init method to initialize the request to perform the cryptographic operation using various registers. In initialization process, the cryptographic coprocessor flags are initialized and device drivers are initialized to process crypto requests. In the second step, the process register algorithm is used to initialize the register that is required for cryptography implemented in CCP. The third step is to process the cryptographic process. The CCP register algorithms call dynamic link libraries.

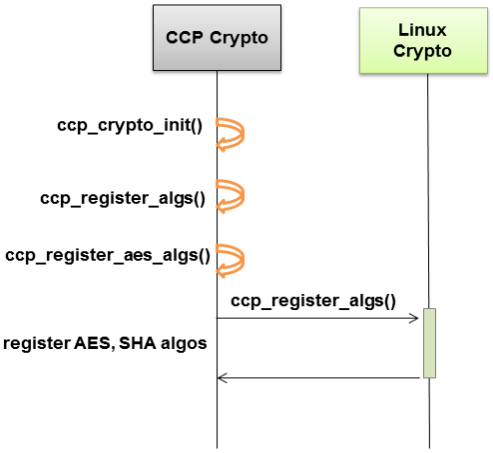

Fig 3: Crypto API for CCP

5. CONCLUSION

Corporate mobility management has several dimensions and one of the main important dimensions is Security. Because mobile devices are easily lost or stolen, the data on those devices is highly vulnerable. When corporate data is accessible via a personal mobile device, organizations suddenly lose a great deal of control over who can access that data. In the current technological corporate world, each corporate differ from the unique quality product. To establish their identity, they have to secure their product design information and their raw material information. In this paper, the architecture for end to end secure Mobile corporate information Management system is proposed. In this paper, it is proposed a system to prevent unauthorized access to enterprise applications and/or corporate data on mobile devices.

6. REFERENCES

[1] Roshan Duraisamy, Salcic, Z., Morales-Sandoval, M., Feregrino-Uribe, C. 2006. A fast elliptic curve based key agreement protocol-on-chip (PoC) for securing networked embedded systems. IEEE, International Conference on Embedded and Real-Time Computing Systems and Applications.

[2] Miguel Morales-Sandoval, Claudia Feregrino-Uribe, Rene Cumplido and Ignacio Algredo-Badillo. 2009. A Run Time Reconfigurable Co-Processor for Elliptic Curve Scalar Multiplication. IEEE, Mexican International Conference on Computer Science.

[3] Barker, E., Barker, W., Burr, W., Polk, W., and Smid, M. 2007. "Recommendation for key management – part 1: General". National Institute of Standard Technology, Tech. Rep., 201.

[4] Dan Yong-ping and He Hong-li per. 2012. Tradeoff design of Low-cost and Low-energy Elliptic Curve Crypto processor for Wireless Sensor Networks. Wireless Communications, Networking and Mobile Computing (WiCOM), 8th International Conference.

[5] Fan Mingyu, WangJinahua, and WangGuangweI. 2003. A Design of Hardware Cryptographic CO-Processor. Workshop on Information Assurance United States Military Academy, West Point, NY.

[6] MuthuKumar, B. and Jeevananthan, S. 2010. High Speed Hardware Implementation of an Elliptic Curve Cryptography (ECC) Co-Processor. IEEE, Trendz in Information Sciences & Computing (TISC), 17th-19th Dec, Chennai.

[7] Muthukumar, B. and Dr. Jeevananthan, S. 2009. Design of an Efficient Elliptic Curve Cryptography Coprocessor. First International Conference on Advanced Computing (ICAC 2009).

[8] SeongHan Shin, Kazukuni Kobara and Hideki Imai. 2006. Elliptic Curve based Authenticated Key Agreement Protocol for Wireless Security. IEEE, International Conference on Computational Intelligence and Security.

[9] Erez Shmueli, Ronen Vaisenberg, Ehud Gudes and Yuval Elovici. 2014. Implementing a database encryption solution, design and implementation issues. Computers & security, Volume 44, July 2014.

[10] Tutanescu, I., Anton, C., Ionescu, L., Caragata, D. 2012. Elliptic Curves Cryptosystems Approaches. IEEE, International Conference on Information Society (i-Society 2012).

[11] Ravi Kishore Kodali. 2013. Implementation of ECDSA in WSN. IEEE, International Conference on Control Communication and Computing (ICCC).