Security Protocol for Mobile Data System

Prof. Dr. Hilal Hadi Salih
Dr Ahmed Tariq Sadiq
Alaa K.Farhan
Dep. Of Computer Science, University of Technology

Abstract

Protection data in mobile device is not an option, it is very necessary process. The best way to protect data on the move is to encrypt them. However, providing the right tools is not an easy task especially when the cost as issues, any tools must easy to use by only one user. The process of accessing discrete database exposes to opposed of attacks from unauthorized, where, same sensitive data are change when the intruder access and may not reach to user in a complete form. For that purpose, protection the data and assuring of the receiving them in a complete form one of most important subjects in data security. In this paper, design and implementation new secure system are called Security Protocol for Mobile Data, SPMD. The proposed system can protect the sending and receiving data between terminal and server device by using proposed block cipher algorithm.

بروتوكول أمني لنظام بيانات محمولة

أ.د. هلال هادي صالح د. أحمد طارق صادق علا ء كاظم فرحان

الخلاصة

حماية البيانات في الاجهزة المحمولة ليس خياراً انما هو هو ضرورة قصوى. يعتبر تشفير البيانات من أفضل الطرق لحمايتها. توفير ادوات صحيحة وخاصة لعمل ذلك ليس بالامر السهل اذا اخذ بنظر الاعتبار الكلفة والمستفيد. عملية الوصول الى قواعد البيانات تكون معرضة للهجوم من قبل غير المخولين وبعض البيانات الحساسة تتعرض الى التغيير عندما تقع بيد المتطفل بالتالي تكون غير كاملة بالنسبة الى المستفيد. لهذا الغرض حماية البيانات والتأكد من استلامها بشكل متكامل واحد من الاهداف الاساسية في أمنية البيانات. في هذا البحث تم تصميم وتنفيذ نظام أمني جديد سمي "برتوكول أمني للبيانات الجوالة". النظام المقترح يعمل على حماية البيانات المرسلة والمستلمة بين الاجهزة الطرفية والخادم باستخدام خوارزمية التشفير الكتلي المقترحة.

1. Introduction

Information securities are the process by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations [1]. Computing technology reaches every corner of our lives. Mobile communication, personal computation (e.g. personal digital assistants: PDAs), and portable navigation devices are just a few examples of the most commonly known applications. Recent advances in ultra-low-power technology enabled the development of even smaller, more mobile, autonomous devices [2]. Protecting the integrity of data is of utmost importance for many application scenarios [3].

2. Information Security Concept

Information security relates to the need to keep information from falling into the wrong hands. Failure to follow good security practices may lead to unauthorized uses of information, to fraud and to identity theft. In contrast, businesses collect and share information about people for a variety of appropriate reasons: improving service, decreasing costs, reducing fraud, and targeting offers of goods and services. This normal flow of information in a business context is not an example of lax security practices and does not lead to the unauthorized use and fraud associated with bad security. The policy issues relating to information security differ markedly from the policy issues relating to information sharing.

Nevertheless, issues related to information security are sometimes confused with issues related to information sharing. While many opinion polls describing the fears some consumers have regarding online commerce do not distinguish the two, the public clearly understands the difference between some one stealing information about them to engage in fraud and identity theft and the sharing of information among companies for legitimate business purposes. Consumers clearly want to be notified about information sharing and given some choice about what information businesses collect about them and how it is used. But overwhelming majorities say they are much more concerned about fraudsters and others gaining unauthorized access to information about them and using it for illegal purposes [4]. On a broad scale, the financial institution industry has a primary role in protecting the nation’s financial services infrastructure [5]. The protection of information systems against unauthorized access to or

modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats [6].

3. Information Security Threats

Bad things can happen to an organization's information or computer systems in many ways. Some of these bad things are done on purpose (maliciously) and others occur by accident. No matter why the event occurs, damage is done to the organization. Because of this, all of these threats are called "attacks" regardless of whether there is malicious intent or not. There are four primary categories of attacks:

• Access
• Modification
• Denial of service
• Repudiation

4. Communication Media Types

Every communications relationship can be characterized in relation to two independent characteristics concerning kind of physical access media and logic relation to the network. [7]**Show in table (1)**.

On the one hand, the **wired** and **wireless** terms relate to the media used for the physical connection to the network (or in a more generic sense: the other communicating device). On the other hand, **fixed** and **mobile** relate to the logical connection of the component to the network. The difference between fixed and mobile communications lies in their use of two key network functions:

1. Assigning of unique identification (addresses) to devices.
2. Association of these identifiers to specific network access points.

In **fixed** communications, a permanent association exists between an end-user device address and a single unique access point into the network (this definition can also be applied to associations between devices within the network).

In **mobile** communications the end user device can connect itself to multiple access points in order to use network services. The fundamental issue is the association between the end user device address and the various network access points. Both portable device (i.e. devices, which don't maintain network connection during transportation) and continuously working movable devices can be considered as mobile. Actually, every of the four possible connectivity

domains (fixed/wired, fixed/wireless, mobile/wired, mobile/wireless) has slightly different security requirements, influenced by the different level of the security offered by the access medium and different security demands of mobile and fixed network access.

4.1 Wired vs. Wireless Security

In general, the wireless medium (i.e. radio links) is considered much more insecure than conventional wire transmission. Despite that most of existing wired links (e.g. phone lines) are not encrypted, in common sense they are assumed to provide the basic level of security need by end-users. It is important to realize, that, as long as we don't speak about the Telecommunications Management Network (TMN) security, the integrity and confidentiality of transmitted data is mostly sole user-side requirement. The most obvious difference between the wireless and wired link from the security point of view is the virtual incapability to discover any eavesdropping attempts and to locate the alleged attacker. As far as an attacker possesses sufficient technical knowledge and moderate resources, it can stay virtual invisible or, at least, elusive. Wireless links (especially radio links) are not only less secure as wired ones they are also much more unreliable. Hence, used encryption algorithms must be easy to resynchronize in case of transmission errors [8].

5. The Proposed System Platform Requirements

The platform is foundation of the software solution and should be presented first. The core component will be indicted, piecing it all together in overall architecture, with some though about communication, **figure (1)** shows the proposed system's platform, SMD content the following parts:

A. Client

The propose SMD system is a one of secure system to run must has a hardware, the hardware are different types of device, recommendation should run at the following device:

1. Personal computer or laptop with a minimum specific as below:

- Microsoft windows XP
- IIS which provide basic HTTP
- TCP/IP protocol
- HTTP protocol
- Web browser
- LAN Cart
- 512 RAM
- 1.7 CPU

2. Cellular Mobile Device: the cellular mobile is the popular example of the mobile communication system; the

cellular mobile is characterized as a system ensuring bidirectional wireless communication with mobile station moving even at high speed in the large area cover by system of base station. Smart phone or PDA's with minimum requirements:

- Microsoft Windows Mobile or Windows CE
- IIS
- Browser
- 1 GHz CPU
- 512 RAM

B. Internet

- **Internet connection Side**: which PC or Laptop sends and receive over an Internet Protocol (IP)-base internet network.
- **GBRS Connection Line**: which allow mobile device as Personal Computer (PC) or Laptop with the following feature to send and receive data an Internet Protocol (IP)-base internet protocol. GBRS is a data bearer that enables wireless access to data network such as internet.

C. Server

The SMD recommendation system is a web application so that SMD depends and uses web server feature like:

- **IIS(Internet Information Services)** : which provide basic HTTP,FTP and SMTP Service.
- **ADO.NET (Active Data Objects)**: which provide as robust development platform for building web application, which OLE DB provider (ODEDB) and can connect with any Microsoft tools and interface with underlay SMD databases.

6. Implementation toolset

The tools use to implementation proposed system in world web site must use different types of tools, one of the tools is language, web programming language and data manipulation language used to compose a system, the language types are:

- **ASP.NET(Active Server Pages)** are HTML page, which include scripting and create active web server applications,ASP.NET language is very important to build web application and different from the previews language to have many tools to build site and can used the visual basic or JavaScript .NET language to

easy be programming functions, and ASP.NET can be connected with Emulator Smart phone, It has tools for drawing and designing the interface in web applications, when used the ASP or HTML to build the web applications, we need to programming all functions, the preview web design language not have any facility when compare with NET language.

- **Structure query language** is a standard computer language for access and manipulation database system, SQL statements are used to retrieve update data in database and used execute query against database. SQL work with data base programs like MS access , Oracle and DB2.ect
- **Visual Basic.** NET is used to programming algorithm for a new block cipher, the visual Basic has many facility as tools web use to build and connect with internet, this language is easy connect with ASP.NET, when programming is debugger Program can easy discover the error by used many windows for watch, and in writing code for programming the debugger work in real time to increase speed.
- **Using** modern language not used the classical language to work with mobile as WML JAVA script .

7. System components

The system can be explained by describing these components:
Encryption keys, database tables and administrative tools see **figure (2).**Any user who wants see the data through his account must be able to get authentication from administrate to use enter to system.

7.1 Encryption Keys

The system generates two type of keys used for authentication and exchange key.

- When client registry initializations in system and enter data from client to system, the system generate secret key (symmetric key) as password and must unique key, this key used to encryption data in scenario send and receive to encryption and decryption data.

- In the connection, the client used user name and password to enter the system, to avoid attacker in channel these information encryption by public key for administrator, therefore the system generator public/private keys used for that.

7.2 Tables

System database tables are stored in the server and are controlled by administrator, access for database in server by using ADO.NET , the database contains three tables represent the system, see **figure (2).**

- User login table: Content two fields, user name and password, the structure of table is show in **table (2).**
- Client table: content several fields as name, job, gender, phone, address, Ncount, Ucont, Mail and these field depend for type application, the structure of table is show in **table(3).**
- Administrator tables: content name and password for administrator, the structure of table is show in **table (4).**

7.3 Administrative tools

The administrator is as client accounts have some facilities as other. However, the administrator tools are an anther application design for reprinting. Controlling the administrator tools can shown in figure (3), the tools consist of:

1. Key selector: this operation is performing when makes account for used system in the first time,
2. Add/remove account: in this operation, adding and removing account is done by the administrate through administrate tools.
3. Authentication check: in this operation the administrator can check if the user is authorized to enter system by password in login table.
4. Transaction: this operation views the data of the counts in sending and receiving query, when the client sees his sensitive data display in device.

8. Client account

The client account is client-base application in the server as data mobiling system installed the client in laptop or mobile phone device used to receive encryption client message as some filed of data from remote data base, This application is guarded by user name and

password, if the enter to system is true else is exit.

The system is designed to be friendly used, by using clear interface and interactive, the system used the proposed block cipher algorithm to protect data when translate data between client and server, the client can used PDA's or smart phone to enter system and display his sensitive data.

9. Installation Algorithm

The installation process is done by administrative

Begin

The user sends to request system.

The administer responses to user's request for sends to user

request special information to enter in system.

The user sends data.

The administrator in the system receives data and puts it in client table.

Administrator generates the authentication for user as secret key (symmetric key), this key is put in login table.

The client is sent or gives a secret key.

End

- The administrator installs new block cipher in terminal device.
- The administrator publishes public key used to encryption when the user sends authentication information to connect with system, **figure (4)** shows the steps of connection.

10. Send/ Receive Scenario Algorithm

Begin

The user can login to his account by using user name and password.

The systems will encryption the user name and password by public key for administers and sends them to the web service.

The last (web service) receives user name and password to decryption by the

private key of administrator.

The web check these information in login table, if the user is registry then the service retrieved to the user account in the account table.

End

11. System Services

The actual operator of SMD consists of two services confidently and authentication. They will summarize in turn:

Confidently: it is the most important basic service, which is provided by encryption message to be transmitted, the proposed encryption is used.

Authentication: The encryption algorithm used in SMD is of secret key type therefore the user authenticity is determined by the owner of the secret key.

12. System Implementation

When proposed system is implemented we need connect to internet, the all page can display in PDA's or smart phone and the main page shows in **figure (6).**

In execute the application by using the local host to not connect to internet and the administrator not to install in server internet, the user can enter to system. But the user name and password must be used, when inter in special pace the administrator check in login table and enter to next page to display data or exit, when they are not found, **figure (7)** shows how to use user name and password of system.

The display page display the data for client, but the data is cipher by proposed block cipher, to display the data clearly the client must reenter the password as secret key, when reenter the secret key the system used the same algorithm to decryption data and display clearly, **figure(8)** explain cipher and plain data.

The administrator can modify the system in login table or client table by added new client or remove a client, the administrator modify the client data by search, add, delete, modify option. In display option by using multi methods, client first, the last client and serial display. The system used the password for administrator to check the administrator authentication, **figure (9), figure (10)** shows the authentication and transaction administrator pages.

13. Conclusions

1. One of the major and the simple attack approach is by trying

several attempted to login in the system ,the enhancement system control on this approach by making the administrator monitors the number of the login attempts to distinguished the legal ones form the illegal ones and then make a decision to block the system.

2. To achieve the authenticity process to reach data in the proposed system, the secret key is encrypted by the RSA public key method so to get a high level of key management security.
3. Essentially ASP.NET has powerful capacities in web programming as well as the ability to use the ADO.NET language as in addition tool in its programming environment, (because the ADO.NET has ability to connect different database such as SQL server, Oracle and MS Access in the unique platform with ASP.NET interface). Therefore, the propose block cipher algorithm has been programmed by using VB.NET language that can be embedded simply in an ASP.NET environment.
4. The proposed algorithm is implemented as a software in terminal devices by simplifying the process operations and reducing the consumed time based on partitioning the block itself to achieve the task of multiprocessing and use a new technique in designing the S-Box, because the cost of using hardware is expensive.

References

[1] Wikipedia the free encyclopedia: http://***en.wikipedia.org/wiki/Information_security***

[2] Sarma S., Brock D.L. and Ashton K. "***The Networked Physical World – Proposals For Engineering The Next Generation Of Computing, Commerce & Automatic Identification***", White paper, MIT: Auto-ID Center, Oct 2000.

[3] Jens-Peter Kaps "***Cryptography for Ultra-Low Power Devices***", Worcester Polytechnic Institute , Ph.D Thesis in Electrical Engineering, May, 2006

[4] Alan W., "***Prepared Statement before the House Subcommittee on Commerce***", Trade and Consumer Protection, For a good summary of these surveys May 8, 2001. ***www.cdt.org/privacy/ccp/security1.shtml***

[5] **Wikipedia the free encyclopedia:** Federal financial institutions examination council, Information Security Booklet – July 2006. ***http://en.wikipedia.org/wiki/Information_security***

[6] Richard C., "***Why is Information Security Important***", Keynote Address to the Federal Trade Commission, May 20, 2002. ***http://www.cdt.org/privacy/ccp/security1.shtml***

[7] "***Baseline Text for Wireless ATM Specification***", ATM Forum Wireless ATM Working Group, BTD-WATM-01.03, July 1997.
Xinri Cong, cong@cis.ohio-state.edu ***http://rajjain.com/cis788-97/ftp/wireless_atm.pdf***

[8] Konrad W,"***Information Security In Mobile Communication system***", Diploma thesis, Instytut Telekom unikac Jl Politechnika Warszawska, Aachen, September 1997.

Table (1) Network Access Options**.**

	Wireless	**Wired**
Mobile	Network Access Point changes over time, connections can be continues	Network Access Point changes over time, connections are interrupted
Fixed	Terminal is permanently connected by wireless link to the network Access Point	Terminal is permanently connected by wire to the network Access Point

Table (2) User login

NAME	**TYPE**	**LENGHT**
User name	Text	256 Bytes

Password	Text	8 Bytes

Table (3) Client information

NAME	TYPE	LENGHT
Name	Text	20 Bytes
Job	Text	15 Bytes
Gender	Text	5 Bytes
Phone	Number	10 Bytes
Address	Text	50 Bytes
Ncount	Number	10 Bytes
Ucount	Number	10 Bytes
Mali	Text	15 Bytes

Table (4) administrator

NAME	TYPE	LENGHT
User name	Text	8 Bytes
Password	Text	8 Bytes

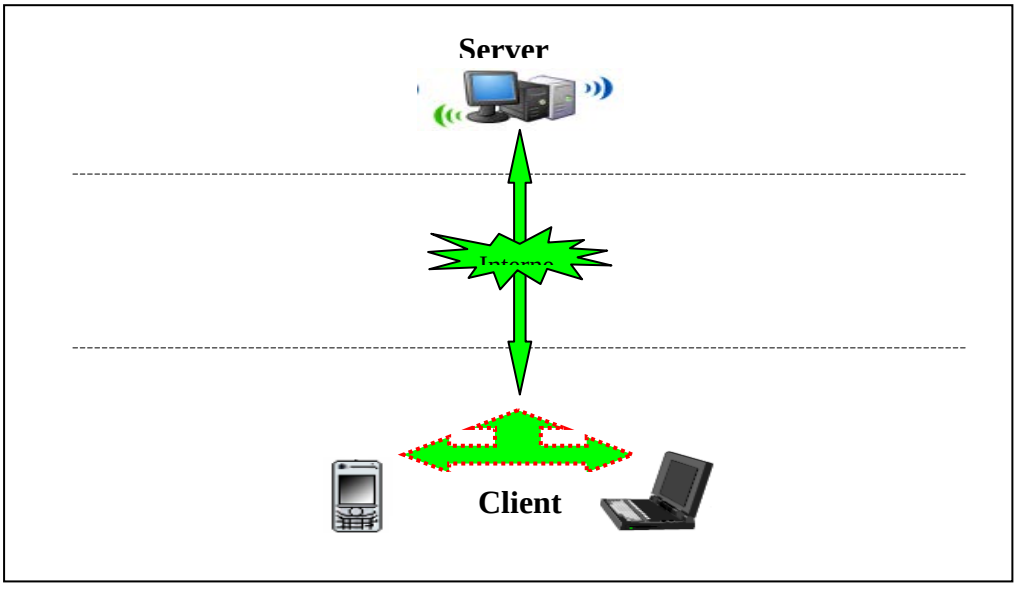

Figure (1) The Proposed SMD platform

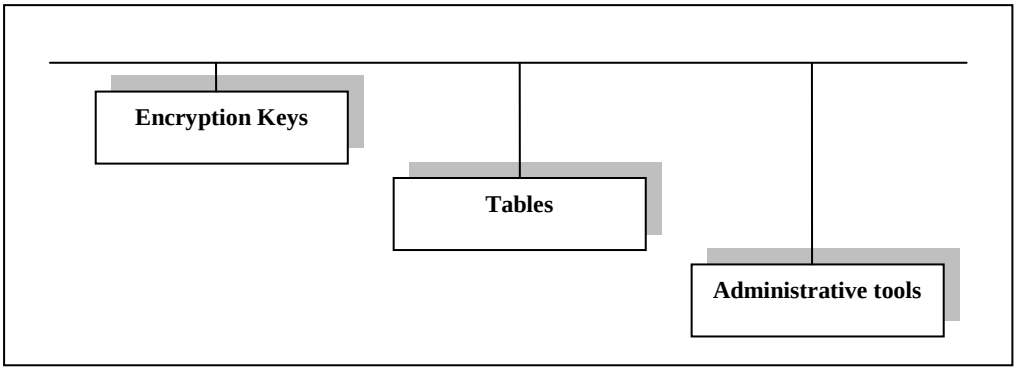

Figure (2) system Component

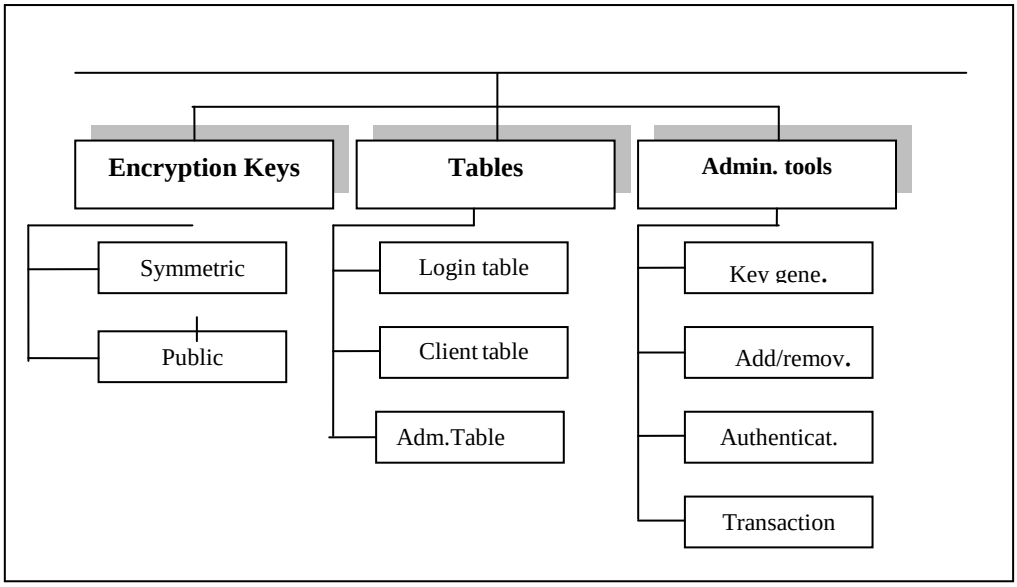

Figure (3) described for system parts

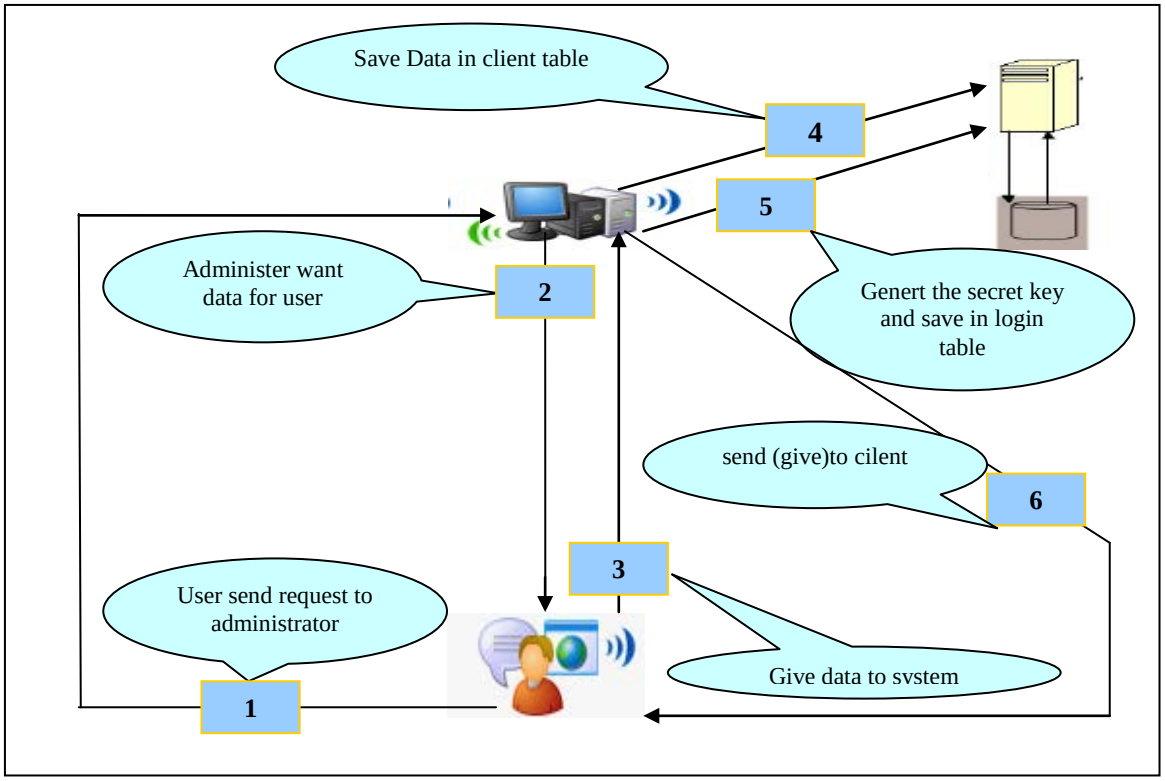

Figure (4) installation system

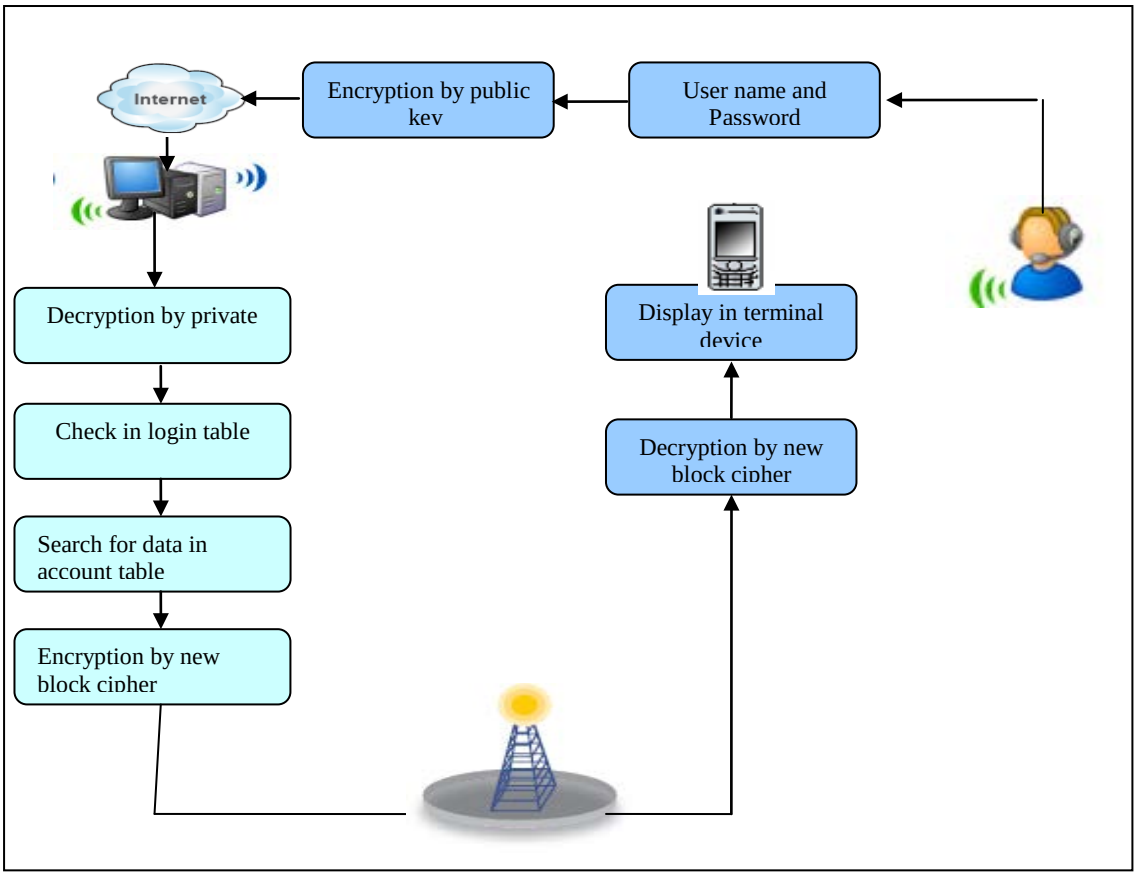

Figure (5) Send/Receive Scenario

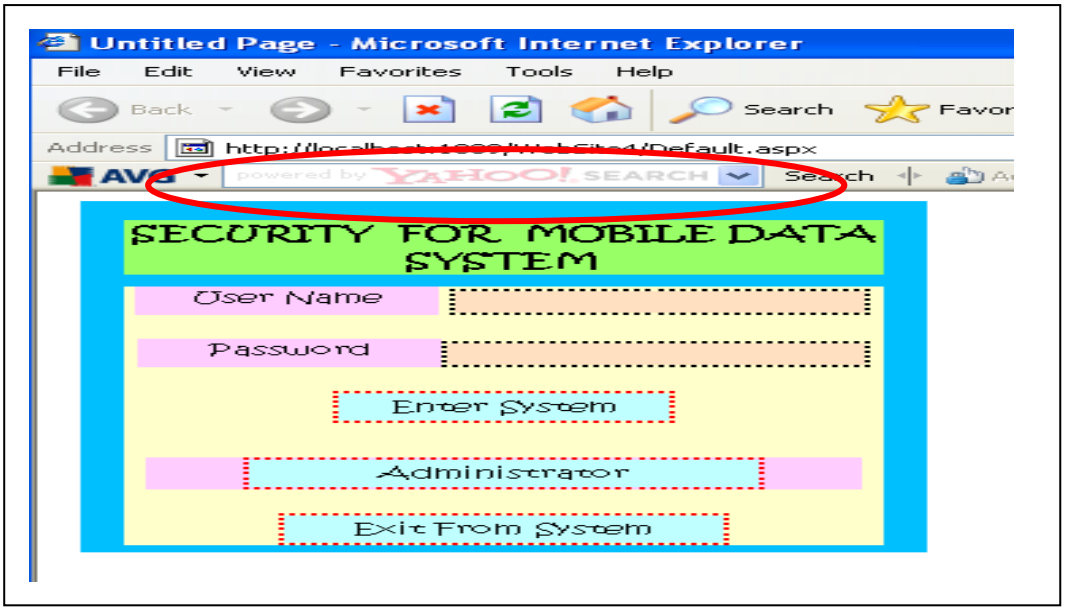

Figure (6) main Page in Proposed System

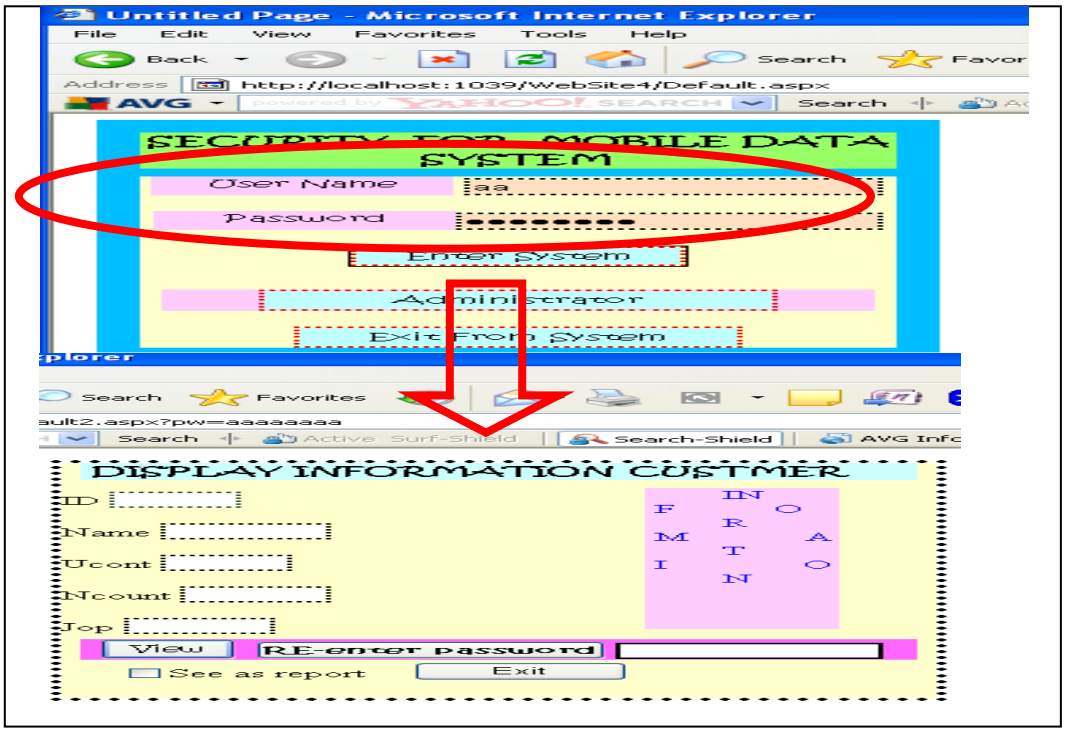

Figure (7) Enter to System

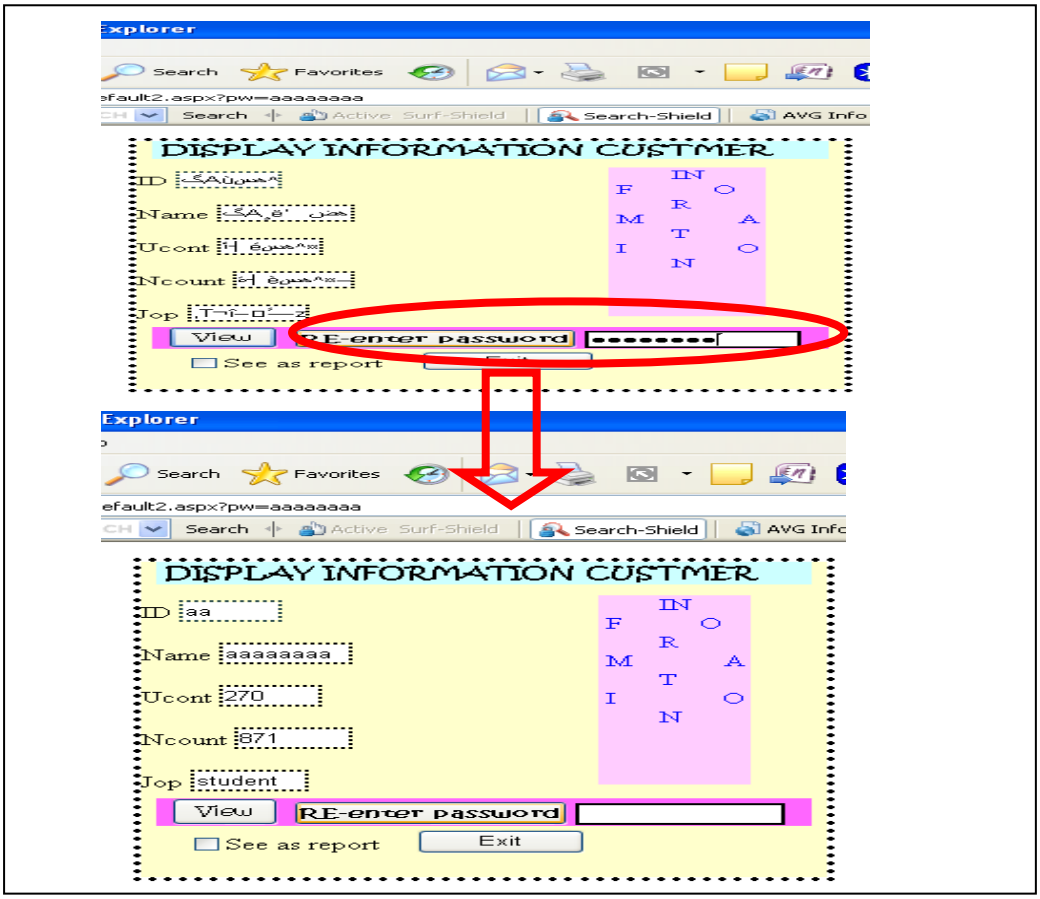

Figure (8) Encryption and Decryption

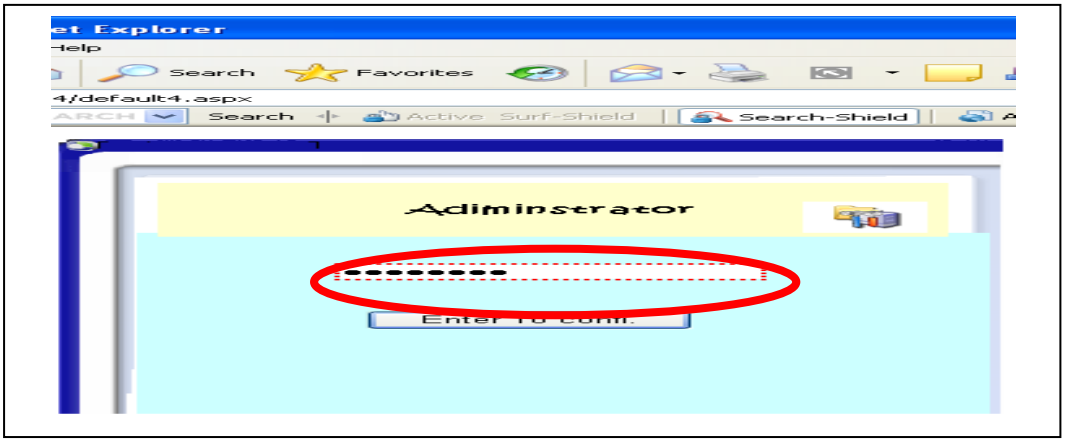

Figure (9) Authentication Page

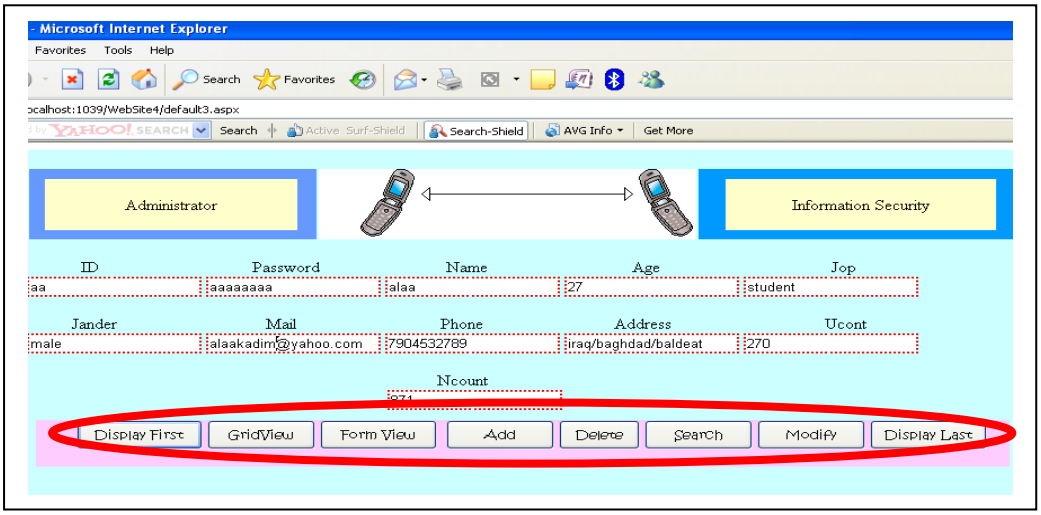

Figure (10) Transaction administrator pages