CHAPTER 5

BLUETOOTH APPLICATIONS WITH PSPFW SECURITY ALGORITHM

5.1 INTRODUCTION

Telecommunications has the potential to provide a solution to medical services to improve quality and access to healthcare regardless of geography. The advances in information and communication technologies enable technically, the continuous monitoring of health-related parameters with wireless sensors, wherever the user happens to be. They provide valuable real-time information enabling the physicians to monitor and analyze a patient’s current and previous state of health (Tura et al. 2003). To remove or minimize cables, a robust wireless link with low power capabilities is required. Although many wireless standards can be used, there are important considerations such as range, throughput, security, ease of implementation and cost. Bluetooth is quickly becoming the preferred technology for wireless patient monitoring (Noel Baisa 2005). A major motivation for reducing the number of cables or for doing away with the cables completely is to eliminate the potentially harmful currents to the patient. The patient monitoring involves handling of sensitive data. These data should be transmitted securely without any intrusion. Even a Bluetooth enabled gadget can try to participate in the network which introduces risk.

The national exchequer, the banking industry and regular citizens all incur a high overhead in using physical cash. Electronic cash and cell
phone based payment in particular is a viable alternative to physical cash since it incurs much lower overheads and offers more convenience. E-payment systems offer huge cost savings to the Government because use of electronic cash is much cheaper than printing paper currency. By eliminating the need to transport, handle, store and dispense physical cash, electronic cash offers enormous savings to banks, customers and merchants. Mobile payment schemes are dominating the world of electronic payments. This is due to the easy availability of mobile phones (Shivani Agarwal et al 2007, Thulasibai and Srivatsa 2006, Upkar Varshney 2006). Security is of paramount importance in an e-payment system. Mobile payment transactions may enable people to walk into a store and purchase items by just pressing a button on their mobile phone. While a mobile device acting as a replacement for the wallet, would be desirable, there are several security concerns that arise when turning to practical implementations. The macro payment presents the highest risk, and requires strong security measures William Stallings (2006).

5.2 CONNECTED LIMITED DEVICE CONFIGURATION (CLDC)

The Sun JAVA wireless toolkit is a state of the art toolbox for developing wireless applications that are based on J2ME’s connected limited device configuration (CLDC) and mobile information device profile (MIDP) and designed to run on cell phones, mainstream personal digital assistants, and other small mobile devices. The toolkit includes the emulation environments, performance optimization and tuning features, documentation and examples that developers need to bring efficient and successful wireless applications to market quickly. The J2ME Wireless toolkit supports a number of ways to develop MIDP applications.

In this chapter, PSPFW algorithm that offers increased security, data transfer rate and speed is tested by implementing a real time patient
monitoring system. The effectiveness of the algorithm is also analyzed for macro payment application developed at the laboratory level.

5.3 REMOTE PATIENT MONITORING

The problem found in most hospitals is that the physician has to frequently visit the patient and assess his/her condition by measuring the parameters such as temperature, blood pressure, drip level etc. In case of emergencies, the nurse intimates the doctor through some means of communication like mobile phone. A growing selection of innovative electronic monitoring devices is available, but meaningful communication and decision supports are also needed for both patients and clinicians.

The aim is to develop a reliable, efficient and easily deployable remote patient monitoring system that can play a vital role in providing basic health services to the patients. This system enables expert doctors to monitor patients in remote areas of hospital. Mobile phones or personal digital assistants (PDAs) with wireless networking capabilities may serve as gateways that process, store, and transfer measured parameters to clinicians for further analysis or diagnosis. The timely manner of conveying the real time monitored parameter to the doctor is given high priority which is very much needed.

5.3.1 Objective

The objective of this work is to create an automated patient monitoring system for the patient in hospital. Presently, the care is being provided by nurse, who performs all the steps of patient care manually. They take readings of patient’s physiological data using instruments which are difficult to handle and require manual tuning etc. Then, they record this data into printed forms manually. Finally, the collected forms are sent to a doctor
who goes through them looking for any symptom of abnormality. The doctor then takes decision regarding the patient’s treatment. The automated system that replaces all this hectic activity, should be able to gather the physiological data, transmit it, record it, find any abnormality and then assist the doctor in the decision making process.

5.3.2 Mode of Monitoring

The mode of monitoring the patient is determined by the nature and seriousness of disease. A patient with mild problems needs to be monitored only at periodic intervals, whereas a critical patient must be under constant monitoring. Remote monitoring systems in general, are divided into two basic modes of operations namely periodic checkup mode and continuous monitoring mode (Daeki Cho et al 2008).

5.3.2.1 Periodic checkup mode

A typical patient under normal circumstances can be monitored at periodic intervals. The periodic checkups will be performed by the health worker. In this mode, it is rather easy to establish a reliable and error free communication channel that can preserve all relevant characteristics of the transferred medical signals, regardless of the communication service.

5.3.2.2 Continuous monitoring mode

Continuous monitoring mode is required for critical patients. In this mode, the patient’s physiological data is under constant surveillance. However, the doctors suggest that the patients in critical condition are admitted to the hospital instead of being provided with remote monitoring. This mode is particularly useful in emergency scenarios.
5.3.3 Infrastructure Requirement

A rapidly increasing number of health care professionals now believe that wireless technology will provide accurate data with improved patient care. A wireless telecare system is needed along the patient bedside to provide good health care. The system must be interactive. The physician is needed to send the suggestion back about the patient to the nurse so that nurse can take immediate action. The proposed system consists of three main blocks. They are mentioned below and the block diagram is shown in Figure 5.1.

The system is constructed such that it measures the biomedical parameters at the patient end without any intervention and then transmits the data acquired to the remote station. Sensors play an important role in monitoring the parameters. The precision at which the handheld device is to be operated is decided by the sensor that is used. Vital parameters such as temperature, glucose level, ECG, drip level, pulse rate can also be measured. The measured value is then transmitted to the base station via Bluetooth. The Temperature sensor is used for sensing the temperature. This system is constructed with low power consumption so that it would not cause much hindrance to the patient. The device is constructed such that it transmits the vital information periodically say 2 minute.

5.3.4 Working Model

Each patient is connected with a temperature sensor. Measured parameters of patients are interfaced with the system at the patient end. The patient end system is connected with server and doctor mobile via Bluetooth. The server stores the central database of all the patients. The status of the parameter is decided in the patient end system. If the status is normal, the parameter is transmitted to the server and entered in the database. If the status
is abnormal, then the parameter is immediately communicated to the doctor end and also the data is stored in the database of the server and is depicted in Figure 5.1.

![Figure 5.1 Working Model](image)

**Figure 5.1 Working Model**

Figure 5.2 shows the block diagram of temperature sensor module. The measured temperature is in analog. The analog value is converted into digital value for further processing using 8051 microcontroller. The digital data is transmitted to the PC through MAX 232 driver and RS 232 serial interface. The recorded temperature is saved in a database.

![Figure 5.2 Block Diagram of Temperature Sensor Module](image)

**Figure 5.2 Block Diagram of Temperature Sensor Module**
5.3.4.1 Temperature sensor

The LM35 series are a precision integrated circuit temperature sensor, whose output voltage is linearly proportional to the Celsius (Centigrade) temperature. The LM35 has an advantage over linear temperature sensors calibrated in ° Kelvin, as the user is not required to subtract a large constant voltage from its output to obtain convenient centigrade scaling. The snapshot of temperature sensor is shown in Figure 5.3.

![Temperature Sensor Module]

Figure 5.3 Snapshot of Temperature Sensor Module

Features

- Calibrated directly in ° Celsius (Centigrade)
- Linear + 10.0 mV/°C scale factor
- 0.5°C accuracy guarantee able (at +25°C)
- Rated for full −55° to +150°C range
- Suitable for remote applications
- Low cost due to wafer level trimming
- Operates from 4 to 30 volts
Figure 5.4 Recording Setup

Figure 5.4 shows the recording setup. The LM35 sensor is attached to the patient. The data is received from the patient end in ASCII form. The ‘Bluetooth Hospital Client’ does the conversion of ASCII values into decimal values. The application reads from the serial communication (COM) port.

5.3.4.2 Patient end system

Each patient at the Intensive Care Unit (ICU) is provided with a computer system, that has ‘Bluetooth Hospital Client’ application. This application reads the temperature sensor through the interface. The patient parameters like patient identification number (PID), temperature, heart beat, sugar, inhale, exhale and blood pressure can be transmitted to the server from the patient end system. The user interface of the patient end system is inferred in Figure 5.5.
Figure 5.5 Patient End System

The Bluetooth Hospital Client application has two menus: File and Client. The File Menu has a sub menu ‘Exit’. Exit submenu is used to close the application. Client has two submenus: ‘ServerIP’ and ‘Start’. ‘ServerIP’ submenu is used to connect with the central server and ‘Start’ submenu initializes the connection. Authentication is done after clicking the start submenu and entering a valid pass key. This pass key is a secret shared between client and the server. This process is needed to pair the client with the server. The various patient parameters are given in the user interface. The status of the patient is displayed in the user interface.
Figure 5.6 Status Window

Figure 5.6 shows the various parameters of the patients with the status displayed as normal or abnormal. The unique ID of the patient is displayed in PID field. The temperature of the patient is displayed in Fahrenheit. If the temperature of the patient is less than or equal to 99 °F, then the status of the patient is normal. If the temperature of the patient is greater than 99 °F, then the status of the patient is abnormal. The readings recorded at 2 minute intervals are displayed in Figure 5.7.
Figure 5.7 Database in Patient System

This work can be extended to measure other parameters by interfacing the respective sensor. The work in this thesis is done only for temperature therefore the other fields are displayed as NA. The data collected for a period is stored in client database. The database consists of patient ID, patient name, time, temperature and the status.
5.3.4.3 Server

Bluetooth enabled server is the centralized system. An application ‘Bluetooth Hospital Server’ is present in the server. This application is used to store the various details of the patients. The server is always active. Server updates the patient details from each patient end system and provides authentication for each patient end system. This process is shown in Figure 5.8.

![Figure 5.8 Server Authentication](image)

The server application has two menus namely ‘File’ and ‘Bluetooth’. ‘File’ has a submenu ‘Exit’. Exit submenu is used to close the application. ‘Bluetooth’ menu has a submenu ‘start’. This start menu is used to begin the application. A passkey is provided to disable the unauthorized access. The same passkey is used in the patient end system in order to participate in the network. After authentication, the server displays the details of any received patient data and the attack list.
The server displays as ‘Bluetooth Started’ when server become active. The data is encrypted in the patient end system (client system). The encrypted information is transmitted to the server via Bluetooth. Server decrypts the data and the decrypted information is stored in the server. Server and the client applications use PSPFW Bluetooth security algorithm to decrypt and encrypt the data respectively. The message is displayed in the server window as shown in Figure 5.9.

Figure 5.9 Server Interface
The display consists of two blocks. The first block displays the received patient information. IP24342 is the Identification number of the patient. 100 ° F is the measured temperature of the patient. NAs are other patient parameters which are not applicable in this work. The second block consists of attack list. The attack list displays the number of hits after which the attacker is able to hack, time of attack and the attack status.

The server database stores the parameters of all patients in ICU as shown in Figure 5.10. It displays the recent updates of each patient.

![Figure 5.10 Server Database](image)

### 5.3.4.4 Bluetooth Hospital Mobile

An application ‘Bluetooth Hospital Mobile’ is present in the Bluetooth enabled mobile of the doctor. PSPFW algorithm is implemented in this application to decrypt the information received. This application presents the critical information of the patient as shown in Figure 5.11.
This mobile application has two menus, namely ‘File’ and ‘Client’. ‘File’ is used to close the application. ‘Client’ has two sub menus: Server IP and Start. The server IP submenu is used to connect with the server. Start submenu is enabled after providing server IP address, and now the mobile is connected with the server. Start menu starts the application and the details of the patient with unique ID are displayed. Search option is also provided in this application. Doctor can use the search option to know the details of other patients.
The mobile displays the PID and the monitored parameters. Temp is the temperature of the patient measured in Fahrenheit. The analysis is made at the patient end system. If abnormal, the doctor receives the patient information in his mobile.

5.3.4.5 Attack

Attack is performed by developing an application ‘Bluetooth Hospital Attack’. The pass key in the server is used to find any unauthorized access. If the passkey is incorrect, the server recognizes that it is the attacker who tries to hack the data. Bluetooth hospital server window shown in Figure 5.12 displays the number of hits made by the attacker and the time taken for the hits. The attack failure or success is also displayed. From the Figure 5.12 it is observed that even after the 1572825 of hits, it is not possible to hack the data.

Figure 5.12 Server with Attack List
5.4 MACRO PAYMENTS

A macro payment system typically involves three main contributors. These include a Financial Service Provider (FSP), a payer and payee. A payer is normally a customer who usually purchases the products from the store. A payee is one who sells the products in a store (Shivani Agarwal et al 2007). FSP is usually a bank and is responsible for performing the backend processing required for settling a transaction between payer and payee. The steps involved in the macro payment system are listed below and is depicted in Figure 5.13.

![Figure 5.13 Macro Payment System](image)

The process involved in macro payment system is

Step 1: The invoice is sent from the payee to the payer.

Step 2: Using the invoice, payer now sends the cheque request to the FSP.
Step 3: The FSP issues the mobile cheque (m-cheque) to the payer.

Step 4: The payer transfers the m-cheque to the payee

Step 5: The payee receives the cheque and sends confirmation to the payer.

In this macro payment system, the payer initiates the actual payment transaction by invoking a mutual authentication and session key establishment security service (Gianluigi Me et al 2006).

In this phase, the key is generated and it is available for all the contributors involved in session. This key is valid for a single transaction session. For every session, a new session key is generated randomly (Saleem Kadhiwal et al 2007). After the establishment of the private channel, three communication sessions take place.

They are:

- Payer to payee (via Bluetooth)
- Payer to Financial service provider (via GPRS)
- Payee to Financial service provider (via the Internet)

In the practical implementation, the system utilizes GPRS and the internet for communication of payer to FSP and payee to FSP respectively. In this work, the implementation is done at the laboratory level using Bluetooth technology for all the sessions. When the payer receives the invoice from the payee, the payer sends the cheque request to the FSP. The payer saves a copy of the invoice in the payer’s mobile device. The FSP sends m-cheque to the payer using PSPFW encryption algorithm.

When the m-cheque is received at the payer mobile device, payer verifies the cheque amount and the requested amount. If they are found to be
correct then the payer transfers the cheque to the payee. In the payee side, the Bluetooth technology with PSPFW security algorithm is applied to retrieve the m-cheque and then it is processed. The cheque can be easily validated in the FSP, avoiding for example, cheque bouncing, counterfeiting, and double cheque clearance. Once the process is completed the confirmation is sent to the payer. The mobile payment is categorized based on the payment value involved as Pico, Micro, and Macro payments. Since the macro payment presents more risk, steps are taken to avoid attacks.

5.4.1 Threats

MITM attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker is able to intercept all messages going between the two victims and inject new ones (Andrew Lindell 2008). Weak cryptography algorithm is susceptible to MITM attack in the banking sector, which offers great risk. By implementing the PSPFW security algorithm in this transaction process, it is observed that the risk against the MITM attack is minimized, there by increasing the security of the transaction.

5.4.2 Simulation Results

The macro payment system with PSPFW Bluetooth security algorithm is simulated using JAVA CLDC tool kit. The simulated model specified in section 5.2 is adopted.
Invoice from payee to payer is depicted in Figure 5.14. The cheque validation time and encryption algorithm is mentioned. The amount requested as invoice to the payer is also displayed. The application has two menus namely, ‘File’ and ‘Connect’. ‘File’ has a submenu of ‘Exit’. It is used to exit the application. ‘Connect’ has two submenus: ‘start’ and ‘server IP’. Using start menu, the application is started. The server IP menu is used to communicate with the appropriate payer process. The payee is then asked for the amount of the purchased products by the payer. It is then sent to the payer.
Based on the invoice amount, the cheque request is made by the payer to FSP and is shown in Figure 5.15. The payer application has two menus namely, File and Server. Server has a submenu of start. By clicking start menu, the message ‘The payer started’ is displayed. After this, IP address entered to start the transaction process. The account number and the amount is mentioned.
The cheque is encrypted and sent to the payer by FSP. The information of sending the cheque is displayed in the Figure 5.16. File and server are the two menus displayed in the FSP application. File has the submenu of exit. It is used to exit the application. Server has submenu of start, which is used to perform the authentication between the payer, payee and FSP. By using the valid pass key, the channel is established and the data is sent.
Each payer has an account number, user name, password, date of birth, branch of the bank and balance amount maintained in the server database. Account number is unique for each payer. Password is secretly maintained. The details of the payers in the FSP database are displayed in Figure 5.17. The information is maintained in SQL server and the server is always active to enable the transactions.

The cheque received by the payer from FSP and in offline the payer downloads cheque from the FSP and stores it in his mobile device. It prevents the manipulation of invoice by the payee and payer after the payer confirmation.
Figure 5.18 Cheque received at the Payee Mobile Device

The cheque received by the payee is displayed in Figure 5.18. Decryption is performed to retrieve the cheque. This cheque is then sent back to the FSP which performs the backend processing.
Figure 5.19 Confirmation

In Figure 5.19, the confirmation sent to the payer from payee is shown. After the process is completed, the payee sends the confirmation through mobile device to payer and ‘Transaction Completed’ is displayed.
Figure 5.20 Attack Session

Figure 5.20 describes the FSP module where an attacker tries to hack the data by entering the wrong pass key. This is informed to the payer. ‘File’ and ‘Connect’ are the menus displayed in the attack session. ‘File’ has the sub menu of ‘Exit’. It is used to exit the application. ‘Connect’ has submenu of ‘start’ and ‘server IP’, start is used to start the application. When the server IP menu is used, it asks the entry of pass key. If pass key entry is incorrect, then notification is sent to the user regarding the attack.
Figure 5.21 Attack Notification

If the attacker tries to hack the data, time of attack and the status of the attack is displayed in Figure 5.21. The display shows that even after 1656073 attempts, the attacker is not able to hack the transaction process.
Laboratory setup of macro payment system is shown in Figure 5.22. The desktop acts as FSP Server. Two laptops are used in the system where one acts as payer and another acts as payee. Using Bluetooth dongle in desktop, it is able to communicate with the other two laptops, thereby forming a personal area network (PAN) for communication.

5.5 CONCLUSION

The field of telemedicine has seen a tremendous technical development in the developed countries. Sustained efforts are also underway in the developing countries like China, Egypt and India in this field. The timely manner of conveying the real time monitored parameter to the doctor and providing 24 hours per day supervision increases the cost of treatment. A
real time patient monitoring system with PSPFW algorithm is implemented for transmission of patient data to doctor’s mobile.

To validate the effectiveness of the proposed security algorithm a Macro payment system is simulated at the laboratory level. By performing MITM attack on the transaction, the algorithm is proven to be secure.