Body Area Network (BAN) Based Smart Security Card System: A Survey

Anup Ramesh Wadavi,Ashwin S, Chiranthan C.V, M Krishna Prasad, Sangeetha V[1]

Department of ECE, K.S. Institute of Technology, Bangalore, Karnataka, India
Assistant Professor, Department of ECE, K.S. Institute of Technology, Bangalore, Karnataka, India[1]

Abstract: ATM security has always been a major concern for everyone. Cloning of ATM cards, stealing of magnetic strip details, compromising with the security pin, etc. have been some of the major issues concerning the withdrawal of money at ATMs. In order to enhance the security for ATM cards, RedTacton based smart security card is presented. This paper looks at some of the earlier works done on ATM security and RedTacton. RedTacton is a Human Area Networking technology that uses human body as a safe high speed network transmission path. RedTacton uses minute electric field on the surface of the human body as a medium for transmitting the data. A transmission path is formed at the moment a part of human body comes in contact with RedTacton transceiver. Communication is possible using any body surfaces, such as the hands, fingers, arms, feet, face, legs or torso. RedTacton works through shoes and clothing as well. When the physical contact gets separated, the communication is ended.

Keywords: Body Area Network, RedTacton, DTMF, driver, buffer.

I. Introduction

There are many technologies present for networking which are in use. These technologies connect people, objects and other networks together so as to share data and thus make information ready for access. Nowadays, electronic devices are smaller, less expensive and lower in power requirements. We have begun to adorn our bodies with personal information and communication appliances. Such devices include cellular phones, pagers, personal digital assistants and many more. But currently there is no such method for these kinds of devices to share data. Networking these kinds of devices can reduce functional I/O redundancies and allow new conveniences and services. Human society is entering an era of modern computing, where networks are smoothly interconnected. The implementation of ubiquitous services requires three levels of connectivity: Local Area Networks (LAN), Wide Area Networks (WAN) and Body Area Networks (BAN) for connectivity to personal information, share data, media and communication appliances within the much smaller areas for communication. BAN is a technology that uses the surface of the human body as a high speed and safe network transmission path.

This project explains the unique new functional features and enormous potential of Body Area Networking technology in an Automated Teller Machine (ATM). Here, the human body acts as a transmission medium supporting half duplex communication at 10Mbit/s. The objective of this project is to give a better security system to transmit data via human body. There is no risk of hacking, as our body itself acts as the transmission medium and can be used more in fields where there is a need to upgrade the security in times of high theft rate.

II. Literature Survey

Jignesh J. Patoliya et al. [1] proposed a high level system where the system captures the human face and if not detected it will lock the door and generates a 3 digit OTP which is sent to the watchman’s RMN using GSM which will be used to unlock the door. It ensures a secured and authenticated transaction using face detection. But, the author doesn’t address about the problem against cloning of cards which is the major issue of security in ATMs nowadays.

S.Shriram and Swasthik B. Shetty et al. [2] proposed a system unlike other systems uses a number of smart sensors to detect an attack and avert it, like PIR Sensor, ADXL335 Accelerometer, FSR to detect motion, heat, change in orientation, sudden acceleration, force, and vibration. The paper puts forward a method which would provide very high security against physical attacks on ATM and robbery of cash box. But, again the author doesn’t address the issue against cloning of cards.

N V Uma Reddy et al. [3] puts forward a new approach wherein RFID card is used as ATM card, IR sensor in order to sense the presence of the card holders and to turn on Fan and Light, if ATM is tampered then SMS is sent to two main stations via GSM. GPS is used to track the location in case the cash box is robbed. Finger print is used to identify and verify authorized bank personnel. Provides a secured and authenticated transaction and also provides security for the ATM system. The only disadvantage in the proposed system is that using the ATM becomes inconvenient as the user has to first scan his/her fingerprint and then enter the OTP, and also doesn't provide any protection against skimming.

D. Narmada et al. [4] proposed a system to implement a low cost stand-alone Embedded Web Server (EWS) based on ARM11 processor and Linux Operating System using Raspberry Pi. The setup is proposed for ATM security, comprising of the modules namely. Authentication of shutter lock, web enabled control, sensors and camera control. The system provides high security for the ATM against intrusion and theft.

Sambarta Ray, and Anindya Sen et al. [5] proposed a system which is capable of counting the number of people present in the ATM kiosk, where it is possible to detect whether a person is wearing mask or not. It reduces the storage of unnecessary video feed and transmitting only an anomalous situation. This system makes efficient use of storage and bandwidth for transmission required for video surveillance and processing. The only disadvantage of this system is it does not provide anti-skimming measures.

Javier Arcenegui, Iluminada Baturone et al. [6] states that a demonstrator has been developed to illustrate the performance of a lightweight fingerprint recognition algorithm based on the feature QFingerMap16, which is extracted from a window of the directional image centered at the convex core of the fingerprint. It provides fingerprint identification with low power consumption and high accuracy. But the extraction time is very high.

Kishor Kumar, Sadasivuni et al. [7] proposed a system which senses the capacitance and pulses from human fingers. The fingerprint scanner takes an image of a user's unique fingerprint traits, the image quality is measured in dots per inch (DPI). The final step in the process is to identify and locate distinctive characteristics. It also provides anti-spoofing and high accuracy of fingerprint identification.

Rong Hu and Ming Li et al. [8] proposed system creatively puts forward CDMA as the communication medium, and takes ARM as main control unit. It has completed the entire Communication and control functions, and taken the cost into consideration. It lists out the advantages in using the DTMF technology for coding and CDMA for communication purposes. But until now, it is rare to see such products or designs using similar communication technologies.

Michael J. Callahan Jr. et.al [9] proposed a system used for DTW detection, most of which require eight narrow-band filters, one for each frequency to be detected. The major drawbacks addressed here are numerous precision components and additional logic is minimized by use of Integrated circuits. But this also creates system complexity and higher costs.

Sao-Jie Chen et al. [10] proposed two circuit-level techniques in which Razor and Surger are exploited to form a hybrid error detection mechanism by observing both global and local timing information. The paper provides systematic solutions to real-time timing error detection. Thereby, making the ARM processor power-efficient.

Wira Firdaus Hj Yaakob et al. [11] proposed a paper which describes about the design and implementation of My-MS smart card chip's prototype in Xilinx's Zynq-7000 XC7020-1-CLG484 FPGA device. The comparison is done based on terms of area and time requirements. The paper addresses some of the basic functions of the smart card embedded operating system (OS), its simulation and its implementation. The smart card chip design has been used as a national ID and health insurance.

F. A. Lima, E. D. Moreno et al. [12] proposed a paper that presents the results obtained during the simulations which measured the performance of a low-cost cluster with ARM processors. The cluster performance increased considerably when compared to Sequential solutions and this good speedup is better when the measured amount of processed data also increased.

Sandeep Raj, T. C. Krishna Phani et al. [13] proposed a paper which presents the analysis of various disturbances like voltage swell, voltage sag, spike and harmonics by using a signal processing technique. In this paper, all the power disturbances caused, are analyzed, to give a better resolution for the ARM processors, to make them more power-efficient.

Teodor Neagoe, Ernest Karjala et al. [14] proposed a paper which talks about the way in which attention to detail in voltage management, conditionally executable instructions cache controller design, etc. contribute to the ARM architecture's high performance and low power operation. It lists out the detailed advantages of the ARM processors for low-power applications, which makes the processor a better suit.

Thang Manh Tran Gustavo Vejarano [15] designed a system that predicts the received signal strength during activity at the elbow and shoulder joints, using BAN. Numerous wireless sensor nodes are attached near the joints to predict the RSSI. It mainly helps athletes and sportspersons to know their joint movements and helps them to correct it.

Muhammad Usman Shahid Khan, Assad Abbas, et al. [16] proposed a method to detect the type of physical activity of patients using BAN. It helps in diagnosing and treatment, by placing different sensors on the body. It might help in recognition of some particular type of diseases which are hard to diagnose. It may become uncomfortable, since a lot of sensors are placed.

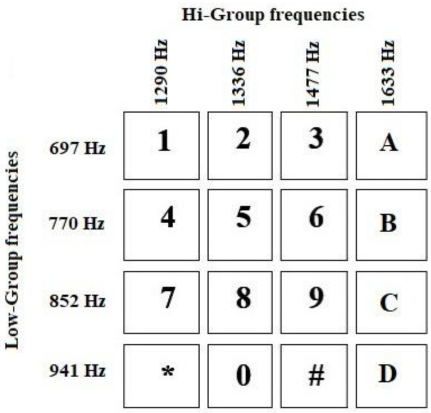
Yuichi Kado, Taku Kobase, et al. [17] proposed a system that helps to broaden the fields of application by not only placing transceivers on the body, but also embedded on the floors, PCs, equipment, etc. It helps in the better and faster transmission of signals, as there are transceivers everywhere. It becomes expensive, as it requires a setup of a lot of transceivers everywhere.

Tanveer Rashid, Muhammad Riaz et al. [18] proposed a paper which talks about how BAN can be employed by physical contact and also by implanting the sensors under the human skin. It gives an account of the safety of humans in BAN and different applications.

III. Proposed Method

a. DTMF Encoder and Decoder

Each digit in DTMF (dual tone multi-frequency) code corresponds to a combination of two discrete frequencies, one each from a low and high group of frequencies, which are generated when any switch on a dialler key-pad is pressed. Such a key-pad along with the frequencies is associated with each row and column (Fig 1).



Hi-Group frequencies

Low-Group frequencies	1290 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Fig.1 Tones in DTMF Dialling

The DTMF encoder encodes the signal and is transmitted to the DTMF decoder. The transmission medium that is used is the human contact with the help of touch plates. The touch plates used are of Copper material. The DTMF encoded signal is given to the touch plate which has been suitably mounted on the body. The receiving touch plate is on the receiver side that is on the ATM machine. The user has to make contact with this touch plate for authentication from where the signal is sent to the DTMF Decoder. The DTMF code being used is in the form of BCD as a DTMF to BCD converter is used before transmission. Hence the decoder receives signal in the form of BCD or hexadecimal which represents a combination of frequencies.

b. Microcontroller and supporting peripherals

The microcontroller we use is LPC2148. The LPC2148 is a 32-bit RISC microcontroller. It is a widely used IC from ARM-7 family. It is manufactured by Philips (NXP) and it is pre-loaded with many inbuilt peripherals making it more efficient and a reliable option. It has 8kB to 40 kB of on-chip static RAM and 32kB to 512 kB of on-chip flash program memory.

This allows us to reprogram the IC as and how we wish. This microcontroller houses the main ATM code, which is to ask for the PIN and to authenticate the user.

We use a specially designed power supply to get the +12V and +5V regulated voltages to run the whole setup. The power supply plays a very important role in smooth running of the connected circuit. The main object of this 'power supply' is, as the name itself implies, is to deliver the required amount of stabilized and pure power to the circuit. The power supply that we are using has 4 stages. The stages being Step-down Transformer, Rectifier Stage, Filter Stage and the Voltage Regulation Stage.

We use the IC4050 HEXBUFFER. The logical state of a digital signal is not affected by the Buffer. Buffers are normally used to provide extra current drive at the output, but can also be used to regulate the logic present at an interface. The inverters are used to complement the logical state (i.e. logic 1 input results into logic 0 output and vice versa). Also Inverters are used to provide extra current drive and, like buffers, are used in interfacing applications. This 16-pin DIL packaged IC 4050 acts as Buffer as-well-as a Converter. The input signals may vary from 2.5 to 5V digital TTL compatible or DC analog but the IC always gives 5V constant signal output. The IC acts as buffer and provides isolation to the main circuit from varying input signals. The working voltage of IC is 4 to 16 Volts and propagation delay is 30 nanoseconds. It consumes 0.01 mW power with noise immunity of 3.7 V and toggle speed of 3 Megahertz.

We also use the ULN2003 relay. Relays are basically electromagnetic devices which are activated by current or voltage in one circuit to activate or deactivate another circuit. This voltage or current in some circuits may sometimes not be able to directly drive the relays. Thereby high-voltage high-current Darlington arrays are designed to interface with such circuits. The series ULN2000A/L ICs can drive up to seven relays. Typical loads for relays include magnetic print hammers, solenoids, stepping motors, multiplexed LED and incandescent displays and heaters. These Darlington arrays are furnished in 16-pin dual in-line plastic packages and 16-lead surface-mountable SOICs. An additional feature of this IC is that all the output pins are opposite to the input pins, this makes it easy for circuit board layout.

c. Output Peripherals

The output peripherals we use are 16X2 LCD, buzzer and APR33A3 voice chip. The buzzer rings every time there is an unauthorized user trying to access the system. The voice chip is used to store 4 pre-recorded messages, each message being 15 to 20 seconds long.

d. RF Transmitter and Receiver

To add an extra layer of security, we have added a RF transmitter and receiver. The transmitter will be placed in the system and whenever there is an unauthorized signal/user detected, it sends a signal to the receiver which can be placed in the nearest police station or the bank branch. The receiver also has a microcontroller and we have used the same microcontroller. The code is burnt into the IC and whenever it detects an unauthorized signal a buzzer starts ringing and on the LCD, 'unauthorized' is shown.

IV. Block Diagram

The block diagram is shown in figure 2. The encoder generates the signal and sends it to the touch plate which is in contact with the human body. When the human comes in contact with the touch plate on the machine, the signal is transferred through the body to the decoder. The decoder, decodes the signal and sends it to the microcontroller. If it is an authorized signal, then the LCD display will ask to enter the password or verify the fingerprint, upon verification of which it will display whether or not the entered password is correct. Now if the signal sent is detected as unauthorized by the microcontroller then the buzzer starts ringing and the microcontroller circuit is switched off using the relays. A paging message also reaches the nearest police station, stating there is a breach.

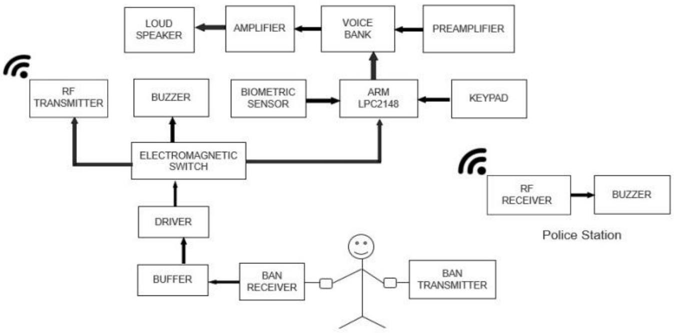


Fig. 2. Block Diagram of the proposed system

There is always the question of human safety. How safe this would be for the human health? In real time we will be using RedTacton devices. The electrodes of the RedTacton is completely covered so the human body is also completely insulated. The electrons that are present in our body generate something called the displacement current when there is transmission in progress. This is because the body is subjected to minute electric fields. However, such displacement currents are very common everyday occurrences to which we are all subjected. RedTacton conforms to the "Radio Frequency-Exposure Protection Standard (RCR STD-38)" issued by the Association of Radio Industries and Businesses (ARIB). The levels produced by RedTacton are well below the safety limit specified by this standard.

V. Methodology

The proposed system consists of a RedTacton transmitter, receiver, driver, microcontroller unit, voice chip and regulator. RedTacton is a Human Area Networking technology, which uses human body as a safe channel for transmitting the signal. A transmission path is formed, the moment a part of the human body comes in contact with a RedTacton transceiver. Communication is possible using any body surfaces, such as the hands, fingers, arms, feet, face, legs or torso. RedTacton works through shoes and clothing as well. When the physical contact gets separated, the communication is ended.

The RedTacton transmitter induces a weak electric field on the surface of the body. The RedTacton receiver senses changes in the weak electric field on the surface of the body caused by the transmitter. This module consists of a RedTacton transmitter, RedTacton receiver, Driver, Microcontroller unit and the Voice bank. RedTacton is a HAN; the human body is used for transmission of signals. RedTacton transmitter consists of a DTMF encoder which generates both valid and invalid signals and can be transmitted through human body through the RedTacton receiver (DTMF decoder) for further processing. In the RedTacton receiver, the transmitted signal is identified with the help of a DTMF decoder. As the transmitted signal is of very low voltage, buffers and drivers are used to send the received signal to the electromagnetic switch. Electromagnetic switch checks the received signal with the predefined valid code. If an invalid code is received and detected in the switch, then the buzzer starts ringing indicating that an invalid card is trying to access the ATM. Also, a message is sent through paging to a nearby police station, indicating an unauthorized card usage. If a valid code is received, only then the switch sends the signal to the main control unit which is the microcontroller. When the microcontroller gets active, it switches on the keypad where predefined options are stored to perform various tasks such as entering the password, change of password, new password, etc. There is also an option of using the biometric sensor to verify the fingerprint of the card holder for verification. After entering the valid password the voice bank gets activated. In voice bank predefined options with keys are present which guides the user to select appropriate action in the ATM such as cash withdrawal, pin change, account balance, etc.

VI. Advantages

i.) RedTacton does not require the electrode to be in direct contact with the skin.
ii.) High-speed communication is possible between any two arbitrary points on the body.
iii.) Body-based networking is more secure than other broadcast systems, such as Bluetooth which has high range of about 10m.
iv.) Network congestion due to fall in transmission speed in multiuser environments is avoided.
v.) Superior than Infrared technology.
vi.) Superior than Wi-Fi.

VII. Disadvantages

i.) It has no compelling applications that aren't already available.
ii.) It may be slightly expensive.

VIII. Conclusion

This technology definitely stands out with perfection, when transfer of data is fast, feasible and more importantly reliable. So, in few years from now everything is going to fall under this super technology.

IX. References

[1]. J. J. Patoliya and M. M. Desai, "Face detection based ATM security system using embedded Linux platform," *2017 2nd International Conference for Convergence in Technology (I2CT)*, Mumbai, 2017, pp. 74-78.

[2]. S.Shriram1,Swastik B.Shetty1,Vishnuprasad P.Hegde1,KCR Nisha2,Dharmambal.V3, Department of electronic communication engineering, Bangalore ,India, ”Smart ATM surveillance system”/International Conference on power circuit, power and computing technologies[ICCPCT],2016.

[3]. Bharathi M Nelligani, Dr.N V Uma Reddy, Mr.Nithin Aswathi, Banglore, India, ”Smart ATM security system using GPS, FPR, GSM”,/International conference on inventive Computing technologies,Vol.3,page 1-5,2016.

[4]. D. Narmada and J. V. Priyadarsini, "Design and implementation of security based ATM using ARM11," *2016 International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, 2016, pp. 1-4.

[5]. S. Ray, S. Das and A. Sen, "An intelligent vision system for monitoring security and surveillance of ATM," *2015 Annual IEEE India Conference (INDICON)*, New Delhi, 2015, pp. 1-5.

[6]. J. Arcenegui, R. Arjona and I. Baturone, "Demonstrator of a fingerprint recognition algorithm into a low-power microcontroller," *2017 Conference on Design and Architectures for Signal and Image Processing (DASIP)*, Dresden, 2017, pp. 1-2.

[7]. K. K. Sadasivuni, M. T. Houkan, M. S. Taha and J. J. Cabibihan, "Anti-spoofing device for biometric fingerprint scanners," *2017 IEEE International Conference on Mechatronics and Automation (ICMA)*, Takamatsu, 2017, pp. 683-687.

[8]. Wei Song, Ming Li and Rong Hu, "A wireless access control system based on CDMA and DTMF technologies," *Proceedings of 2011 International Conference on Computer Science and Network Technology*, Harbin, 2011, pp. 759-761.

[9]. M. Callahan and H. Davis, "An integrated dual-tone multi-frequency decoder," *1978 IEEE International Solid-State Circuits Conference. Digest of Technical Papers*, San Francisco, CA, USA, 1978, pp. 88-89.

[10]. S. J. Chen, G. Liu, H. P. Yang, C. H. Luo and W. M. Hwu, "Design of a power-efficient ARM processor with a timing-error detection and correction mechanism," *2016 29th IEEE International System-on-Chip Conference (SOCC)*, Seattle, WA, 2016, pp. 217-222.

[11]. W. F. H. Yaakob, H. H. Manab and S. N. M. Adzmi, "Smart card chip design implementation on ARM processor-based FPGA," *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)*, Tokyo, 2014, pp. 294-297.

[12]. E. Moreno, F. A. Lima and W. R. Azevedo Dias, "Performance Analysis of a Low Cost Cluster with Parallel Applications and ARM Processors," in *IEEE Latin America Transactions*, vol. 14, no. 11, pp. 4591-4596, Nov. 2016.

[13]. S. Raj, T. C. K. Phani and J. Dalei, "Power quality analysis using modified S-transform on ARM processor," *2016 Sixth International Symposium on Embedded Computing and System Design (ISED)*, Patna, 2016, pp. 166-170.

[14]. T. Neagoe, E. Karjala and L. Banica, "Why ARM processors are the best choice for embedded low-power applications?," *2010 IEEE 16th International Symposium for Design and Technology in Electronic Packaging (SIITME)*, Pitesti, 2010, pp. 253-258.

[15]. T. M. Tran and G. Vejarano, "Prediction of received signal strength from human joint angles in body area networks," *2016 International Conference on Computing, Networking and Communications (ICNC)*, Kauai, HI, 2016, pp. 1-6.

[16]. M. U. S. Khan *et al.*, "On the Correlation of Sensor Location and Human Activity Recognition in Body Area Networks (BANs)," in *IEEE Systems Journal*, vol. PP, no. 99, pp. 1-10.

[17]. Y. Kado *et al.*, "Human-area networking technology based on near-field coupling transceiver," *2012 IEEE Radio and Wireless Symposium*, Santa Clara, CA, 2012, pp. 119-122.

[18]. T. Rashid, M. Riaz and M. Y. Wani, "Safety of human in body area network: A review," *2017 International Symposium on Wireless Systems and Networks (ISWSN)*, Lahore, 2017, pp. 1-5.