An Efficient Architecture for Trusted Financial Services in ATM

Mukul Pathak[1], Uday Pratap Singh[2], Neeti Bhatnagar[3] and Garima Srivastava[4]

[1, 2] Department of Computer Science & Engineering, Galgotias College of Engineering & Technology, Greater Noida (U.P.), India
[3] Department of Computer Science & Engineering, College of Engineering & Technology, Moradabad (U.P.), India
[4] Department of Computer Science & Engineering, United Institute of Management
Allahabad (U.P.), India

ABSTRACT

Financial service outlets such as ATMs are vulnerable to various attacks like shoulder surfing, data skimming, fake machines etc. Therefore these outlets are easy targets for attackers. In the current financial service transactions, there is no provision for users to verify genuineness of the financial service outlets like ATMs. Therefore users are forced to trust the ATMs. Fake ATM can be designed to steal the account information and private information like password from the user. This information later can be used to steal money from the user. Further, the financial outlets require a dedicated communication channel for user authentication. Installing these outlets is therefore an expensive operation. In this work, we are providing Secure Communication Protocol for financial services based on a smart card. By authenticating ATM, the user is ensured of the genuineness of the ATM. Hence fake ATM cannot steal the user information. After the session establishment, communication is carried out in encrypted form. This way the attacker cannot get any meaningful transaction information. Thus our approach handles security vulnerabilities in the current model. Transaction cost in our approach is significantly reduced, compared to the current model because the continuous network is not required due to localized authentication process.

***KEYWORDS*- Secure ATM; Attacks on financial services; Communication Architecture; Network Security.**

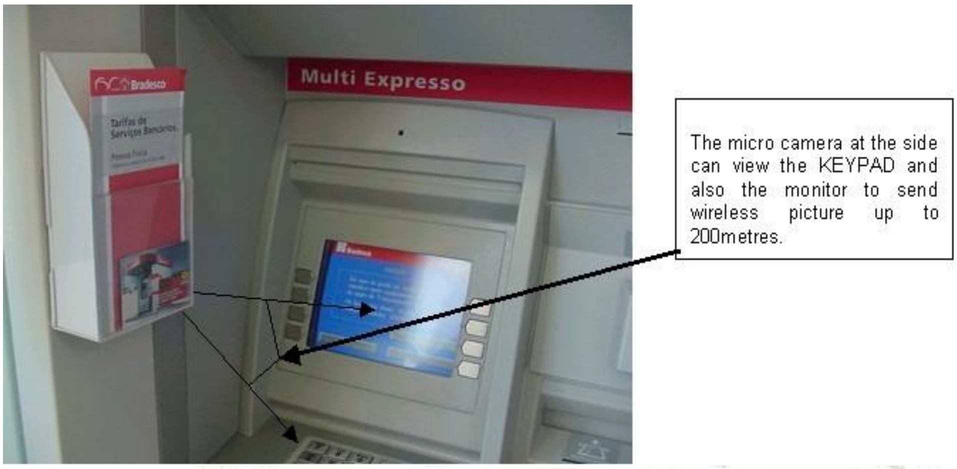
1. INTRODUCTION

There is gradual increment in uses of Electronic Commerce to a level, where it has captured the role of processing transactions from physical bank branches. The convenience offered by e-commerce has resulted in it becoming necessary part of our daily life so commercial organizations like banks, credit card companies, insurance companies etc. have shown great interest towards providing new technologies to their users. These technologies are provided in form of variety of services like ATM, credit cards, electronic fund transfer etc. These organizations vie for greater share in user market by introducing newer and better services. But current services have some security flaws. Fraudsters try to exploit these flaws. It is therefore desirable to cover these flaws and ensure that the security is not compromised. Our approach is a step towards meeting this goal.

Financial service outlets like ATMs are now very important part of one’s daily life. Any time a user wants to withdraw money, instead of going to the bank he goes to an ATM. While shopping, user can pay bills at Point of Sale (POS) using ATM cards instead of cash payment. Performing these transactions is very swift and less time consuming as compared to visiting a bank. But there are some issues with current financial services as listed below.

1.1 Infrastructure Cost

An ATM incurs the cost for I/O devices, communication devices to contact central database server of the bank and also for cooling. A dedicated link between ATM and central database server has to be maintained, because of two reasons. The link is used to authenticate a user and to update log of transactions, performed by the user. Due to this setup, transaction cost is very high.



The micro camera at the side can view the KEYPAD and also the monitor to send wireless picture up to 200metres.

1.2 Trust Issues

In current financial service system, only user authentication mechanism is used. There is no way to check the authenticity of ATM machine or machine used for electronic fund transfer like a Point of Sale (POS) device. In such a scenario, an attacker can install a fake machine and can steal user information like account information and other private information such as PIN.

1.3 Attacks on Financial Service Outlets

With the use of electronic mechanisms in financial services, frequency of attacks on machines has also increased. Current financial service outlets can be compromised in variety of ways as described below.

1.3.1 Fake Automated Teller Machine

In this attack, the attacker installs a fake ATM which is similar to the genuine machines. Since in current approach, user can not authenticate the ATM, he cannot verify whether the machine is genuine or not. So user has to use the ATM without any trust. The fake machine can read all user account information also it can record user private information (like PIN). Attacker can use this information to

Forge duplicate ATM card First recorded instance [5] of using fake ATM occurred in 1993, in Connecticut, Manchester, when some criminals put bogus ATM. It was used to create forged ATM cards.

1.3.2. Shoulder Surfing

In this attack, an attacker can look directly, or can use video cameras, to capture PIN entered by an user. Wherever merchants accept ATM cards, there are ample opportunities to observe PIN entered by a user as the environment is more open and public. In Figure 1.1 a brochure holder is organized in such way that it captures PIN entered by a user. This technique is normally used with skimming devices, which record account information stored on card. Using both techniques attacker can forge duplicate card successfully.

.

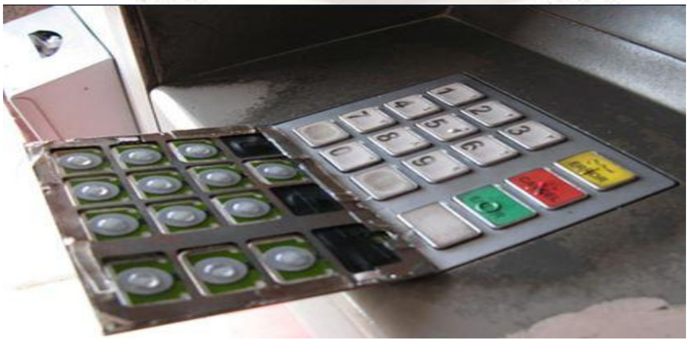
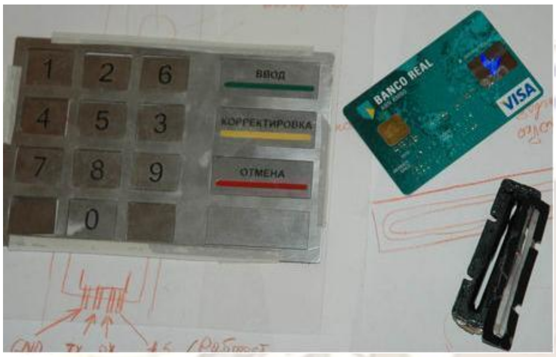


Figure 1.1: Micro Camera Embedded in Different Positions

1.3.3 Skimming Devices

An invader can record data from magnetic strip of ATM cards by using skimming devices (figure1.2). These devices can be clamped together with card reader of ATM and can record data of multiple (~200) ATM cards. These devices are often used by attackers, at point of sale (POS) in shops or restaurants, where cards are handled by staff. These devices are especially dangerous whenever they are used for credit card swiping, as they can be used to record credit card numbers. There are various criminal cases where this technique was used to store credit card numbers and other information.



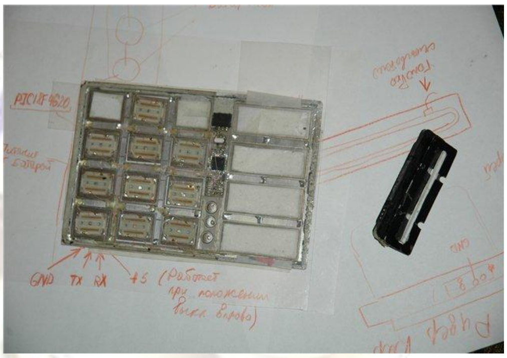
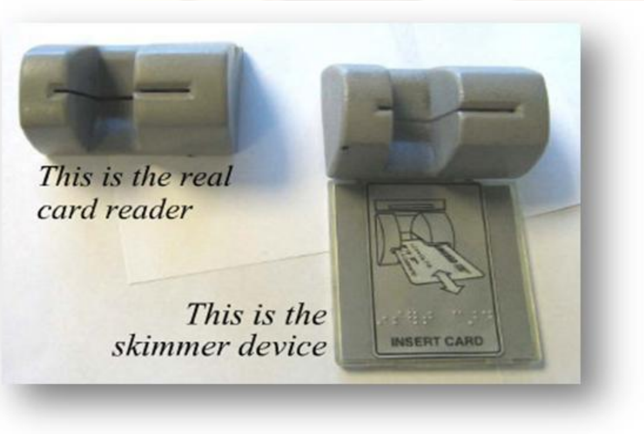


Figure 1.2: Skimming Device Attached to ATM

Figure 1.3: Fake Keypad

1.2.4 Fake Keypad Overlay Attack

In this kind of attack, the attacker places fake keypad overlay over a genuine keypad. The fake keypad overlay is transparent and cannot be detected easily by naked eye. The fake overlay then stores pressed keypad buttons with time. This information can be used to compromise PIN.



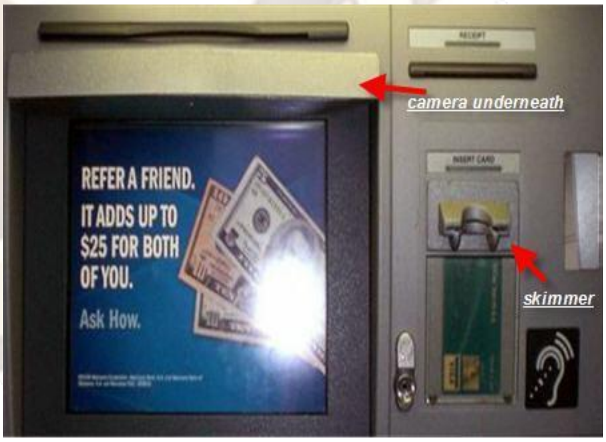


Figure 1.4: Fake Keypad Overlay

Figure 1.5: Fake Keypad Overlay Backside

Figure 1.3 show the Fake keypad and Figures1.4 and1.4 show the electronic circuit on back side of keypad overlay that record and stores user’s key presses.

1.4 Why Smartcard?

Smart cards improve the convenience and security of transactions. They provide tamper-proof storage of user and account identity. Smart card systems have proven to be more reliable than other machine-readable cards, like magnetic strip. They protect against a full range of security threats, from careless storage of user pass-words to sophisticated system hacks. Smart cards are chosen for applications with security concerns, due to their small size, data storage capability and processing abilities.

Smart cards which we are using an operating system (OS). This OS supports security mechanisms like encryption, decryption, authentication, session key establishment etc. based on both symmetric and asymmetric key algorithms. It also supports various file and data access mechanisms.

Since a smart card provides for mutual authentication mechanism, in our financial service system, the users do not have to trust the financial outlets. The smart card can check the authenticity of outlets. Smart cards also allow various measures to provide access and security control for application data. Hence transaction information can also be stored on smart card without losing the aspects of security. In our approach, financial outlets do not have to contact bank database server for each transaction performed on ATM. This reduces dedicated network cost, which in turn reduces the transaction cost. Smart cards also provide session key establishment facility to provide data confidentiality. Data transferred between smart card and financial outlet can be encrypted by session key. Even where an attacker captures this data, he cannot use it for forgery.

2. Related Work

Han et al.[10] came up with hybrid concept of Biometrics based authentication scheme for ATM like banking applications. They proposed two level authentication process, first level based on PKI and second level authentication based on biometrics like fingerprint or iris matching. In this model, authentic biometric reference data is stored on a database server of the bank. Therefore, this model requires a dedicated network and secure channel between ATM and database server to retrieve reference biometric information and to match biometric data. Further, biometric devices are expensive to deploy, the size of biometric data exchanged between the ATM and server is large causing the operations such as transfer of data, encryption, processing etc. to be resource expensive, thereby increasing the cost of transaction. Jhunjhunwala [4] proposed a design of low-cost ATM for deployment in rural areas. Further, their ATM, known as Gram teller does not need personal information and magnetic stripe cards, but uses smart cards and biometrics based on fingerprints. Gram teller is connected to a PC with internet access. It communicates with bank database server through this PC. Installation cost in this model is very low. However, it suffers from security vulnerabilities and unreliable network connection. Around the world, financial corporation’s (like Visa, MasterCard, Discover, and American Express) have rolled out smart cards under the EMV (Europe, MasterCard, VISA) standard [9]. The majority of implementations of EMV cards and terminals confirm the identity of the cardholder by requiring the entry of a PIN.EMV standards implement only some of the commands defined in ISO/IEC 7816-4 standard.

Moona et. al. [3] proposed a solution which uses mobile devices (like mobile phones or laptops) of user to communicate with ATM machine. This model does not require I/O console or keypad. It also eliminates the need of dedicated network as transaction records can be stored on mobile devices. Since keypads or I/O console are not used, their approach eliminates the possibility of fake keypad overlay attack, or use of skimming devices. This solution reduces infrastructure and transaction cost significantly.

Munjal et. al. [8, 1] proposed a new financial service model to overcome various drawbacks in the current model. Smart cards are used to provide secure storage for data, which protect data from unauthorized writing and reading. In this model, new secure protocol for communication between ATM and smart card is proposed based on PKI. This model removes need of dedicated network and reduces transaction cost. The paper work we have done is mainly based on the work of Munjal et. al.

3. Layered Architecture

As described earlier, there are various shortcomings in current financial service model. In our paper, we know the Deployment Scenario for financial services that will overcome these shortcomings. We use a smart card in our system to provide security framework. Application uses computation and storage capabilities of a smartcard for secure storage and authentication. The organization of our layered architecture is as shown in figure 3.1.

Interface layer
Command library layer
Smart card reader layer
Smart card layer

Figure 3.1: Layered Architecture

- **Smart Card Layer:** The smart card layer comprises of a smart card that communicates with the application with the help of a device known as 'reader'. Communication between a smart card and the reader is half-duplex, that is only one side can transmit data at a time. Communication is always initiated by the reader which sends commands to the card. The card then responds with the output for the command. Smart card uses an operating system known as SCOSTA-PKI to provide standard mechanisms of command and data exchange. SCOSTA-PKI is an operating system compliant to ISO standards

- **Smart Card Reader Layer:** Smart card readers are used as communication medium between the smart card and a host (like a computer, a point of sale terminal) or a mobile telephone. Smart card readers are available in two categories: contact smart card readers, contactless smart card readers based on 'radio frequency'.

- **Command Library Layer:** Command library is a standard C++ library developed for handling smart card interactions, according to SCOSTA specifications (SCOSTA-CL, SCOSTA-PKI).

- **Interface Layer:** Interface layer is the uppermost layer in the layered architecture of our application. It directly communicates with the user of the application. This layer is the software application that implements secure ATM protocol.

4. Proposed Work

4.1 Secure Communication Protocol

There are various protocols to establish mutual authentication and to derive session key between two communicating parties. Some of examples for these protocols are Diffie-Hellman Key Exchange protocol [7], RSA (Public key) based session key establishment protocol, IPSEC protocol, Kerberos, TLS protocol [6] etc.

4.1.1 Deployment Scenario 1

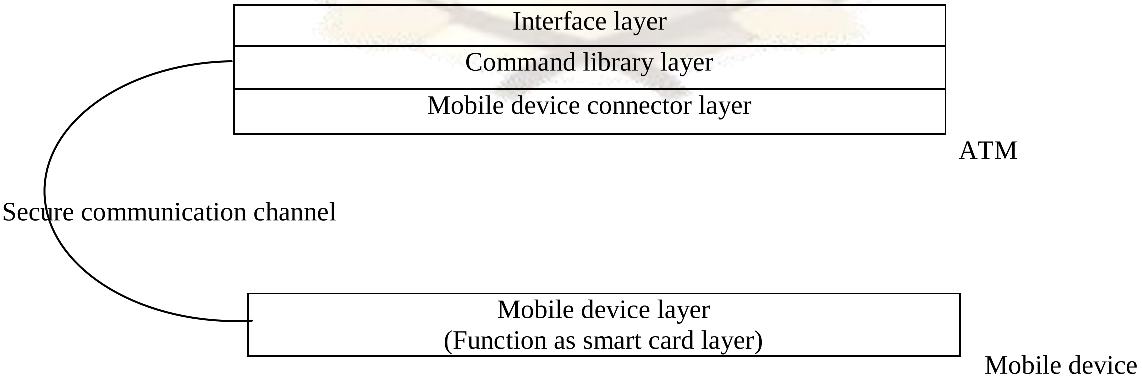

Interface layer
Command library layer
Mobile device connector layer
ATM
Secure communication channel
Mobile device layer
(Function as smart card layer)
Mobile device

Figure 4.1: Deployment Scenario 1

In this scenario, the user uses a personal electronic device like mobile phone. It has capability to communicate

with the financial service outlet using either Bluetooth [11] or infrared or USB [2] communication technology. All user's personal information, user's digital certificates, and account information are stored on the personal device. This information need to be transferred from the mobile device to the financial outlet. Since this information is private, it should be transferred confidentially. So attackers cannot get this information.
As shown in figure 4.1, we have applied layered architecture. The mobile device layer acts as the smart card layer. We establish secure communication channel between mobile device layer and command library layer using secure communication protocol.

4.1.2 Deployment Scenario 2

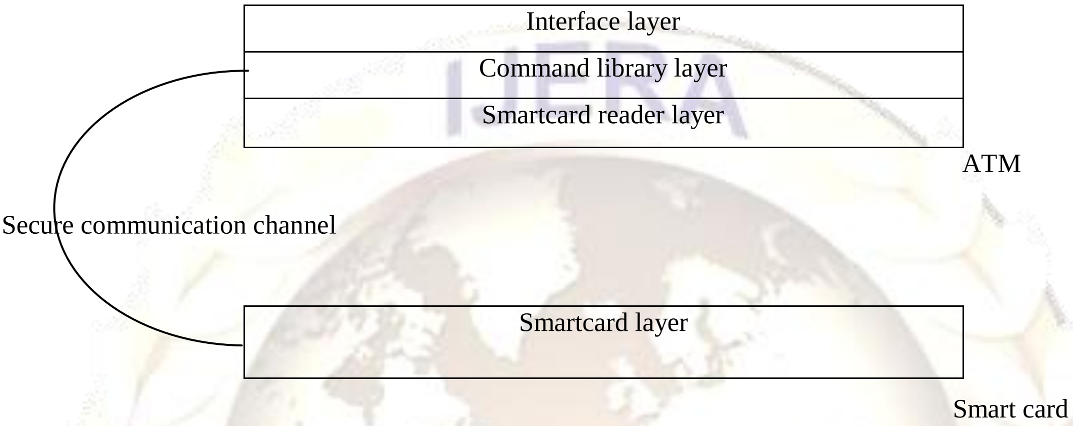


Figure 4.2: Deployment Scenario 2

In this scenario, the user uses a smart card to store personal information, certificate chain, and account information. Smart card communicates with the financial outlet service. This communication is made secure by using secure communication protocol. Layered architecture for this scenario is shown in figure 4.2 Secure communication protocol establishes secure channel between smart card layer and command library layer.

4.1.3 Deployment Scenario 3

In this scenario, a smart card is connected to the mobile device and the mobile device is connected to the financial outlet. Layered architecture for this scenario is rearranged as shown in figure 4.3. Since the smart card contains the private information of the user, secure channel is established between smart card layer and command library layer in mobile device, using secure communication protocol.

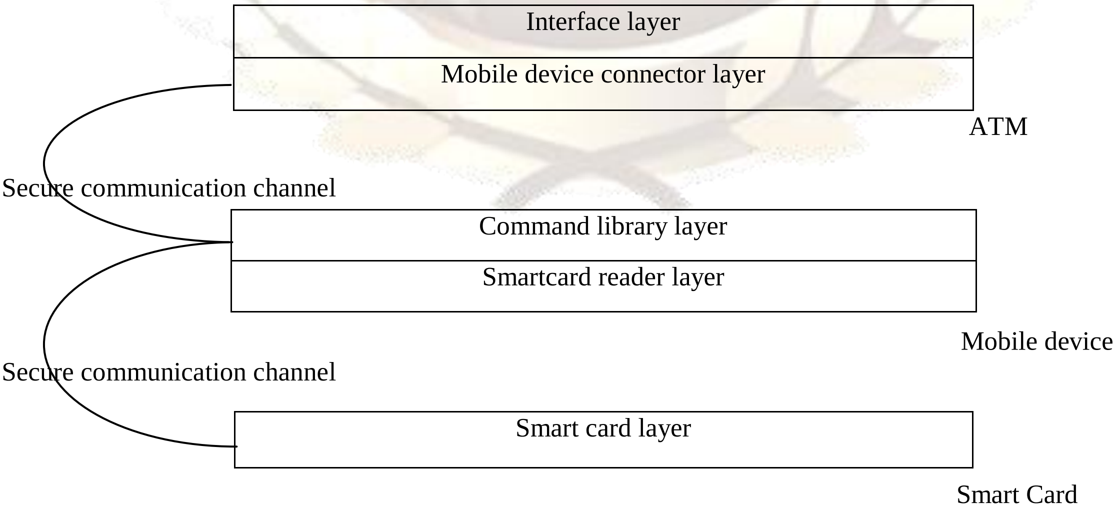


Figure 4.3: Deployment Scenario 3

5. RESULTS & OBSERVATIONS

This paper has discussed the attacks and Architecture of application which can be used in ATM easily. After implementation it is observed that:-

- A fake outlet will not be authenticated by the smartcard and therefore personal and confidential data of the user will not be revealed. Therefore, a fake ATM attack (Section 1.2.1) is not possible.
- User can identify whether outlet is genuine or not, he will not enter his PIN on untrusted outlets. In this way, attacks like shoulder surfing (section1.2.4) and fake keypad overlay attack (section 1.2.3) can be avoided in most cases.
- The communication between the outlet and the smart card is in encrypted form. This makes skimming devices (section 1.2.2) useless.
- In the current financial service model, a dedicated link is maintained between the outlet and the bank database server. The link is used to authenticate the users and to update transaction logs. In our approach, there is no need to maintain the dedicated link as, user authentication is performed locally. The transaction logs are stored securely on the smart card and on the ATM. These transaction logs can be updated periodically to the bank database server by the ATM. Therefore, transaction cost is reduced significantly.

6. Conclusion

In this work, we discuss financial service model and implemented Scenario for this. This model addresses various security flaws in current financial service model. Our financial service model is secure model with low transaction cost. With low transaction cost, it is feasible to introduce financial services in less- developed areas and contribute to the development of these areas.

There are three deployment scenarios for the proposed financial service model. We implemented scenario consisting smart card and financial outlet (ATM). Secure channel is established between the smart card and the financial outlet using a secure communication protocol based on the public key infrastructure (PKI). All Communication between these two entities is in encrypted form.

7. Future Work

Our Scenario implements the deployment scenario containing smart card and ATM. It is however susceptible to fake keypad overlay attack and shoulder surfing, in some cases. These attacks can be avoided if the user can enter the PIN in his personal mobile device.

This ability is provided in the deployment scenario consisting of smart card connected to the mobile device and personal mobile device connected to the ATM. An application can be developed on the mobile device which can communicate with the ATM and the smart card securely. In this implementation scenario, an NFC enabled mobile device can communicate with a contactless smart card. The mobile device can communicate with financial outlet via USB or Bluetooth communication technology.

8. References

[1] Nitin Munjal and Rajat Moona. “Secure and Cost Effective Transaction Model for Financial Services”. OPNTDS-09, 2009.

[2] Universal serial bus - implementer’s forum. http://www.usb.org/home.

[3] A. Gaurav, A. Sharma, V. Gelara, and R. Moona. “Using Personal Electronic Device for Authentication-Based Service Access”. In Communications,2008, pages 5930–5934. ICC’08, IEEE International Conference, May 2008.

[4] Ashok Jhunjhunwala. “Banking towards rural empowerement: challenges and oppurtinities” September 2006.

[5]I.DieBold, ATM Fraud and security http://www.diebold.com/atmsecurity/resources.htm, September 2006.

[6] Dierks,T. and Rescorla, E. RFC5246:The Transport Layer Security (TLS) Protocol Version 1.2 RFC Editor United States, August 2008.

[7] W. Diffie and M. E. Hellman. Multiuser cryptographic techniques. In AFIPS'76: Proceedings of the June 7-10, 1976, national computer conference and exposition, pages 109–112, New York, NY, USA, 1976. ACM.

[8] Nitin Munjal, Ashish Paliwal, and Rajat Moona. "Low Cost Secure Transaction Model for Financial Services".In International Conference on Security and Identity Management(SIM)-09. IIM Ahmedabad, India, May 2009

[9] EMVco. EMV standards. http://www.emvco.com/.

[10] Fengling Han, Jiankun Hu, Xinghuo Yu, Yomg Feng, and Jie Zhou. "A novel hybrid crypto-biometric authentication sceeme for atm based banking applications". In David A.Zhang and Anil K. Jain, editor, ICB,volume 3832of Lecture Notes in Computer Science, pages 675–681. Springer, 2006.

[11] Bluetooth special interest group.http://www.bluetooth.org.

Authors:

Mukul Pathak

The author is pursuing M-Tech in CSE from Galgotias College of Engineering & Technology, Greater Noida (U.P.). He had completed B-Tech from College of Engineering & Technology; Moradabad affiliated to Gautam Buddha Technical University in 2010.

Uday Pratap Singh

The author had worked in HCL Infosystems Ltd. and some other well known organizations and he is pursuing M-Tech in CSE from Galgotias College of Engineering & Technology. He had completed B-Tech from Shambhunath Institute of Engineering and Technology; Allahabad (U.P) affiliated to Uttar Pradesh Technical University in 2008.

Neeti Bhatnagar

The author is pursuing M-Tech in CSE from College of Engineering & Technology, Moradabad (U.P.). She had completed B-Tech from College of Engineering & Technology; Moradabad (U. P.) affiliated to Uttar Pradesh Technical University in 2009.

Garima Srivastava

The Author is currently working in a well known Institute as a lecturer. She had completed Bachelor of Computer Application from United Institute of Management Allahabad (U.P.).