A Novel Approach for Enhancing Security in Smart Cards using Biometrics

P.Praveen
Research Scholar,
K.L.University,
A.P.,India.

S.Balaji
Professor,
K.L.University,
A.P.,India

A.S.N.Chakravarthy
Professor,
K.L.University,
A.P.India.

ABSTRACT

To provide security in Smart cards is a challenging problem because now-a-days the use of smart cards is being increased.Biometrics is one among the security providing issues which shows the path to increase the level of security in smart cards.Here the biometric template is stored in the memory of the smart card as well as the databases of the servers.The authentication is performed at the both sides i.e.,in smart card and central server.After the essential authentication and verification levels only,smart card can be accessed

Keywords

Authentication, Biometrics, Data security, Smartcards, Verification.

1.INTRODUCTION

1.1 Biometrics

Biometrics [1] is the term is which is associated with the use of unique physiological characteristics to identify an individual. A variety of biometric traits have been developed and are used to authenticate the person's identity such as face, iris, fingerprint, signature etc.A biometric system can be used either as an 'identification' system or a 'verification' (authentication) system, which are defined below

Identification – This is called as 'One to Many' process. The biometric identity captured without the person's knowledge is used for identification process.

Verification – This is called as 'One to One' process.In verification, biometric templates are used to verify a person's identity.

1.1.1 Types of Biometrics

Fingerprint: It uses the patterns found on the fingertip.

Face Recognition:It analyzes the characteristics of an individual's face.

Hand Geometry: It measures the shape of the hand.

Iris Scanning : In this, the unique characteristics of the human iris are analysed to identify an individual

Voice: Voice authentication is based on voice-to-print authentication, where complex technology transforms voice into text.

1.1.1.1 Fingerprint Biometrics

A fingerprint [2] consists of number of ridges and valleys on the surface of the finger. The upper skin layer segments of the finger are called ridges and the lower segments are called valleys. The ridge forms are called as minutia points.A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Fingerprint matching techniques can be placed into two categories: minutae-based and correlation based.

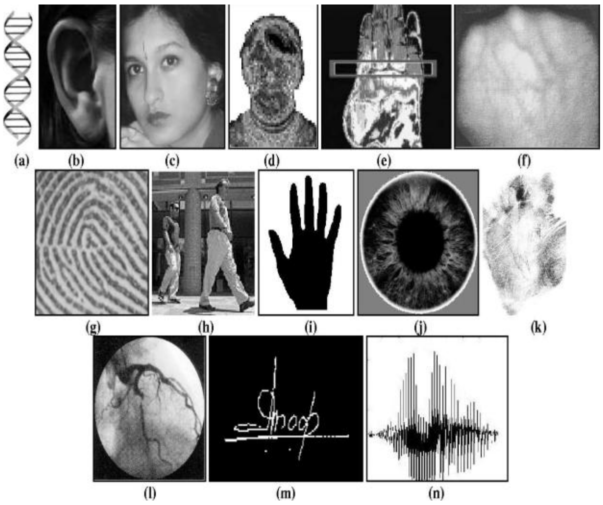


Fig 1: Examples of biometric characteristics: (a) DNA, (b) ear, (c) face, (d) facial thermogram, (e) hand thermogram, (f) hand vein, (g) fingerprint, (h) gait,(i) hand geometry, (j) iris, (k) palmprint, (l) retina, (m) signature, and (n) voice

Fig 2: Fingerprints Sample Illustration

Minutia matching compares only the specific issues of the fingerprint ridges. At the enrollment stage, the minutia points are located, together with their relative positions to each other and their directions. At the matching stage, the fingerprint image is processed to extract its minutia points, which are then compared with the enrolled(registered) template.Fingerprint matching based on minutiae has problems in matching different sized (unregistered) minutiae patterns. Local ridge structures can not be completely characterized by minutiae.

The limitations of biometrics are-misidentification, false acceptance, false rejection, privacy, dry, wet or dirty hands, hair growth, facial expression and aging.

1.2 Smart Cards

A Smart card[3] is a pocket sized plastic card which consists of a embedded microprocessor in it.A Smart card[4] contains 8 kilobytes of RAM, 346 kilobytes of ROM, 256 kilobytes of programmable ROM, and a 16-bit microprocessor.Smart card readers[5] are needed to access the contents of the smart cards present in them because card as acts as the interface between the smart cards and the information systems.Microprocessor based smart cards and Memory based smart cards exists.The microprocessor based smart cards will generally have greater storage memory capacity.So,the security to it should be as much of that. The memory-based smart cards are used for applications in which the function of the card is fixed.

Generally there are three types of smart cards.They are:

Contact Smart Cards--A contact smart card [5] must be inserted into a smart card reader with a direct connection to a conductive contact plate on the surface of the card. Transmission of commands, data, and card status takes place over these physical contact points.

Contactless Smart Cards--A contactless card [5] requires the close proximity to a reader. Both the reader and the card have antennae, and these two communicate using radio frequencies (RF) by this contactless link. Most contactless cards also derive power for the internal chip from this electromagnetic signal. The range is generally one-half to three inches for non-battery-powered cards,useful for applications like building entry and payment that require a very fast card interface.

Combinational Smart Cards--The combination smart cards are a combination of the contact smart cards and contactless smart cards. These cards can be read and written with contact or without contact with the reader.

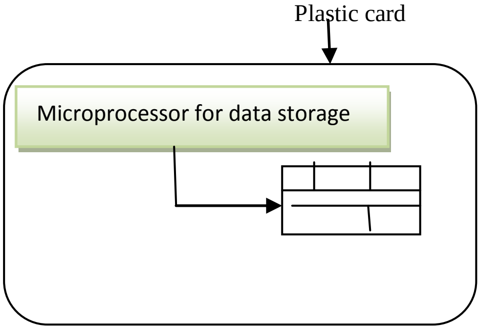


Fig 3: Overview of a Smart Card.

1.2.1 Smart Card Architecture

The smart card architecture can be explained by using Physical characteristics, Electrical characteristics and their components which are as follows.

- Physical Characteristics

A smart card is a piece of silicon in a piece of plastic.The manufacturing of smart cards consists of a silicon chip which is connected to a contact module and then the whole being assembled on a plastic card body.

- Electrical Characteristics

Electrical characteristics are defined by the standard ISO/IEC 7816-3 (electrical interface and transmission protocol).Basically, most smart cards uses the asynchronous serial transmission protocol. The electrical interface is of five contact parts: Vcc and GND (for power supply), Reset (for initialisation), Clock and I/O (serial interface).

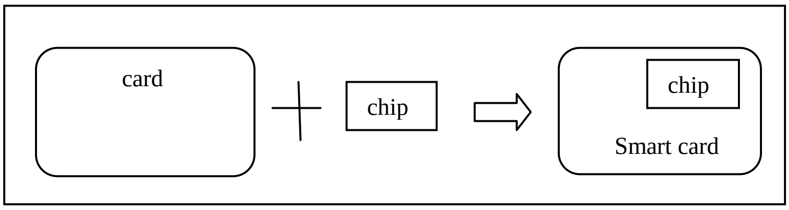


Fig 4: Smart Card Manufacturing

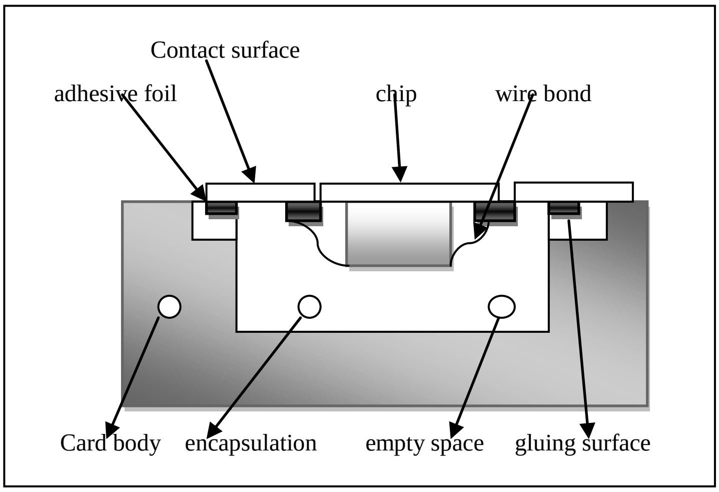


Fig 5: Smart Card Architecture Module

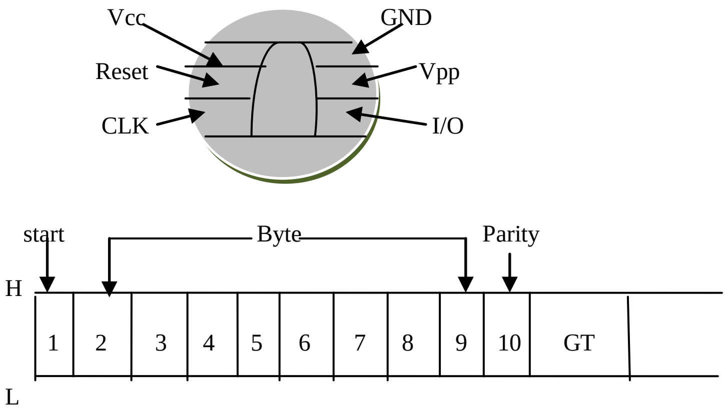


Fig 6: Smart Card Contacts Attribution and I/O Character

2.RELATED WORK

1.3 Common Attacks on Smart Cards

The best method for classifying the possible attacks on the smart cards is to categorize the attacks by the parties involved in the attack action.The different parties in the smart card based system are Cardholder, Dataowner, terminal, card issuer, card manufacturer, software manufacturer.

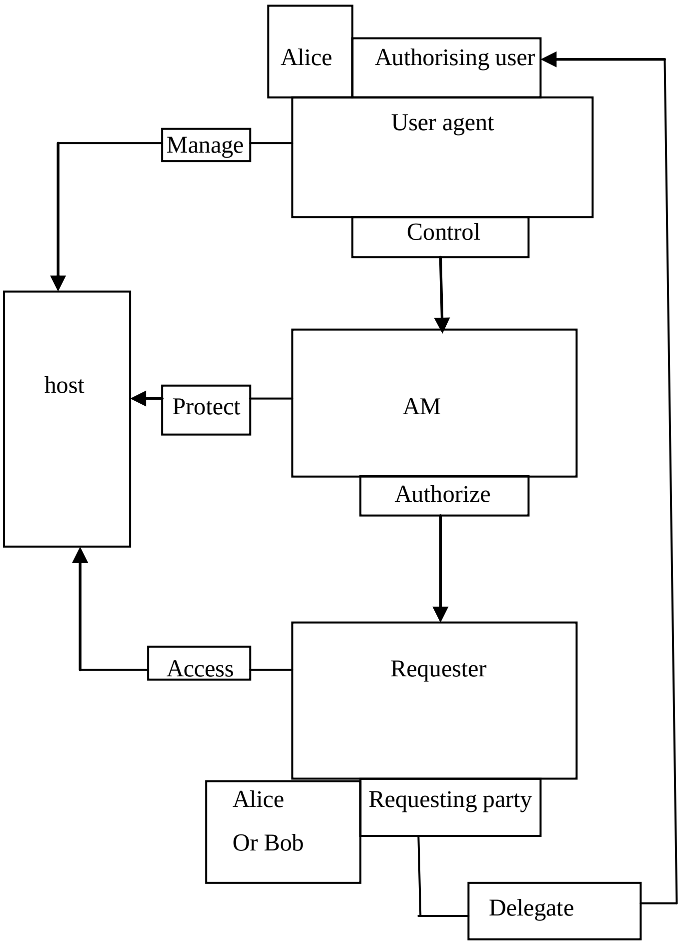
1.3.1 Classifying the Attackers

The possible attackers can be divided to following categories:

Class I (clever outsiders)--This type of attackers are intelligent but their knowledge is not sufficient.
Class II (knowledgeable insiders)--These attackers have some specialized technical education and experience.
Class III (funded organizations)--They are able to perform some in-depth analysis of the system and can design powerful attacks.

There may be different types of attacks on smart cards.Differential power analysis is a typical attack on the smart card.In this,the power consumed by the smart card is analysed to guess the internal behavior of the card.Side channel attacks,illeagal code attacks and fault induction attacks are certain types of attacks.

The authorization and trust model for the card[5] is as shown below



AM= Authorization Manager

Fig 7: Authorization and Trust Model

In order to convert the data, an encryption algorithm and a key are required. If the same key is used for both encryption and decryption then that key is called a secret key and the algorithm is called a symmetric algorithm

1.3.2 Algorithms of Data Security

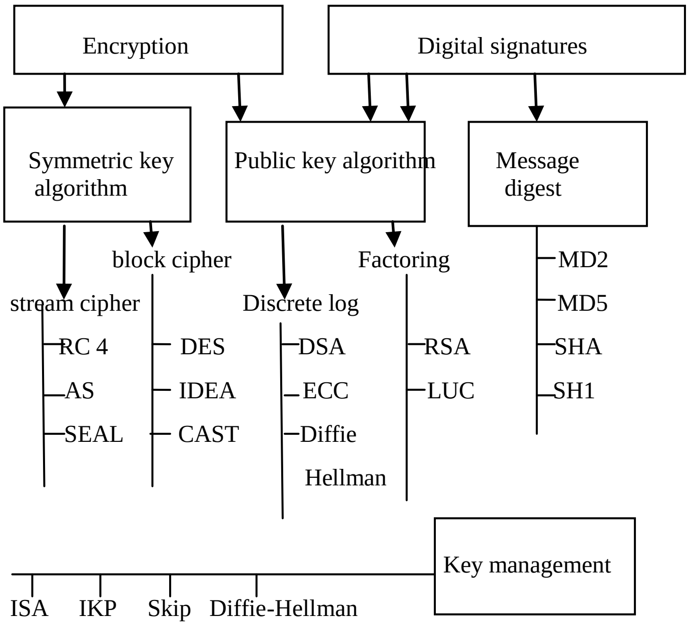


Fig 8: Classification of Data Security Mechanisms and Their Respective Algorithms

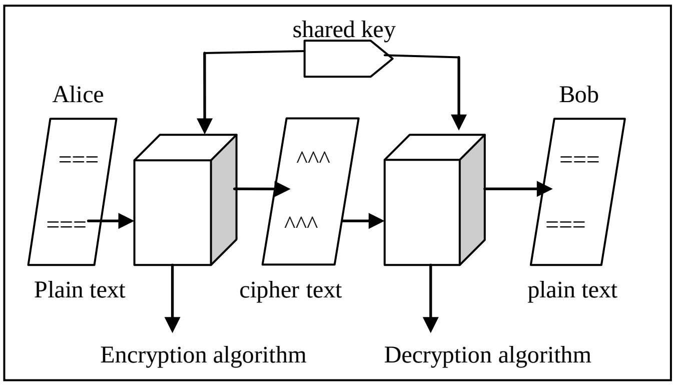


Fig 9: Symmetric Encryption

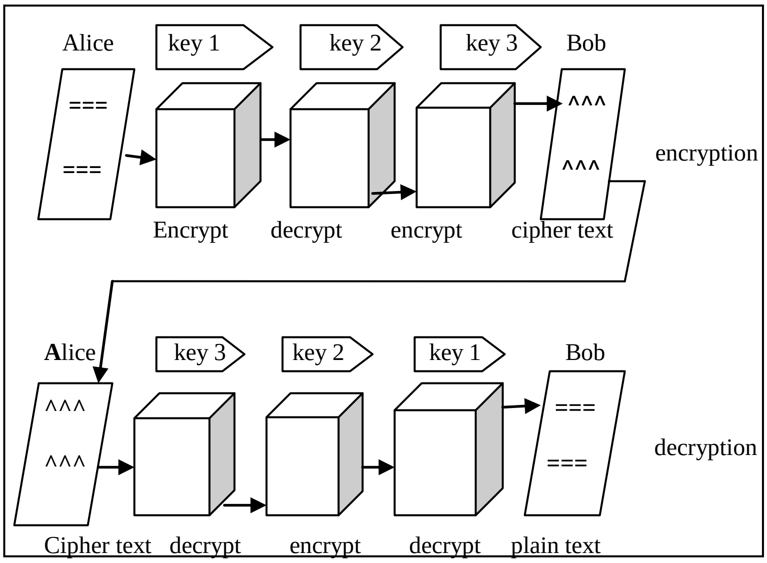
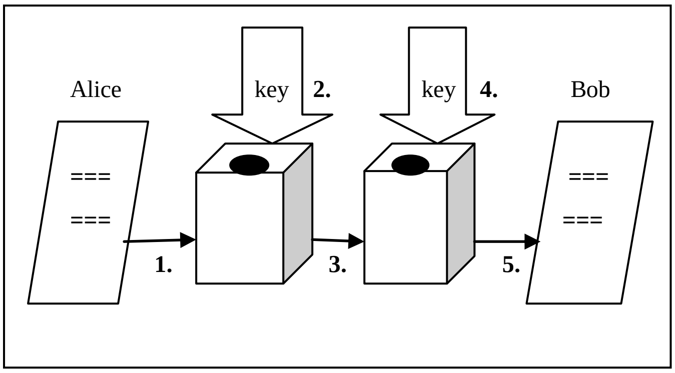


Fig 10: Symmetric Key(Triple DES) Encryption

If different keys are used for encryption and decryption, the algorithm is called an asymmetric algorithm.



1.Alice places a document in dual key strong box
2.Alice locks box with a public key
3.Box transported to Bob
4.Bob unlocks box with his private key
5.Bob retrieves the document.

Fig 11: Asymmetric (Public key) Encryption

1.4 Combining Biometrics with Smart Cards

Biometrics and smartcards[6] is considered to be a very useful combination of technologies. The security and convenience of biometrics increases the level of security in smart card applications. On the other hand, smartcards have a secure and portable way of storing biometric templates,otherwise they need to be stored in a central database. Among the various biometrics technologies available today, fingerprint recognition seems to be particularly suitable for smartcard systems.[7]

In general biometric authentication in smart cards is classified into three types:

- Template on Card (TOC)

In this type of cards,the fingerprint template is stored in the memory of the card itself.So,whenever the user's fingerprint template is captured,it will be sent to another system for authentication.

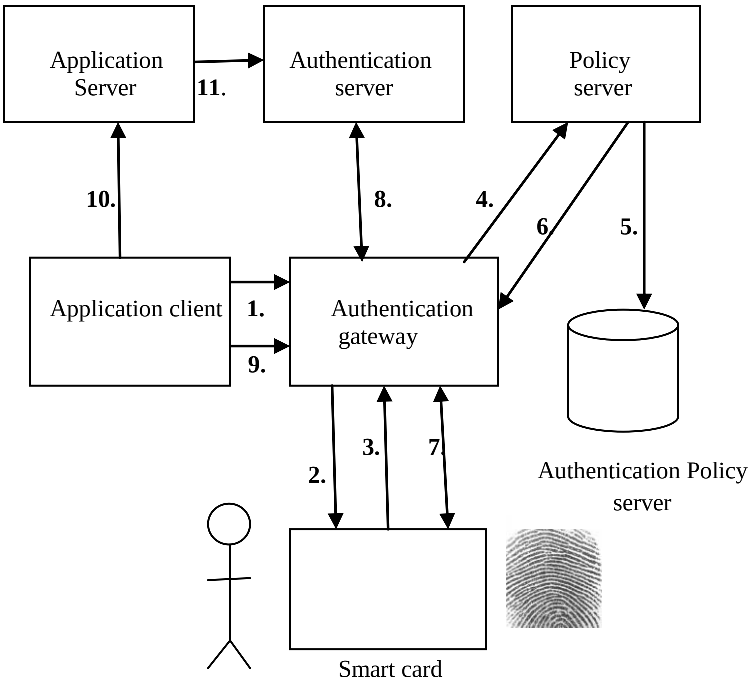
- Match on Card (MOC)

In MOC[8] also the biometric template is stored in the memory of the smart card.But,unlike in TOC,the authentication and matching process in the card itself.

- System on Card (SOC)

The SOC intermixes the technologies of both Template on Card(TOC),and Match on Card(MOC).Here also,the process of acquiring live template and authentication,matching process remains the same.

Client application requests an authentication from Authentication Gateway by sending Application Label (AL). Application Label is used for deciding authentication level. With AL, different security levels can be applied. Authentication gateway retrieves the information of the smart card and policy from the policy server. The authentication phase initiates by sending policy to smart card. Thereafter,a message is created at smart card side which is sent to authentication server.Authentication server performs the authentication and sends it back to the authentication gateway only if the sent message is valid. Authentication gateway returns this assertion to client so that the client can use it in login operation[9].



1.Authentication request
2.Card request
3.Card information
4.Card information+Application type
5.Policy retreival
6.Authentication policy
7.Authentication credentials
8.Protocol Messages
9.,10.Authentication assertion
11.Authentication validation

Fig 12: Architecture of Biometric Enabled Smart cards

When an application server receives this authentication assertion, it will send this assertion to the authentication server for validation.

1.4.1 Three-Factor Authentication

In today's digital world, three-factor authentication is not only helpful for security issues but also provides the ease of use to the user.Three-factor authentication can make the smart cards more securable[10]. For instance,giving two biometric templates such as fingerprint and face for an embedded application,and thereafter,entering the password to login a system can be a Three-factor authentication.There may exists another password for the application the user uses.In smart cards, PIN code, fingerprints and facial recognition is a three-factor authentication.But it cannot be a four-factor authentication.

1.4.2 The YesCard / NoCard Issue

The YesCard is a unauthorizedly modified smart card.In this smart card,a positive authentication reply will be obtained even in the case of the fake fingerprints received.This easily helps the intruders to attack the system by inserting his own biometric data.The NoCard is completely opposite to the YesCard.The NoCard is a smart card which has been unauthorizedly modified so that it always answer with a negative authentication, despite of the biometric data it receives. In this case,the access to the smart card is denied even to the authorized user.

The Match-On-Card has the unique feature of acquiring and storing the user's biometric template in the smart card's memory module.Only the authorized users will be acknowledged positively after performing internal authentication process. Here, the smart card takes the decision and does the authentication. The main argument against this MOC [11] are YesCard and NoCard.These are explained easily by the following protocols.

Let us assume the use of a secure block cipher E and a cryptographic key k to be shared between smart cards and the system. The challenge response protocol[12] is primarily used to show the decision made by the smart card.The verification of the candidate template T is done and if it is positively verified then smart card sends r=E_k(c).And if the T does not matches i.e., negatively verified,then smart card sends r=c.

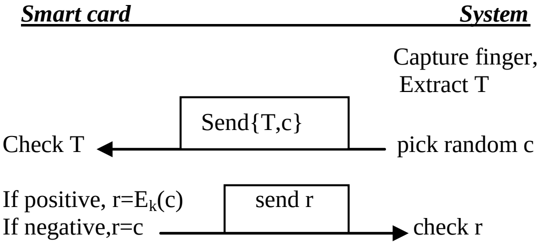


Fig 13: Protocol #1

The above protocol is useful for only the YesCard. So we will replace c by c_kb.This denotes the combination of c with a bit b. where b= 0 if negative authentication is done and b= 1 if positive authentication is done.Then the smart card will send r = E_k(c_kb). This protocol definitely protects from an unauthorized smart card whether it is a YesCard or a NoCard.

1.4.3 The Oracle Issue

An oracle is an algorithm in which we can give input as questions and can get output as answers.The oracle model is a powerful tool to provide the security for a system.Even though, a smart card can be used as an oracle by an unauthorized system to see a matching candidate T.

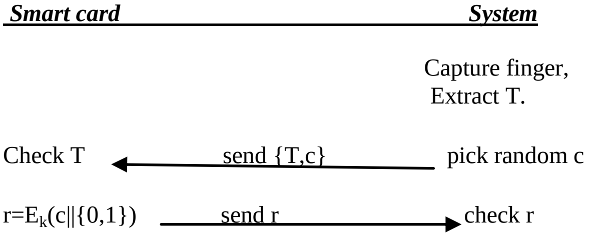


Fig 14: Protocol #2

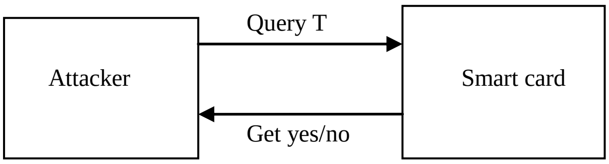


Fig 15: Smart Card as an Oracle

The protocol #2 could not protect the system from the attcker's access.An easy way to protect the smart card[13] from the unauthorized access is to encrypt the couple {T, c} by using a shared key k. This can protect the smart card from side-channel attacks.The concatenated bit cannot be known because all the other bits of the challenge c are no longer available.

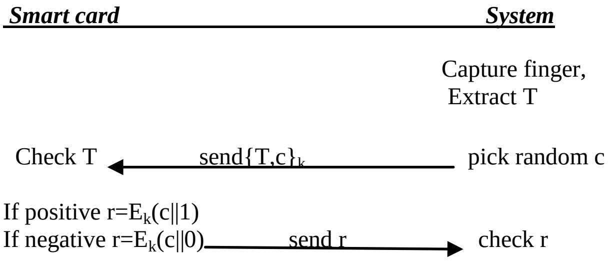


Fig 16: Protocol #3

3.EXPECTED RESULTS

By combining biometrics with the smart cards,the security is well enhanced.Also,we have introduced the problems faced in the YesCard and NoCard issues.The proposed protocol also helps to provide security in the biometric enabled smart cards.Hence,this protocol prevents the attackers from being smart cards used as an oracle to guess its biometric content.These biometric smart cards can be implemented in designing Auto Teller Machines(ATM).In ATMs,card owner will be recognized based on fingerprints.This system can be more secure as entire system is designed using embedded systems.

4.ACKNOWLEDGEMENTS

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The authors would like to thank K.L. University management for providing necessary facilities to carry out this work

5.REFERENCES

[1] http://searchsecurity.techtarget.com/definition/biometrics (19 March 2012).

[2] www.smartcardalliance.com (12 January 2012).

[3] R. Das, "Introduction To Smart Card", Bimaquest - Vol. Iv Issue I1, July 2004

[4] Bart Jacobs and Erik Poll, "Biometrics and Smart Cards in Identity Management" Radboud University Nijmegen,February 15,2010

[5] Claude Barrala, "Biometrics & Security: Combining Fingerprints, Smart Cards and Cryptography", 2010.

[6] "Xiong Li a, Jian-Wei Niu b, Jian Maa, Wen-Dong Wanga, Cheng-Lian Liu c, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards" Journal of Network and Computer Applications 34 (2011) 73–79.

[7] www.smartcardbasics.com (5 January 2012).

[8] Luca Bechelli, Stefano Bistarelli and Stefano Frassi, "A protocol for simulating Match-on-Card authentication through the use of Template-on-Card technology", 2003.

[9] De-song Wang, Jian-ping Li, "A Novel Mutual Authentication Scheme Based on Fingerprint Biometric and Nonce Using Smart Cards" International Journal of Security and Its Applications Vol. 5 No. 4, October, 2011.

[10] A Smart Card Alliance Physical Access Council White Paper, "Smart Cards and Biometrics" March 2011, Publication Number: PAC-11002.

[11] P. Grother "Performance of fingerprint match-on-card algorithms".Technical report, National Institute of Standards and Technology, 2008, 2009.

[12] Carmit, Hazayy, Yehuda, Lindelly "Constructions of Truly Practical Secure Protocols using Standard Smartcards"February 23, 2009.

[13] Sandeep Kumar Sood , "An Improved and Secure Smart Card Based Dynamic Identity Authentication Protocol" International Journal of Network Security, Vol.13, No.3, PP.208-215, Nov. 2011.