ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

SMARTCARD FRAUD DETECTION USING SECURE ONETIME RANDOM MOBILE PASSWORD

Ramesh Javvaji[1], Roopa Goje[2], Praveen Pappula[3]

Assistant professor, Computer Science & Engineering, SR Engineering College, Warangal, India[1]
Assistant professor, Computer Science & Engineering, SR Engineering College, Warangal, India[2]
Assistant professor, Computer Science & Engineering, SR Engineering College, Warangal, India[3]

Abstract— EMV is the dominant protocol used for smart card payments worldwide, with over 730 million cards in circulation. Known to bank customers as "Chip and PIN", it is used in Europe; EMV secures credit and debit card transactions by authenticating both the card and the customer presenting it through a combination of cryptographic authentication codes, digital signatures, and the entry of a PIN. In this paper we describe and demonstrate a protocol flaw which allows criminals to use a genuine card to make a payment without knowing the card's PIN, and to remain undetected even when the merchant has an online connection to the banking network. The fraudster performs a man-in-the-middle attack to trick the terminal into believing the PIN verified correctly, while telling the card that no PIN was entered at all. The paper considers how the flaws arose, why they remained unknown despite EMV's wide deployment for the best part of a decade, and how they might be fixed. Because we have found and validated a practical attack against the core functionality of EMV. This paper also provides the solution to detect the fraud, authentication to the genuine cardholder, transaction verification with a one time random mobile password.

Keywords: EMV, Card Fraud, ORMP, Chip and PIN

I. INTRODUCTION

Smart card is a credit card with some intelligence in the form of an embedded CPU. This card-computer can be programmed to perform tasks and store information, but the intelligence is limited – meaning that the smart card's power falls far short of a desktop computer. Smart credit cards operate in the same way as their magnetic counterparts, the only difference being that an electronic chip is embedded in the card. These smart chips add extra security to the card. Smart credit cards contain 32-kilobyte microprocessors, which is capable of generating 72 quadrillion or more possible encryption keys and thus making it practically impossible to fraudulently decode information in the chip. The smart chip has made credit cards a lot more secure; however, the technology is still being run alongside the magnetic strip technology due to a slow uptake of smart card reading terminals in the world market. Smart cards have evolved significantly over the past decade and offer several advantages compared to a general-purpose magnetic stripe card.
The advantages are listed below:

- Stores many times more information than a magnetic stripe card.
- Reliable and harder to tamper with than a magnetic stripe card.
- Performs multiple functions in a wide range of industries.
- Compatible with portable electronic devices such as phones and personal digital assistants (PDAs), and with PCs.
- Stores highly sensitive data such as signing or encryption keys in a highly secure manner
- Performs certain sensitive operations using signing or encryption keys in a secure fashion.

In EMV, customers authorize a credit or debit card transaction by inserting their card and entering a PIN into a point-of-sale terminal; the PIN is typically verified by the smart card chip, which is in turn authenticated to the terminal by a digital certificate. The transaction details are also authenticated by a cryptographic message authentication code (MAC), using a symmetric key shared between the payment card and the bank that issued the card to the customer (the issuer).

One goal of EMV was to externalize the costs of dispute from the issuing bank, in that if a disputed transaction has been authorized by a manuscript signature, it would be charged to the merchant, while if it had been authorized by a PIN then it would be charged to the customer. The net effect is that the banking industry, which was responsible for the design of the system, carries less liability for the fraud.

II. EXISTING TRANSACTION TYPES

There are two types of debit card transactions: PIN-based (online) and signature-based (off-line). Debit cards that

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

have a VISA or MasterCard logo on them can be processed without entering a PIN code. These types of transactions are referred to as "off-line" debit transactions. In this type of sale the merchant accepts a debit card the same way in which they would accept a normal credit card. The card is swiped through the terminal and the consumer signs the receipt. As far as the merchant is concerned there is no difference in the way a credit card or an off-line debit card is processed. Funds are transferred from the consumer's bank account just as in a PIN based ("on-line") debit transaction. However, the main disadvantage to the merchant is that the same discount fees charged to credit card transactions also apply to off-line debit transactions, significantly increasing the expense of processing.

- **PIN-based** - The cardholder's ATM, debit or check card, Personal Identification Number (PIN) and a magnetic-stripe reader are used at the point of sale to provide fast, efficient online debit transactions. The POS terminal dials for an authorization directly to the card issuer, and the cardholder's checking account is immediately debited for the transaction. Your customer receives a speedy and convenient payment choice, while you reap the rewards of immediate funding, a low transaction fee and chargeback protection.
- **Signature-based** - MasterCard and Visa-branded debit cards, often referred to as check cards, may be accepted at any credit card POS terminal. Unlike PIN-based debit transactions, signature-based purchases are debited to the cardholder's checking account within 2 to 3 business days rather than immediately. With signature-based debit, you'll pay a little more to process a transaction, eliminate the customer cash-back option and receive little protection against potential charge backs

III. TRANSACTION PROCESSING

Debit card payment method is convenient and secure, and it allows consumers to "pay as they go and track their spending of ready funds," But what really happens when a consumer makes a purchase with a debit card? What happen once card swipes?

Authorization: When someone swipes a debit card through a merchant's terminal, the terminal reads the magnetic strip on the back of the card and transmits the data to a card-processing network. Visa is a card-processing network as are MasterCard, Pulse, STAR Network, Interlink and Maestro.

The network ensures the pieces of transaction data are correctly formatted. Then, it performs a fraud analysis and forwards the information to the bank that issued the debit card. The issuer then validates that the card hasn't been reported as stolen or lost, confirms whether funds are available in the cardholder's account and then notifies the merchant, again through the network, whether the transaction has been approved."The vast majority of times, the issuer of the card will authorize the transaction, and it will go back through the process in the blink of an eye"

The transmitted data typically include the card number, transaction amount and date. The data will also include the merchant's name and location and a merchant category code, or MCC, that's used for rewards programs, among other purposes. If the consumer entered a personal identification number, or PIN, that would be encrypted and sent as well.

Clearing: At the end of the day or several times throughout the day, the merchant sends all the authorized transactions back to the network, which splits up and recompiles those transactions and then sends them back to the issuers. In turn, the issuers post the transactions to their customers' accounts.

Settlement: Finally, the network calculates how much money each issuer owes the network and how much money the network owes each merchant, Whyte says. Payment of the funds to the merchant can happen the same day as the swipe, or the next day, or within a few days.

IV. PROBLEMS IN EXISTING TRANSACTION PROCESSING

The 16-digit number on the front of the debit card is crucial to the process, the 16 digits are comprised of a six-digit bank identification number, or BIN, the customer's bank account number, and a so-called check digit that's generated by the Luhn test algorithm and is used to verify that the account number is legitimate. The back of the card contains the magnetic strip, or stripe, a security code and signature panel,

Signature or PIN?

Visa and MasterCard tend to process signature-based transactions, which typically use a so-called two-message process in which authorization and settlement are performed separately. The smaller networks usually handle PIN-based purchases, which occur via a single message that incorporates both authorization and settlement,

"Signature is a legacy technology, but it has broader acceptance,". "Merchants take MasterCard and Visa all around the world. PIN you'll find mostly at supermarkets, gas stations and major retailers".

The line between the two technologies is blurring now that some merchants accept debit card transactions where the card user doesn't have to sign or use a PIN. "Those used to be distinct, but now you have signature (transactions) that don't have any signature, and you're starting to see PIN transactions that don't have a PIN" "The preference for most merchants as well as cardholders is swipe and go. It's a fast way to pay."

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

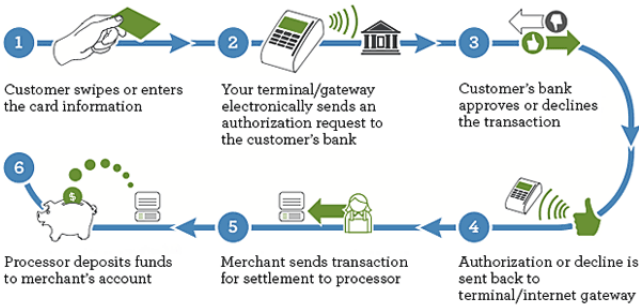


Figure 1: Debit card transaction process with swipe

When a consumer makes a purchase with a debit card "pay as they go and track their spending of ready funds", the way above figure shows.

When a customer uses the debit card for their purchase with an above procedures there is real scope for the fraud to make loss to the customer and transfer funds from his account within short period. There are few problems with an existing card transaction type 1) PIN based 2) Signature based.

1. Physical Theft
2. PIN and Card number theft.
3. Identity theft.

Physical Theft:

One of the most obvious types of debit card fraud is when someone steals the debit card itself, either by stealing a wallet, not reporting a lost card they find or removing a card from an unattended purse, briefcase or ATM. In this case fraud can use the signature based type of transaction and he succeeds without entering a pin number.

PIN and Card Number Theft:

Another form of debit card fraud is theft of the cardholder's PIN and card number. This can occur in several different ways. Thieves can use cameras, or their own eyes, to watch users enter a PIN at an ATM or store checkout counter.

They can also commit debit card fraud by "skimming," which involves using equipment to capture the magnetic tape, keypad information, or internal memory of an ATM, gas pump or other payment device. In this case fraud can use the Pin based type of transaction and he succeeds with a dummy pin number.

Identity Theft:

Identity theft can include an extreme form of debit card theft, when the thief attempts to impersonate the cardholder using personal information she has managed to obtain, such as a birth date or social security number.

With this information the thief may be allowed to get the debit card number and withdraw cash from the cardholder's account or purchase merchandise which can then be sold for cash or kept.

V. PROTOCOL WORKING PRINCIPLE

A bank that issues EMV cards selects a subset of the EMV protocols, choosing for instance between digital signature methods, selecting a MAC algorithm, and deciding on hundreds of customizable options regarding authentication and risk management. Their selection must comply with card scheme rules as well as the EMV framework. Meanwhile merchants and acquiring banks (who receive payments on behalf of merchants) simply procure EMV-compliant hardware and software and connect it to the payment networks (operated by card schemes). In particular, the attack we introduce in this paper results both from a protocol failure of the EMV framework, and a failure of the proprietary MAC protocols that are used by issuing banks (and approved by the card schemes).
As Figure shows in detail, the EMV protocol can be split into three phases:

1. **Card authentication**: Assures the terminal which bank issued the card, and that the card data have not been altered
2. **Cardholder verification**: Assures the terminal that the PIN entered by the customer matches the one for this card
3. **Transaction authorization**: Assures the terminal that the bank which issued the card authorizes the transaction

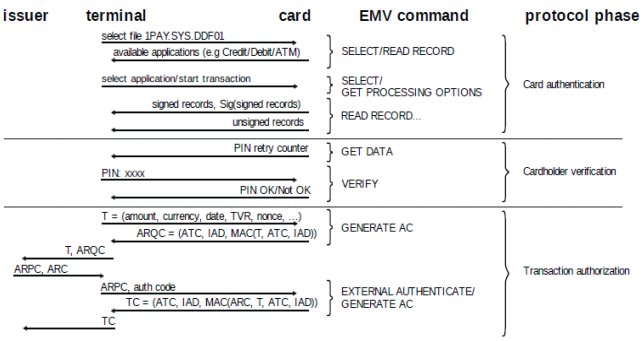


Figure 2. A complete run of a Chip and PIN protocol.

Card authentication: EMV smart cards may contain multiple separate applications with different cryptographic keys, such as a debit or credit card for use at shops, ATM functionality, and MasterCard Chip Authentication Programme (CAP) applications for online banking. Thus when a card is inserted into a point of sale terminal, the terminal first requests a list of supported applications (by reading the file "1PAY.SYS.DDF01") and selects one of them. The actual transaction is then initiated by sending the Get Processing Options command to the card.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

Next, the terminal reads cardholder information from the card by sending a Read Record command with the appropriate file identifiers. These records include card details (e.g. primary account number, start and expiry date), backwards compatibility data (e.g. a copy of the magnetic strip), and control parameters for the protocol (e.g. the cardholder verification method list, and card data object lists, which will be discussed later).

The records also include an RSA digital signature over a subset of the records, together with a certificate chain linking the signing key to a card scheme root key known to the terminal. In one variant of EMV, known as SDA (static data authentication), the card itself is not capable of performing RSA operations, so it can only present the terminal with a static certificate. Cards employing the DDA (dynamic data authentication) variant additionally contain RSA private keys which are used to sign a nonce sent by the terminal and whose corresponding public keys are authenticated by the certificate chain.

Cardholder verification*:* The cardholder verification step starts with a mechanism negotiation, performed between the card and the terminal, to establish what cardholder authentication method they can (or must) use. This is driven by a data element called the cardholder verification method (CVM) list. The CVM list states the card's policy on when to use a PIN, or a signature, or nothing at all, to authenticate the cardholder.

The vast majority of transactions are 'PIN verified', which means the customer enters the PIN on a PIN entry device. The PIN is sent to the card, and the card compares it to the PIN it stores. If they match, the card returns 0x9000, and if it fails the card returns 0x63C*x*, where *x* is the number of further PIN verification attempts the card will permit before locking up. Note that the card's response is not directly authenticated

Transaction authorization: In the third step, the terminal asks the card to generate a cryptographic MAC over the transaction details, to be sent to the issuing bank. The terminal calls the **Generate AC** command, to request an **ARQC** (authorization request cryptogram) from the card. The payload of this command is a description of the transaction, created by concatenating data elements specified by the card in the **CDOL 1** (card data object list 1). Typically this includes details like the transaction amount, currency, type, a nonce generated by the terminal, and the TVR (terminal verification results), which will be discussed later.

The cryptogram sent to the bank includes a type code, a sequence counter identifying the transaction (ATC – application transaction counter), a variable length field containing data generated by the card (IAD – issuer application data), and a message authentication code (MAC), which is calculated over the rest of the message including a description of the transaction. The MAC is computed, typically using 3DES, with a symmetric key shared between the card and the issuing bank.

If the card permits the transaction, it returns an ARQC; otherwise, it returns an AAC (application authentication cryptogram) which aborts the transaction. The ARQC is then sent by the terminal to the issuing bank, via the acquirer and payment network. The issuer will then perform various cryptographic, anti-fraud and financial checks: such as whether the card has been listed as stolen, whether there are adequate funds, and whether the risk analysis algorithm considers the transaction acceptable. If the checks pass, the issuer returns a two byte ARC (authorization response code), indicating how the transaction should proceed, and the ARPC (authorization response cryptogram), which is typically a MAC over ARQC + ARC. Both items are forwarded by the terminal to the card with the **External Authenticate command**.

The card validates the MAC contained within the ARPC, and if successful updates its internal state to note that the issuer authorized the transaction. The terminal then calls **Generate AC** again, but now using the CDOL 2, requesting that the card issues a TC (transaction certificate) cryptogram, signifying that it is authorizing the transaction to proceed. Finally, the terminal sends the TC to the issuer, and stores a copy in its own records in case there is a dispute. At this point it will typically print a receipt, which may contain the legend 'Verified by PIN' if the response to Verify indicated success. One copy of the receipt is given to the cardholder and a second copy is retained. We have also seen different receipts with 'confirmed' for the cardholder and 'PIN verified' on the merchant copy (perhaps to assure the merchant that the liability for disputes is no longer on them).

VI. THE ATTACK

The central flaw in the protocol is that the PIN verification step is never explicitly authenticated. Whilst the authenticated data sent to the bank contains two fields which incorporate information about the result of the cardholder verification – the Terminal Verification Results (TVR) and the Issuer Application Data (IAD), they do not together provide an unambiguous encoding of the events which took place during the protocol run. The TVR mainly enumerates various possible failure conditions for the authentication, and in the event of success does not indicate *which particular method was used* (see Table I).

Table I
TERMINAL VERIFICATION RESULTS (TVR) BYTE 3
.

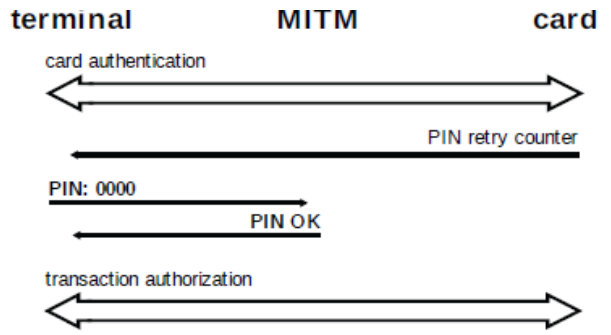
Bit	Meaning when bit is set
8	Cardholder verification was not successful
7	Unrecognized CVM
6	PIN Try Limit exceeded
5	PIN entry required and PIN pad not present or not working

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

4 PIN entry required, PIN pad present, but PIN was not entered
3 Online PIN entered
2 Reserved for future use
1 Reserved for future use

Therefore a man-in-the-middle device, which can intercept and modify the communications between card and terminal, can trick the terminal into believing that PIN verification succeeded by responding with 0x9000 to Verify, without actually sending the PIN to the card. A dummy PIN must be entered, but the attack allows any PIN to be accepted. The card will then believe that the terminal did not support PIN verification, and has either skipped cardholder verification or used a signature instead. Because the dummy PIN never gets to the card, the PIN retry counter is not altered. The modified protocol flow is shown in Figure 2.



'igure 3. The man-in-the-middle suppresses the PIN Verify command to he card, and tells the terminal that the PIN has been verified correctly. A omplete transaction is detailed in Appendix A.

Neither the card nor terminal will spot this subterfuge because the cardholder verification byte of the TVR is only set if PIN verification has been attempted *and* failed. The terminal believes that PIN verification succeeded (and so generates a zero byte), and the card believes it was not attempted (so will accept the zero byte).

VII. THE PROPOSED SOLUTION

When a customer uses the debit card for their purchase, now you have signature (transactions) that don't have any signature, and you're starting to see PIN transactions that don't have a PIN" "The preference for most merchants as well as cardholders is swipe and go. It's a fast way to pay."

Signature Based Transaction

If the customer uses the debit card for their purchase with a signature based transaction, the scenario is follows

1. When someone swipes a debit card through a merchant's terminal, the terminal reads the magnetic strip on the back of the card and transmits the data to a card-processing network. Visa is a card-processing network as are MasterCard, Pulse, STAR Network, Interlink and Maestro.
2. The network ensures the pieces of transaction data are correctly formatted. Then, it performs a fraud analysis and forwards the information to the bank that issued the debit card.
3. The issuer then validates that the card hasn't been reported as stolen or lost, confirms whether funds are available in the cardholder's account and then notifies the merchant,
4. Once the debit card is authorized, then bank generates ORMP (Onetime Random Mobile Password) for that particular transaction, sends it to genuine customers mobile.
5. ORMP is 4digit random number which is valid for the particular transaction only, if the customer enters wrongly then automatically transaction it terminated.
6. Whenever customer receives ORMP in their mobile, then immediately customer need to enter that random password in the specified swipe keypad of merchant terminal.
7. Then secure ORMP information is forwarded from merchant terminal to bank for the verification of cardholder Random password and transaction details.
8. If random password is matched with bank transaction random password, then remaining transaction payment process continues.

With a transaction ORMP we can identifies the fraud, suppose our debit card is stolen by someone. With that debit card the fraud can do purchase some goods with a signature based transaction. Fraud can swipes the card at merchant terminal then automatically terminal reads the card information, and then networks forwards that piece of information to bank for authorization of the cardholder. At this point, Bank verifies the card details and merchant details, also funds available in that account. "If that card is valid then bank generates secure Onetime Random Mobile Password for that particular transaction, sends it to cardholders mobile number for the transaction security purpose". Automatically cardholder gets message from bank of secure 4digit ORMP. Then customer realizes that his card is loosed.

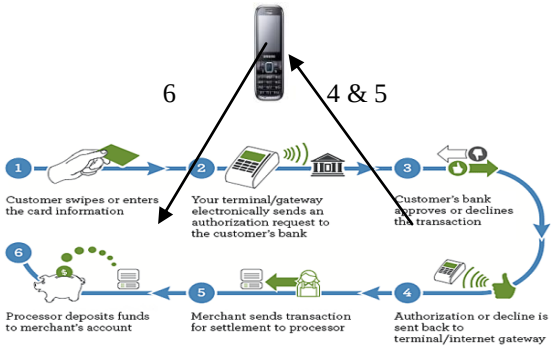


Figure 4: Debit card payment transaction with Secure ORMP technique

Where 4---Bank verifies Card details, amount, and merchant network.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

5----Bank generates 4 digit alpha numeric secure transactions ORMP and sends it to cardholder mobile number.

ORMP= E (TID, Card_NO, BID, MID, T1, Nonce)

6----Cardholder enters the 4digit alpha numeric secure ORMP at merchant swipe keypad.

PIN based Transaction

If the customer uses the debit card for their purchase with a PIN based transaction, the scenario is follows

1. When someone swipes a debit card through a merchant's terminal, the terminal reads the magnetic strip on the back of the card and transmits the data to a card-processing network. Visa is a card-processing network as are MasterCard, Pulse, STAR Network, Interlink and Maestro.
2. Cardholder enters their secrete PIN number at merchant swipe keypad for card authorization
3. The network ensures the pieces of transaction data are correctly formatted. Then, it performs a fraud analysis and forwards the information to the bank that issued the debit card.
4. The issuer then validates that the card hasn't been reported as stolen or lost, confirms whether funds are available in the cardholder's account and then notifies the merchant,
5. Once the debit card is authorized, then bank generates ORMP (Onetime Random Mobile Password) for that particular transaction, sends it to genuine customers mobile.
6. ORMP is 4digit random number which is valid for the particular transaction only, if the customer enters wrongly then automatically transaction it terminated.
7. Whenever customer receives ORMP in their mobile, then immediately customer need to enter that random password in the specified swipe keypad of merchant terminal.
8. Then secure ORMP information is forwarded from merchant terminal to bank for the verification of cardholder Random password and transaction details.
9. If random password is matched with bank transaction random password, then remaining transaction payment process continues.

Bank generates secure transaction ORMP with following elements

ORMP= E (TID, Card_NO, BID, PIN, T1, Nonce)

With the above secure ORMP we can detect the "card and number theft" type of fraud. Suppose a fraud do the skimming trick to enter dummy password for validation purpose. Then bank verifies those details and generate secure ORMP transaction and sends it to genuine cardholder's mobile number.

VIII. CONCLUSION

In this paper we shown the use of the Smart card in various purpose, and what are the crucial things that debit/credit card contains. We also focused EMV protocol and its working principle.

Paper also discussed various transaction types and its transaction processing. We mainly stressed the importance of ORMP secure transaction in both signatures based and PIN based transaction. And how bank generates secure ORMP.

Finally this secure 4digit alpha numerical ORMP for particular transaction is helped to prevent the smart card frauding.

ACKNOWLEDGMENT

We thank the Steven J Murdoch, Rose Anderson for their Past contribution. We also thank the card holders and merchant for their support. We thank the friends and supporters for their valuable encouragement and suggestion.

REFERENCES

[1] EMV – Integrated Circuit Card Specifications for Payment Systems, Book 1: Application Independent ICC to Terminal Interface Requirements, Version 4.2 ed., EMVCo, LLC, June 2008.
[2] EMV – Integrated Circuit Card Specifications for Payment Systems, Book 2: Security and Key Management, Version 4.2 ed., EMVCo, LLC, June 2008.
[3] EMV – Integrated Circuit Card Specifications for Payment Systems, Book 3: Application Specification, Version 4.2 ed. EMVCo, LLC, June 2008.
[4] EMV – Integrated Circuit Card Specifications for Payment Systems, Book 4: Cardholder, Attendant, and Acquirer Interface Requirements, Version 4.2 ed., EMVCo, LLC, June 2008.
[5] Understanding credit card frauds, Tejpul Bhatla, vikram prabhu June 2003.
[6] Secure mechanism for credit card transaction fraud detection system, Alka Herenj, susmita mishra. IEEE 2013.
[7] VISA & MasterCard, SET Secure Electronic Transaction Specification, 1997.
[8] T. Dierks and C. Allen, "The TLS protocol," IETF, RFC 2246, January 1999

BIOGRAPHIES

Ramesh Javvaji completed M.Tech CSE in the year 2009. Presently working as a Assistant Professor in the dept. of CSE, SR Engineering College, Wgl, India. His research interests include Network security (Authentication), Cryptography, database management Systems. He has served on a number of committees of technical conferences and workshops including CISCO, ITFRP09, and VCON10.He reviewed 3 books of Pearson publication like Advanced Database management, Programming with C++, Operating systems.