# ANALYSIS OF SECURITY REQUIREMENTS OF FUTURISTIC MOBILE APPLICATIONS

Pranav Vyas[1] and Bhushan Trivedi[2]

[1]Smt. Chandaben Mohanbhai Patel Institute of Computer Applications, Charotar University of Science & Technology, Changa, Gujarat, India
[2]GLS Institute of Computer Technology, GLS University, Ahmedabad, Gujarat, India

***ABSTRACT***

*Advent of smart phones has brought with it revolution in mobile applications that are available for everyday functions. In this paper we review security requirements for apps from different domains that are communicating sensitive information over insecure network. Some of these apps are already available and some are expected to be introduced in future. We find that there are many parameters that affect security of apps but some are prominent compared to others based on domain of the app. Based on analysis of security requirements we determine the application domain most suitable for implementation of our proposed protocol.*

***KEYWORDS***

***Security, Mobile Security, Mobile Payment, E-Health Care, E-Voting***

## 1. INTRODUCTION

Today, there are various applications that require secure connection for communication over the unsecured network. Key exchange protocols play an important part in this scenario by providing secure technique to exchange the secret key between various parties involved in communication. Although the core requirements from key exchange protocols remains same for all the applications that seek to have secure connection, there are many application specific requirements. These requirements are expected to be fulfilled by key exchange protocol when it is being implemented for particular system.

The origin of these requirements comes from multiple sources. Some of these requirements are traced back to application usage environment, for example, user using application from a desktop computer will have different requirements then user using the same application from his/her smart phone. Some other requirements can be attributed to user's proficiency with computer systems in general or user's expertise in application domain, for example ecommerce systems have different requirements then an online exam or cloud based document sharing systems or domain specific systems such as power grid management system or automated systems used in nuclear reactors to maintain temperature.

The aim of this paper is find out application specific requirements from 3 mobile based applications where our proposed key exchange protocol can be applied: Payment solutions [1], E-Voting systems and E-Healthcare record management systems. These systems have been selected for study as they have been recently introduced [2] or have huge potential to grow in India [3] [4] [5].
Generally there are two types of security requirements: Functional and Non-functional. When we view the functional requirements of the above mentioned systems they seem to be based on the

constitution and laws prevailing in host country. Due to this reason, it is possible that even if the system used is same, some requirements in functional domain will change based on where it is being used. Non-functional requirements on the other hand will remain same as they form core of the system's security requirements. Therefore in this paper we will limit our discussion only to non-functional requirements.

In this paper we try to analyze security requirements posed by these systems. As these systems operate in distinct domains, environment and platforms their applications and functionality vary from each other. The requirements in terms of security from these applications are completely unique. We try to compare these requirements with our proposed protocol in order to determine how effective our protocol fares in providing security to these systems based on different requirements and parameters.

This paper is divided into 6 sections. Section 1 introduces subject of the paper, section 2 deals with information security requirements in E-Commerce systems. Section 3 contains detail security requirements on electronic voting (E-Voting) systems. Section 4 describes security requirements for E-Healthcare systems. In section 5 we check our proposed protocol against security requirements of the systems discussed in previous sections. In section 6 we present our

conclusion of comparison and determine most suitable application for our proposed protocol.

# 2. E-VOTING SYSTEM SECURITY REQUIREMENTS

In this section we will have a brief introduction to the concept of E-voting. We will discuss various security related requirements for generic E-voting system.

An election is regarded as tool to expand and solidify democratic procedure. Putting E-voting in practice can lessen the cost and burden of election administration from authorities. Using E-voting can result in effective and efficient voting process; it can also be especially attractive to vote for young persons and persons with disabilities [1].

According to a report by Internet Policy Institute on E-voting [2] there are number of different criteria for designing voting system. However they can broadly categorized into 3 types: Legal, Technical and User requirements criteria. The scope of this discussion shall be limited to security criteria subsection under technical criteria of system.

Following security related criteria are mentioned in [2]: Authentication, Uniqueness, Integrity, Verifiability, Audit ability, Reliability and Secrecy.

## 2.1. Authentication

Authentication is first step in process of E-voting where user has to identify him/her self to the system. The literature suggests many different ways for users to authenticate themselves to system. There are many methods provided by different authors ranging from assigning digital signatures to users to identify themselves [3] to taking a picture of user from mobile phone before voting and using image processing software to compare it with original picture stored in database of government [4].

## 2.2. Uniqueness

Uniqueness in system implies that a voter should be able to be identified uniquely. The system should only allow users to vote once. It implies that once the user has voted, system should have a technique in place to detect duplicate votes being casted. The techniques to establish uniqueness ranges from assignment of unique digital signature that expires after casting one's vote [5] to possible assignment of nonce or signature assigned and issued by distributor [6].

### 2.3. Integrity

Integrity refers to oneness of message. In case of E-voting system it refers to un-modifiability of votes. Once user has casted the vote the system should put a mechanism in place so that votes are not modified without alerting system administrators. It is possible to do this by encrypting vote information. Some researchers [7] also suggest allocating user a unique receipt number and combining receipt number with a encrypted ballot will let user check for his/her vote and see if it has been manipulated or not.

### 2.4. Verifiability

Verifiability refers to accountability of the votes given by users. The system should have a way to associate user with his/her vote such that user is able to check his/her vote. According to [7] it is possible to provide this functionality by allocating each user a e-receipt number automatically generated when user casts his/her vote by system. The system should have functionality to be able to combine user provided e-receipt number with private key for ballot which results in private key of user's encrypted ballot. Using this private user is able to check his/her vote.

### 2.5. Auditability

Auditability refers system's ability to be reliable and demonstrate authentic election records.

The system should have a feature to allow verification of ballots and votes before the votes are viewed or counted and information regarding voting made public.

### 2.6. Reliability

Reliability refers to ability of system's ability to continue to work despite of repeated failures.

For increasing reliability of the system Dimitris [8] suggest to decrypt and count votes from ballots only after proper auditing procedures are followed. Also voting control and recount should be feasible by system while anonymity of voters is maintained [9] [10].

### 2.6. Secrecy

Secrecy of system means that no one other then user should be able to determine how he/she has voted. That is only user is able to see his/her vote. It is possible to provide feature as demonstrated in [7] by using combination of an automatically generated receipt number with a unique ballot number assigned to user. However according to Vollan [11] it is not possible to provide complete security when casting vote over internet or any such public network.

## 3. E-HEALTHCARE MANAGEMENT SYSTEM SECURITY REQUIREMENTS

In this section we discuss system security requirements of generic E-Health care record system. A traditional health care system is paper based system that can result in thick file with hundreds of pages of report on patient's health history. The interest in moving from traditional system to an e-health care system stems from several reasons according to [1] some of them include lower maintenance cost, increased quality of data, easy record keeping and mobility of data. However EHR need to satisfy certain conditions in order to meet certain requirements [2] regarding data such as failure resistance, high availability, and consistent security policy. Technological breakthroughs and advances in communication technology has slowed advance of EHR system with numerous security and privacy issues [3].

An EHR of patient may be stored on central server in fragmented form. Also data may be accessible from several sites from where patient has received treatment. It is entirely possible that these different places have different rules and follow different guidelines for security of EHR. Therefore data should be protected from manipulation, unauthorized access and abuse.

With above discussion in mind, following requirements can be derived Privacy, Trustworthiness, Authentication and Responsibility [4] [5] [6].

### 3.1. Privacy

Patient's privacy can be maintained by hiding patient's identity when sharing his/her data across hospitals, clinics and research centers. This goal can be accomplished by using pseudo anonymity techniques. There are various references in literature where access to third party is given without disclosing patient's personal data. For example, a hash is shown instead of patient name to identify patient uniquely [7] [8] [9].

### 3.2. Trustworthiness

Trust factor here deals with how much users trust system and administrators to keep their data from being used for malicious purpose. According to a report [10] there are 25 million compelled authorizations for health record discloser in USA. Citizens are also getting more aware of perils of compromised health care records. In Austria, citizens have right to decide if their health information should be shared with other institutes and health care professionals or not [11]. To address these concerns a system must comply with standards set by various government organizations that offers reorganization to system through certifications by extensively and rigorously checking security aspects of system. One such example is Certification Commission for Healthcare Information Technology (CCHIT) in USA [12].

### 3.3. Authentication

Authentication in EHRMS principally means that for all data that is stored or retrieved the address from where it is stored or retrieved must be stored and all information must be authenticated. This can be done design of two-level trust based protocol. For this system to work all the machines will be in a common web of trust. Level one will address challenges of trust arising in accessing data. Level two will address challenges arising from insertion and updating of information.

### 3.4. Responsibility

It is responsibility of EHRMS to provide secure access to data. To prevent malicious users from using data even when they have access to it, data should be encrypted when stored. To increase security data as well as keys, identifiers and metadata are also encrypted [7] [8]. Also communication between systems located remotely need to be encrypted to prevent malicious users from eavesdropping. This can be done by using SSL [10] or TLS [9] or some customized security protocol [11]. Authors also suggest a cloud based encryption technique to ensure that cloud provider cannot see EHR data [12].

## 4. MOBILE APPLICATION BASED PAYMENT SYSTEM

Mobile payment can be defined as an activity with two participants where one participant exchange financial value in exchange of product or service by other participant. If we compare payment on mobile devices with traditional e-commerce web applications on internet, we find that maintaining security and privacy in mobile devices is particularly difficult due to difference in their under laying technologies.

Making payment for services or product bought over internet through mobile version of applications is one example where user shares information such as credit card number or bank account number through application. Such transactions need to be protected by encrypting information when information is transferred so as to prevent misuse of information.

We can derive following requirements for mobile based payment system.

## 4.1. Authentication

Authentication can broadly be defined as a process of confirming that the user/machine is who he/it claims to be and no one else. Authentication can be done with single attribute or single piece of data. Here authentication should not be confused with identification as both have different goals and outcomes in the end. However we can say that authentication is technique for confirming identity.

In their article Needham and Schroeder suggests techniques such as public key cryptography and digital signatures [3].

Public key cryptography requires a third party that should be trusted by both sender and receiver of the message. However sender and receiver have no way of determining if the third party that they trust and share their keys with is compromised or not.

Also a relatively new concept in authentication is digital certificates. Digital certificates are certificates which are provided by certification authorities to a person or entity. A digital certificate is public key of person or entity which is signed by certification authority for authenticity. It can be used public key infrastructure [4]. Here, it is possible to verify digital signature with signature of certification authority. If it is matched it is assured that public key of certificate belongs to the person or entity whose name is present on certificate [5]. However processing certificate can strain processor and other resources

Digital signature can ensure authentic transaction parties, integrity and non-repudiation of the message. Documents can be digitally signed by author to make them authentic. Once signed the documents cannot be altered. Sometimes instead of encrypting the document which may take long time based on size, one way hash function is used. At the time of authentication hash is reproduced from received message and is compared with hash deciphered from message [4]. However problem with this technique is even if the signature is verified correctly, it is not possible to know that the person who has signed the document is the same person whose digital signature is used to encrypt the document thus complete trust is not possible.

## 4.2. Confidentiality

Confidentiality is in keeping some information not accessible from some users. It can be said that confidentiality is about trusting the system that not all the information will be accessible to all the users. Some information that may be private or confidential in nature will only be accessible to a select group of user(s). The system will determine if the user is allowed to access information based on access level and privileges of user defined by system administrator. The importance of confidentiality is even more in wireless network as they are said to be much more vulnerable [6].

Confidentiality of securely transmitting information over insecure networks can be achieved by encrypting information that is confidential. There are two ways one of which can be used to encrypt information. In symmetric key cryptography there are at least 2 parties involved. The sender encrypts information using one of the keys readily available with him/her. All keys of the given set are mathematically related to each other so, it is easy to get the other key by following certain pattern generation algorithm if you have one of the keys. Another type of technique is asymmetric key cryptography.

This concept was first introduced by Diffie-Hellman in their paper in 1976 [7]. In this technique there are at least 3 parties required for communication to happen, a sender, receiver and a trusted third party whom both sender and receiver trust. This technique works on principle of public key and private key. A public key is openly known and can be used to encrypt information but that information can only be decrypted by private key which is only known by the intended recipient of the message to whom public key belongs.

Even though considered slower and more resource consuming then symmetric key cryptography technique, asymmetric key cryptography technique is considered more secure and suitable for exchanging information securely over internet due to public key infrastructure that it uses [8].

### 4.3. Integrity

Integrity of information is in making sure that information does not get altered while being transmitted over insecure network. The integrity of information can be lost if they are accidently modified due to an error on part of user or system or modified and framed with malicious intent.

While it is not possible to prevent accidental modification to information that may result in loss of integrity by user or system, it is certainly possible that modification to the information with malicious intent can be prevented by maintaining proper access level to user and encrypting information that is susceptible to such modifications. However such measures are not adequate to maintain integrity of the information and we must look towards other mechanisms to achieve integrity [9].

One prominent technique that has been designed to maintain integrity of information is message digest. Message digests can be thought of as one way function that can be applied on variable length strings that returns fixed length hash as output. However guarantee of integrity comes with requirements of extra processing of generating hash from given information, which can result in strain on resources in mobile environment where the resources are limited.

### 4.4 Non-Repudiation

Non-repudiation is concept about assuring origin of data so that sender or receiver can be protected from false claims of either not being able to receive data or sending data. It provides means to prevent either side from unilateral modification of information to suit their needs and thus protect other side.

Providing non-repudiation is a key factor to a secure online transaction [10]. It should ensure that involvement of concerned parties in an online involvement of payment is not denied later.

Non-repudiation can be achieved with help of digital signatures. If a message received is signed by one of the parties involved in communication it can guarantee that that party was part of transaction that has been conducted. However this is only a part of solution. The other part of solution is using message digests to maintain integrity of message so that in case of dispute both the parties can use these to prove their point.

## 5. COMPARISION

In this section we will check to see which of the characteristics of various systems discussed in previous section is supported by our protocol [1]. Here, we will do a system wise comparison of characteristics (refer table 1, table 2 and table 3)and check which of the required characteristics are supported by our protocol in order to determine which application is most suitable for our protocol [1].

## 5.1 E-Voting System

In our protocol we use a trusted third party. We also used combination of public and private keys. The receiver's private key is only known to trusted third party and receiver himself. With this assumption, if any request is received from any machine and is encrypted with private key of receiver it is determines that the message is coming from trusted source as it is originally sent to sender from trusted third party.

Uniqueness in our protocol is achieved by generating unique keys for each request key generation service receive.

In our protocol integrity of message is guaranteed by encrypting the key with private key of receiver by trusted third party. As no one other then intended receiver and trusted third party has access to key, only receiver can decrypt message and read contents of message.

Our protocol does not have features to let user verify his/her vote from many vote casted. However the protocol can be modified in future to provide this functionality.

Our protocol does not have feature to authenticate election records. It does not allow verification of ballots and vote counting.

Our protocol shows reliability by being able to execute faster than other similar protocol. This is achieved by shortening number of steps required for key exchange. It is also resistant to attacks resulting from exchange of stale key. This is achieved by using timestamp to check freshness of key.

Our protocol provides secrecy of communication session as no one other then the three parties involved in communication knows about the communication taking place.

## 5.2 E-HealthCare Record Management System

Our protocol does not have any features that can hide identity of patient whose records are being accessed.

Our protocol works on symmetric key cryptography system that has is basis in trust based relationships between communicating devices. There is also a trusted third party that all other devices in network trust. This is the only computer or group of computers that knows secret key of devices other then devices themselves.

Our protocol helps in establishing secure connection on which data can be encrypted and then exchanged, such that guaranteeing that even if malicious user eavesdrops, or captures packets, he/she is not able to decrypt information.

## 5.3 Mobile Based Payment System

Our protocol works on confidentiality based on trust. It is assumed that if the message is coming from device that can identify itself and is among list of trusted devices in network, it can be trusted to be confidential in communication.

It is possible for trusted third party to keep track of all the requests. It can track source and destination of requests. Thus if any one party backs out the trusted party can provide proof of involvement.

# 6. CONCLUSION

In this paper we studied different security requirements posed by applications from various domains during key exchange process. We found several different requirements from applications.

Also due to variation in working domains, applications work with data of different natures. For example, health record management system stores mostly biological details related to patient where are a payment system deals with data of financial nature such as shares and currency.

We found that it is due to these variations in nature of information that these applications deals with, they have such different security requirements.

In analysis of E-voting system we find that our protocol does not fulfill requirements of verifiability and audit ability.

We also find that our protocol does not provide privacy which is one of the key requirements for E-Healthcare management system.

However we find that for a mobile based payment system our protocol fulfils all the requirements set forth by system from our analysis.

Therefore we conclude that our protocol is most suitable to be applied in applications where mobile based payment systems are used.

Table 1. E-Voting System

| | Authentication | Uniqueness | Integrity | Verifiability | Audit ability | Reliability | Secrecy |
|---|---|---|---|---|---|---|---|
| Is Supported by Protocol | Yes | Yes | Yes | No | No | Yes | Yes |

Table 2. E-Health Care Record Management System

| | Privacy | Trustworthiness | Authentication | Responsibility |
|---|---|---|---|---|
| Is Supported by Protocol | No | Yes | Yes | Yes |

Table 3. Mobile Based Payment System

| | Authentication | Confidentiality | Integrity | Non-Repudiation |
|---|---|---|---|---|
| Is Supported by Protocol | Yes | Yes | Yes | Yes |

## REFERENCES


[1] M. A. Azevedo, "Indian Mobile Payment Market Poised for Massive Growth," Cisco Corporation, 05 2014. [Online]. Available: http://newsroom.cisco.com/feature/1416791/Indian-Mobile-Payment-Market-Poised-for-Massive-Growth?utm_medium=rss. [Accessed 05 09 2014].

[2] A. Shukla, "Indians Vote Via Web with Scytl Technology," 9 Asia-Pacific Business and Technology Report, 23 May 2011. [Online]. Available: http://www.biztechreport.com/story/1318-indians-vote-web-scytl-technology. [Accessed 09 September 2014].

[3] "http://jumpseller.com/files/other/final_ecommerce_report07.pdf," 2007. [Online]. [Accessed 2014].

[4] R. Chopra, "Election Commission considering online voting arrangement for NRIs," The Economic Times, 20 02 2014. [Online]. Available: http://articles.economictimes.indiatimes.com/2014-02-20/news/47527324_1_voting-rights-nris-non-resident-indians. [Accessed 02 09 2014].

[5] O. I News, "India soon to get 'e-health care service'," One India News, 2014 08 12. [Online]. Available: http://news.oneindia.in/india/india-soon-to-get-e-health-care-service-1501148.html. [Accessed 02 09 2014].

[6] D. A. Gritzalis, Secure electronic voting, Kluwer Academic Publishers, 2003.

[7] "Report of the National Workshop on Internet Voting: Issues and Research Agenda," Internet Policy Institute, USA, 2001.

[8] R. Alvarez, T. Michael, E. H. Trechsell and A. H, "Internet voting in comparative perspective: the case of Estonia," PS: Political Science & Politics, vol. 42, no. 3, pp. 497-505, 2009.

[9] T. Patel, M. Chowkshi and N. Shah, "Smart Device Based Election Voting System Endorsed through Face Recognition," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 11, pp. 529-531, 2013.

[10] Y.-Y. Chen, J.-K. Jan and C.-L. Chen, "The design of a secure anonymous Internet," The design of a secure anonymous Internet voting system, vol. 23, no. 4, pp. 330-337, 2004.

[11] J. Karro and J. Wang, "Towards a practical, secure, and very large scale online electio," in 15th Annual, Computer Security Conference Applications, 1999.

[12] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, P. Marinella and V. Anna, "SEAS, a secure e-voting protocol: design and implementation," Computers & Security, vol. 24, no. 8, pp. 642-652, 2005.

[13] D. A. Gritzalis, "Principles and requirements for a secure e-voting system," Computers & Security, vol. 21, no. 6, pp. 539-556, 2002.

[14] "Common Position in Use of Internet in Conduct of Elections," International Working Group for Data Protection in Telecommunications, Berlin, 2001.

[15] B. Schoenmakers, "Compensating for a lack of transparency," in Computers, freedom and privacy: challenging the assumptions, Torento, 2000.

[16] K. Vollan, "Voting in Uncontrolled Environment and Secrecy of the Vote," in GI Lecture Notes in Informatics (Electronic Voting 2006), Bonn, 2006.

[17] T. Greenhalgh, S. Hinder, K. Stramer, T. Bratan and J. Russell, "Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace," British Medical Journal (BMJ), p. 341, 2010.

[18] T. Allard, N. Anciaux, L. Bouganim, Y. Guo, L. Le Folgoc, B. Nguyen, P. Pucheral, I. Ray, I. Ray and S. Yin, "Secure Personal Data Servers: a Vision Paper," The International Journal on Very Large Data Bases, vol. 3, no. 1-2, pp. 25-35, 2010.

[19] M. F. S. M. A. a. I. K. Farzandipour, "Security requirements and solutions in electronic health records: lessons learned from a comparative study," Journal of medical systems , vol. 34, no. 4, pp. 629-642, 2010.

[20] B. Third, "The new threat: Attackers that target healthcare organizations (And what you can do about it)," [Online]. Available: http://www.infosecwriters.com/text_resources/pdf/New_Threat_Brigade.pdf. [Accessed 13 09 2014].

[21] D. Mellado, E. Fernández-Medina and M. Piattini, "Security requirements engineering framework for software product lines," Information and Software Technology, vol. 52, no. 10, pp. 1094-1117, 2010.

[22] L. Liu, P. Shih and G. Hayes, "Barriers to the Adoption and Use of Personal Health Record Systems," in Proceedings of the 2011 iConference, 2011.

[23]T . Neubauer and J. Heurix, "A methodology for the pseudonymization of medical data.," International journal of medical informatics, vol. 80, no. 3, pp. 190-204, 2011.

[24] B. S. Elger, J. Iavindrasana, L. Lo Iacono, H. Müller, N. Roduit, P. Summers and J. Wright, "Strategies for health data exchange for secondary, cross-institutional clinical research," Computer methods and programs in biomedicine, vol. 99, no. 3, pp. 230-251, 2010.

[25] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in IEEE 3rd International Conference on Cloud Computing (CLOUD), 2010.
[26]M. A. Rothstein and M. K. Talbott, "Compelled authorizations for disclosure of health records: magnitude and implications," The American Journal of Bioethics, vol. 7, no. 3, pp. 38-45, 2007.
[27] A. Hoerbst, K. D. Christian, P. Knaup and E. Ammenwerth, "Attitudes and behaviors related to the introduction of electronic health records among Austrian and German citizens," International journal of medical informatics, vol. 79, no. 2, pp. 81-89, 2010.
[28] H. S. Committee, "Privacy and security standards applicable to ARRA requirements," 2009. [Online]. Available: http://healthit.hhs.gov/. [Accessed 13 09 2014].
[29] J. Benaloh, M. Chase, E. Horvitz and K. Lauter, ""Patient controlled encryption: ensuring privacy of electronic medical records," in In Proceedings of the 2009 ACM workshop on Cloud computing security, 2009.
[30] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara and G. Müller, "Aspects of privacy for electronic health records," International journal of medical informatics, vol. 80, no. 2, pp. e26-e31, 2011.
[31] N. Shivaramakrishnan, M. Gagné and S.-N. Reihaneh, "Privacy preserving EHR system using attribute-based infrastructure.," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010.
[32] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," Communications of the ACM , pp. 993-999, 12 December 1978.
[33] C. Peikari and S. Fogie, Maximum Wireless Security, Sams, 2003.
[34] S. Oaks, Java Security, O'Reilly, 2001.
[35] W. Lou, W. Liu and Y. Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks," in INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, Hong Kong, 2004.
[36] M. H. Whitfield Diffie, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 6, no. 22, pp. 644-645, 1976.
[37] "Description of Symmetric and Asymmetric Encryptiion," Microsoft Corporation, 26 10 2007. [Online]. Available: http://support.microsoft.com/kb/246071. [Accessed 28 07 2014].
[38] M. Atreya, "Introduction to Cryptography," August 2006. [Online]. Available: http://cs.ship.edu. [Accessed July 2014].
[39] J. Zhou, Non-Repudiation in Electroni Commerce, Artech House, 2001.
[40] P. Vyas, B. Trivedi and A. Patel, "An alternative technique to thwart multiplicity attack in Denning-Sacco protocol using timestamps," International Journal of Scientific and Engineeering Research, vol. 4, no. 11, pp. 617-619, 2013.

## AUTHORS

Pranav Vyas is currently serving as Assistant Professor at Charotar University of Science and Technology, Changa at Faculty of Computer Applications. He has Masters Degree in Computer Applications from Bhavnagar University. His research interests include Applied Cryptography, Security Systems and Intrusion Detection.

Bhushan H. Trivedi, Ph.D. is currently working as a Director in GLS Institute of Computer Technology. He has more than 22 years of academic experience in graduate courses primarily MCA (Master of Computer Applications). Apart from pedagogy and effective teaching methods, his research interests include Information Security and application of mobile agents in distributed intrusion detection as well as prevention systems and wireless sensor networks.