SURVEY ON BIOMETRIC APPLICATIONS FOR IMPLEMENTATION OF AUTHENTICATION IN SMART GOVERNANCE

Sumita Sarkar,

·Assistant Professor
Department of Computer Applications
Durgapur Society of Management Science
(D.S.M.S), W.B, India.

Abhishek Roy,

Research Scholar
Department of Computer Science
The University of Burdwan, W.B, India

ABSTRACT

With large scale proliferation of internet and network, more and more people tend to communicate through the insecure network channels. So, to avoid illegal access of confidential and private resources, user authentication is the primary requirement of this age. Nowadays, smart card based authentication schemes have been deployed widely to ensure the legitimacy of a user's access request. Smart cards can be associated with the other traditional authentication schemes like password or PIN, to enhance the security level of the system. In recent years, numerous researchers have focused on the field of user authentication schemes and figured out a new advanced and secure mechanism by employing biometrics as an authentication tool in smart card systems. In this paper, the authors have made a detailed survey on some eminent existing biometric technique based smart card authentication schemes. Since the existing schemes have several security pitfalls and are susceptible to dangerous attacks, this study will pave a way towards the evolution of an ideal authentication scheme that can attain every possible goals.

Keywords: Biometrics, authentication, non-repudiation, smart card.

INTRODUCTION:

In this web-enabled world, where every well-intended technological advancements makes its fate to be soon abused by someone malevolent, it have become very crucial for us to bring into existence an optimal secure solution that can provide reliable service to all facets of our modern life. With the advancement of science, individuals can move on with its every vital information effortlessly with the help of smart card based technology. This appliance not only can be used as a storage device but also play a significant and inevitable role in proving remote user's authentication, identification or secured access to the ICT systems. But, as usual, these easy to use, portable, intelligent devices are also not free from the mal-intentions of the fraudsters. To get rid of the frequent and severe fraudulent attacks, numerous anti-attack schemes were undertaken by the researchers. Password authentication schemes [36, 37], Dynamic ID-based schemes [38, 39], time stamp based schemes [40, 41], nonce based schemes [42, 43], etc. are some of their eminent creations. In the last few years, a new technology named biometrics has spurred a great deal of interest in the field of research and has also achieved the height of popularity in electronic personal identification and authorization of individuals at the POS (Point of Sale) terminals. Biometrics when combined with smart card technology creates a tight bond between the smart card and the cardholder. In our paper, we have carried out a thorough study over such biometric-based user authentication schemes using smart cards.
Section II describes the need of biometric technology in smart card authentication. Section III includes a literature survey on the biometrics based smart card authentication schemes. Conclusion drawn from the entire study is mentioned in Section IV. Section V contains the references.

NECESSITY OF BIOMETRICS FOR IMPLEMENTATION OF AUTHENTICATION IN SMART CARDS:

Biometrics can be used as an effective authentication tool to be implemented in smart card technology. This section will give an overview of the smart card and biometric technology and discuss the need of biometrics in smart card authentication and working of this combined technology.

a) SMART CARD TECHNOLOGY:

A smart card [44, 45, 46] is an intelligent device which is externally made of plastic containing an embedded integrated computer chip i.e., ICC (a microprocessor with or without memory) in it. This card is capable of storing up to 64Kbytes of information [45]; capable of performing its own processing functions and can be read by a terminal via smart card readers [52]. The information stored on the smart card can be secured using advanced security techniques viz., advanced cryptographic techniques and digital signature schemes. For performing the complex cryptographic computations, some smart cards contain an additional processor called cryptographic co-processor [47, 48] which makes the operations faster with an increase in efficiency. Due to such advanced features, the smart card technology can provide a strong authorization, confidentiality, security and integrity to the users of the authentication systems.
Based on the mode of access, the smart cards can be classified into four types:

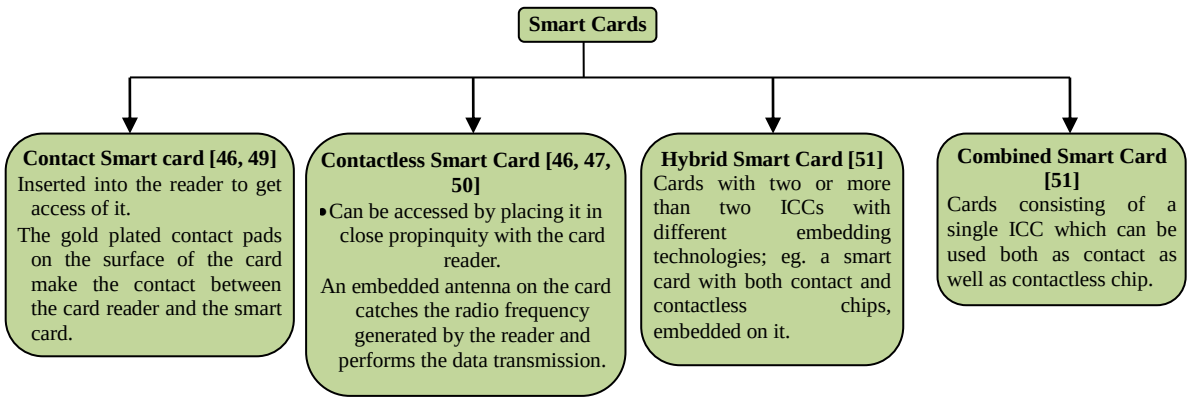

Fig. 1: Classification of smart cards

Smart cards are becoming more and more popular in our day-to-day activities. Their applications [46, 53, 54, 55] include but are not limited to e-commerce applications like payment cards (credit cards, debit cards, EMV cards [67], ATM cards, public phone payment cards, etc.), mobile SIM cards, electronic purse [68], etc.; e-governance [1,5,6,7,9,11,12] applications like citizen ID cards, electronic passports [69], driving license, etc.

and e-health [70] applications like medical ID cards and many more like student ID cards, employee ID cards, token for car parking, in public transits, in getting access to restricted buildings, etc.

b) AUTHENTICATION IN SMART CARDS:

In the context of communications across a network, the network terminals must be protected from the unwanted fraudulent attacks. So, a user of a system needs to prove his identity electronically before getting access to it. This process of validating a user's identity for access to a secured terminal is known as authentication [56, 57, 58, 59, 60, 61]. Authentication of a user can be carried out in the three possible ways-
The information which is known to the user i.e., Password, Personal Identification Number (PIN) or pattern.
The token possessed by the user i.e., Smart card.
The unique physical or behavioral characteristics that a user have i.e., biometric data.
The simplest and cheapest authentication technique widely used for authentication purpose is the password [56] based schemes. Though simple in implementation, this scheme is vulnerable to password guessing attacks, replay attacks, dictionary attacks and social engineering attacks. To reduce the chances of guessing attacks, a user can choose a long and complex password which in turn is difficult for the user to remember. Replay attacks can be curbed to an extent by using encrypted passwords. One-time password [62, 63] is a better authentication technique where the passwords for each login are unique and randomly generated numbers. These one-time passwords can be combined with smart cards to build a secure solution. But this is not the optimal solution as it can be invaded by the man-in-the-middle [2] and man-in-the-browser [8] attacks and is also time consuming. Moreover, passwords or PINs are liable to be forgotten, copied, stolen and subsequently used malevolently by the imposter.
Smart cards are more secure than the other aforementioned techniques due its Public Key Infrastructure (PKI) [64].But, like passwords and PINs, the smart cards are also susceptible to loss, theft and finally can be used for unauthorized access.
The third possibility i.e., the biometrics can provide a stronger authentication and non-repudiation as it is very unique to an individual i.e., hard to copy or replicate or deny and also cannot be easily stolen. Biometrics can be integrated with the second possibility i.e., the smart card to build a more sound, fast and secure user authentication system.

c) BIOMETRICS AS A TOOL FOR IMPLEMENTATION OF AUTHENTICATION IN SMART CARDS:

i) OVERVIEW ON BIOMETRIC TECHNOLOGY:

Biometrics [3, 4] is a term related to the identification or verification of individuals based on its own physical or behavioral traits. The physical biometrics is based on the individual's anatomy. It includes fingerprint recognition, retina/iris scan, face recognition, vein pattern analysis, etc. Behavioral biometrics encompasses speech recognition, signature pattern, gait analysis, keystroke dynamics, etc. These biometric traits are very unique to an individual and can be extensively used as a tool for identification. To get more accuracy and security, some systems use a combination of multiple biometric traits to identify an individual.
These biometric techniques when combined with the smart card technology gives birth to a new generation two-factor authentication tool where the biometrics embedded in the smart card will verify the authenticity of the cardholder, thereby reducing the chances of illegitimate access, identity theft and similar fraudulent actions and enhancing the security, privacy, efficiency, reliability and providing strong non-repudiation to the smart card systems. The confidential information stored on the card including the bio-template is encrypted using advanced cryptographic and digital signature schemes; which make the smart card more tamper proof even on loss of the card. Some systems also employ three factor authentication comprising smart cards, biometrics and PIN/password to build an unbeatable secure solution.

ii) WORKING PRINCIPLE OF A BIOMETRIC SMART CARD:

The working of a biometric smart card [44] can be expressed in the following steps:
Step 1: Enrollment: This is the preliminary phase where a user enrolls its biometrics in the smart card. The user biometrics is first captured using a biometric sensor, its unique features are extracted and converted into a biometric template and finally stored onto the smart card to make it ready for use.
Step 2: Authentication: After enrollment, when the user attempts to access a secure system using smart card, a fresh biometric data is again required to be placed on the capture device, attached to the secured terminal. This live biometric is then compared to the biometrics stored on the smart card. The matching mechanism can be

carried out in two ways:

a) Match-off-card: In this mechanism, the matching operation is carried out outside the smart card. When a user places his biometrics for authentication, the biometric stored on the card is extracted and compared to the live biometric in an external device which may be a card reader or a remote server. This mechanism may face security risks as the communication channel between the matching device and the smart card may face eavesdropping or the matching device may be compromised thereby losing the confidentiality of the smart card data.

b) Match-on-card [65]: This is a more secure way of implementation where the matching is performed within the smart card itself. During authentication the live template is captured and sent to the smart card for its verification. The smart card having the capability of performing the matching operations, compares the live biometric with its stored biometric template and gives the result back to the external terminal. This technology protects the privacy of the biometric information of the user, as the biometric data doesn't need to go out of the card for its processing.

If the matching score is above the threshold value, then the user will be authorized for the system access and if it does not reach that level, then the access is denied. This threshold value [66] is chosen based on the need of accuracy level of the application.

LITERATURE SURVEY:

In this paper, we have carried out an exclusive survey [10, 13] on some of the eminent schemes postulated to implement biometrics as an authentication tool in smart card technology.

Paper Title	Objective	Tools/Techniques
Fingerprint-based remote user authentication scheme using smart cards [15]	• To enhance the security of the password based user authentication schemes in smart cards, the authors have presented a new scheme which introduces a new technology "Biometrics" in the field of information security. • This scheme does not require the system to store password tables and hence makes the system more secure. • It is proven that this scheme can withstand the replay attacks and impersonation attacks. But the system can face impersonation attacks if one of the secret keys used in this scheme is hacked by the attackers. • It can work efficiently and with an enhanced security on a remote user authentication system.	• The security of this approach is based on the ElGamal public key cryptosystem, with two secret keys. • The biometrics used in this approach uses fingerprint verification with minutiae matching techniques.
Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards [16]	• The authors here have analyzed the security pitfalls of the Lee-Ryu-Yoo (LRY) scheme [15]. • The article proves that the LRY scheme is vulnerable to forgery attacks. • It proves that on loss of the server generated password, the system can get compromised and is not easy to repair. • The authors also show that in the LRY scheme, the user do not have the privilege to choose and alter passwords. • They have also pointed out that in LRY scheme, the server generated passwords are too long for a user to remember.	• The authors have proved that LRY scheme is insecure by invading the scheme using some well known attacks. • They have also analyzed the other features of the LRY scheme and pointed out its drawbacks.
Secure Fingerprint-Based Remote User Authentication Scheme Using Smartcards [17]	• In this paper, the authors have proposed a new scheme to resolve the drawbacks of the LRY scheme [15], as figured out in aforementioned Chang-Chiang's article [16]. • The proposed scheme can withstand the well known forgery attacks used to invade the LRY	• The proposed scheme uses one way hash function and fingerprint verification as its security tool. • In order to avoid the complexity and to enhance

	system. • Unlike the LRY scheme, this system can be repaired after being compromised. • The password selection and alteration are convenient in this scheme. • It provides lower computation cost relative to the LRY scheme.	the efficiency, the proposed scheme does not use the multiplication and exponential operations.
A flexible biometrics remote user authentication scheme [18]	• In this article, the authors have presented an enhanced version of the above listed Lee-Ryu-Yoo scheme [15]. • They have pointed out that the Lee-Ryu-Yoo scheme is susceptible to the masquerade attack and so is less secure. • The proposed scheme provides relatively more security and more flexibility (has the provision to change passwords easily). • The scheme can be implemented in high security applications.	• The security is enhanced through ElGamal's cryptosystem using only one secret key, fingerprint verification using minutiae recognition, password and smart card technology. • The techniques involved are one way hashing, Exclusive OR function and modulus operation. • The scheme uses timestamp for synchronization.
Security of the Lin-Lai smart card based user authentication scheme [19]	The authors of this article have figured out that the security of the Lin-Lai's scheme [18] fails in the following aspects: • Absence of any threat model (threat possibilities) in the scheme. • The system gets compromised on loss of smart card and password. • Faults in synchronization attempts. • Absence of any user identifier input format. • The password change facility does not require the user to place the existing password.	In this paper, the authors have analyzed the above mentioned Lin-Lai scheme, discussed its security issues and established that Lin-Lai's scheme cannot provide a fool proof security to the system.
Remote Password Authentication Scheme with Smart Cards and Biometrics [20]	• The authors here have proposed a new and improved remote three factor authentication scheme, compares its performance and security with the previously proposed three factor authentication schemes, and finally concludes that their scheme is more secure, efficient and a truly three factor authentication scheme, capable of preserving the user's privacy. • The attackers cannot invade the system if at least any one of the three factors is unknown to them. • The proposed scheme verifies the authenticity of the three factors (biometrics, smart card and password) in the remote server. • It can resist replay attacks and offline dictionary attacks. • The scheme provides low computation costs which make it more effective and applicable to smart card environments.	• The privacy of the biometric template is preserved by associating it with a random number using an X-OR operation. • The fingerprint sensors are placed on the smart cards rather on the image capture devices, which prevents the invaders to steal the biometric traits. • The security of this scheme is enforced through Rabin's public key encryption algorithm.
A Two-Factor Mutual Authentication Scheme Using Biometrics	• A two factor mutual authentication scheme has been proposed by the authors in this article. • The scheme reduces the chances of identity theft by storing some auxiliary information generated from the biometric template, instead of storing the	• The scheme uses the two factors- Biometrics and smart card to ensure privacy and security of the system. • One-way collision resistant

and Smart Card [21]	template itself, on the smart card. • It is proven to withstand impersonation attacks, stolen verifier attacks, replay attacks and stolen smart card attacks and can also preserve the privacy of the user's biometrics.	hash functions and Exclusive OR operations are the techniques used in this algorithm. • Error control codes are used to remove the noisiness of the biometric templates.
A New Efficient Fingerprint-Based Remote User Authentication Scheme for Multimedia Systems [22]	In this paper, the authors have discussed the security issues of the above mentioned Lin-Lai scheme, proved its vulnerability towards impersonation attacks, and proposed a new improved scheme which provides better security, efficiency and incurs comparatively less computation costs in the multimedia environment.	The security of the scheme has been achieved using the one way hash function and discrete logarithm problem.
An Improved Fingerprint-Based Remote User Authentication Scheme Using Smart Cards [23]	• The authors here have performed a cryptanalysis on the above listed Yoon-Yoo scheme [22] and revealed that the approach is vulnerable to impersonation attacks. • They have launched a new scheme which can withstand such attacks and provide more security and efficiency to the authentication system. • The proposed scheme incurs relatively low computation costs with respect to other similar schemes.	The scheme uses discrete logarithm problem, one way hash function, fingerprint verification and smart card technology to enhance the security of the Yoon-Yoo scheme.
Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics [24]	• This scheme puts emphasis on the privacy protection of the biometric templates. • Timestamps are not required anymore for synchronization. • Users are free to choose their passwords. • This approach achieves its completeness through the GNY logic and its security using the Bellare and Rogaway's model. • Its low computation cost makes it appropriate for smart card implementations.	• Here, the three factors- smart card, Biometrics and password are used to implement the scheme. • The security of the scheme is strengthened using a strong cryptographic algorithm where the biometric template is used as an encryption key. • Therefore, though the matching is performed in the remote server, the server cannot listen to the biometric data, but can check the authentication of the same. • Iris scanning is used as the biometric technique in this approach.
An Improved Three-Factor Authentication Scheme Using Smart Card with Biometric Privacy Protection [25]	The authors have discussed the loopholes of the remote three factor authentication scheme proposed by Chun-I-Fan and Yi-Hui-Lin [24], and proposed a new improved scheme that overcomes those faults and provides more security and ensures user's privacy.	• The algorithm is designed using the 3 factors- Biometrics, Password and smart card. • The feature extracted during enrollment phase is encrypted using a strong public key encryption algorithm and combined with server generated random numbers to enhance

		the privacy and security of the users' information.
An efficient and secure biometric remote user authentication scheme using smart Cards [26]	• This paper launches a new mutual and remote authentication scheme, compares its performance with the previously proposed similar schemes and shows that it can provide more security, efficiency and reliability over an insecure communication channel. • The users can alter their passwords conveniently. • The server is not burdened with biometric data and password records. • A session key is used for synchronization. • The low computation costs and high efficiency of this scheme makes it applicable to environments with limited resources.	The proposed scheme uses the 3 factors- Fingerprint biometrics, Password and smart cards along with two-variant hashing and bio-hashing techniques to enhance the security of the algorithm.
Multi-level Authentication Scheme Utilizing Smart Cards and Biometrics [27]	• The authors here have proposed a new architecture for remote and mutual authentication which can provide multi-level security to the system. • The three factors (biometrics, smart card and password) can be used at different levels of this architecture. • The scheme does not require storing the verification tables within the server. • The scheme is immune to forgery and replay attacks. • It preserves the privacy of the user biometrics along with the password. • The authentication policy can be altered using the policy server. • The verification of the biometric data is performed at the server side.	• The proposed scheme uses RSA algorithm for implementing the security of the system. • The policy server is used to choose the authentication level in the proposed architecture.
An efficient biometrics- based remote user authentication scheme using smart cards [28]	• This paper proposes a biometric based, remote user, mutual authentication scheme, which is computationally less complex and more efficient compared to the other related schemes. • It provides non-repudiation, provision of changing passwords without server's intervention and simple ways to maintain synchronization between the user and the server. • This scheme can be implemented in distributed computing environments.	• The techniques involved in this scheme are one way hashing, exclusive OR and concatenation operations. • This scheme does not require storing the password tables within the server. • It uses random number as a means of synchronizing the server with its user.
Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards [29]	• The authors here have analyzed the security issues of the aforementioned Li-Hwang's scheme [28] and figured out that the scheme cannot protect the system from man-in-the-middle attacks. • Moreover, the scheme in [28] cannot provide proper authentication. • This paper introduces a new biometric based remote authentication scheme that keeps the benefits of [28], but eradicates all its security pitfalls, and brings in some additional features, which are suitable for real life applications. • The proposed scheme maintains the security of the secret key; provides session key agreement; can	• The technique used for biometric verification is biometric template matching. • The security of the secret keys and session keys are enforced using the one way hash function.

	withstand insider attacks, man-in-the-middle attacks and replay attacks; and provides proper mutual authentication between the server and the user.	
Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards [30]	• This paper analyses on the above mentioned schemes in [28] and [29], proves that [29] is an enhanced version of [28], but cannot ensure its foolproof security. The authors here have proposed a new biometric based remote user mutual authentication scheme which eradicates the security loopholes prevalent in the above mentioned schemes. • They have figured out that those schemes [28 and 29] are vulnerable to impersonation attacks, password guessing attacks, replay attacks and denial of service attacks. • In [28] and [29], if the attackers get control over the biometric template, then the system will get compromised. • The proposed scheme can resist the man-in-the – middle attacks and DoS attacks and can provide security to the biometric template and the secret keys and session keys used in the algorithm. • This approach is computationally more efficient than the previous schemes.	• The schemes in [28] and [29] are less secure because the random number used in those approaches can be used by the attackers to crack those systems. • The proposed scheme uses a one way hash function with SHA-256 to improve the security of the system. • The SHA-256 is also used in the proposed scheme for random number generation and in the message authentication code function.
Analysis and improvement on an efficient biometric-based remote user authentication scheme using smartcards [31]	• This article is an enhancement of the Li-Hwang's scheme [28], which figures out the design shortcomings of the scheme and proposes a new system which is capable of resolving all the flaws; provides a strong mutual authentication and ease to change passwords with low computation costs. • The proposed scheme does not use synchronized clocks.	• The strong authentication is achieved with verifying biometrics, passwords and random nonces. • The biometric verification is performed using the pattern matching algorithms.
Security Analysis and Enhancements of an Effective Biometric-Based Remote User Authentication Scheme Using Smart Cards [32]	• In this paper, the author have analyzed the security issues of the above mentioned Das authentication scheme [31], and presented a new and advanced scheme that resolves all the security issues in the Das's scheme and also provides a mutual authentication between the server and the user. • The author had figured out that the attackers can easily invade the Das's system if both the password and smart card are stolen. • The Das's scheme is susceptible to the password guessing attacks, impersonation attacks, server masquerading attack and insider attacks. • It is proved in this paper that the scheme in [31] cannot provide proper mutual authentication.	• The failures of Das's scheme have been proved by imposing several attacks on the system. • To analyze the security of the proposed scheme, the author have assumed that the smart card may be used by an illegitimate user, the security information on the card can be stolen and the communication channel between the user and the server may be intercepted.
Hiding Fingerprint in Face using Scattered LSB Embedding Steganographic Technique for Smart card	• This paper proposes a biometric based authentication scheme in smart cards, which uses both Steganographic and Cryptographic techniques in order to preserve the privacy of the biometric templates in smart cards. • The fingerprint information is stored and verified on the smart card itself.	• The Steganographic technique uses the Least Significant Bit (LSB) embedding algorithm and the Pseudo Random Number Generator (PRNG) chooses the location, where the

based Authentication system [33]	• The scheme hides the fingerprint of the user in their photo on the smart card. • The scheme is resistant to the statistical attacks based on histogram analysis.	encrypted fingerprint data is to be embedded within the cover image.
Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem [34]	• In this paper, the authors have proposed a new secure and efficient biometric based mutual authentication scheme for distributed multi-server network environments and communication resource environments; compared it with the other multi-server authentication schemes and showed that their proposed scheme is more secure, with reduced execution time and less storage requirement. • The proposed scheme provides the facility for easy biometrics and password change through password and biometrics update protocol. • The proposed scheme can withstand several well known attacks viz. guessing attacks, replay attacks, stolen verifier and smart card attacks, insider attacks, server spoofing attacks, impersonation attacks, secret key and session key attacks.	• The authors have used biometrics, password, smart card and one way hash function and Elliptic Curve Cryptography (ECC) to ensure security of their scheme. • The proposed scheme provides an efficient ECC based key agreement function which makes the scheme computationally efficient using the property of perfect forward secrecy.
A Novel Biometric-Based Remote User Authentication Scheme Using Quadratic Residues [35]	• In this article, the authors have proposed an efficient and secure biometric based, remote user, mutual authentication scheme using smart cards for real network applications. • The proposed scheme can resist replay attacks, known key attacks, impersonation attacks, stolen smart card attacks and is able to maintain the forward secrecy.	The techniques used in the proposed scheme involve quadratic residues, biometric verification, exclusive OR operation and one way hash function.

CONCLUSION:

A handful of user authentication schemes using biometrics and smart card have been studied in this article. It has been analyzed that the authentication and security of the schemes have been enhanced with more and more research. Several multi factor and multi level architectures are being used to raise the security level of the system. For security purpose, the servers are also designed not to store the password and verification tables or the biometric records in it. In order to build a strong authentication system, both the user and the server should be involved in mutual authentication and should also be properly synchronized. An ideal biometric based smart card authentication scheme is also immune to replay attacks, stolen smart card attacks, security key attacks, server spoofing attacks, insider attacks, password guessing attacks, man-in-the-middle attacks, denial of service attacks, dictionary attacks and forgery attacks and should conform to the perfect forward secrecy. The stored biometric data is protected from the fraudulent attacks using several cryptographic and steganographic techniques. The system should be flexible enough so that the users can choose and change the passwords easily and safely. Finally, the scheme has to be efficient that is, it ought not to use much exponential operations thereby reducing the computation and communication costs and making the smart card applicable to practical environments.

REFERENCES:

[1] Sur, C., Roy, A., Banik, S. (2010). A Study of the State of E-Governance in India. Proceedings of National Conference on Computing and Systems, pp: (a)-(h), ISBN: 8190-77417-4.
[2] Man-in-the-middle. Retrieved June 18, 2013, from https://en.wikipedia.org/wiki/Man-in-the-middle.
[3] Roy, A., Sarkar, S., Mukherjee, J., Mukherjee, A. (2012). Biometrics as an authentication technique in E-Governance security. Proceedings of UGC sponsored National Conference on Research and Higher

Education in Computer Science and Information Technology, Vol: 1, pp: 153-160, ISBN: 978-81-923820-0-5.
[4] Sarkar, S., Roy, A. (2012). A Study on Biometric based Authentication. Proceedings of Second National Conference on Computing and Systems, 1st Edition - 2012, pp: 263-268, ISBN: 978-93-80813-18-9.
[5] Hoda, A., Roy, A., Karforma, S. (2012). Application of ECDSA for security of transaction in E-Governance. Proceedings of Second National Conference on Computing and Systems, 1st Edition - 2012, pp: 281-286, ISBN: 978-93-80813-18-9.
[6] Roy, A., Karforma, S. (2013). UML based modeling of ECDSA for secured and smart E-Governance system. Computer Science & Information Technology: Proceedings of National Conference on Advancement of Computing in Engineering Research, pp: 207 - 222, ISSN 2231 - 5403, ISBN: 978-1-921987-11-3.
[7] Roy, A., Banik, S., Karforma, S., Pattanayak, J. (2010). Object Oriented Modeling of IDEA for E-Governance Security. Proceedings of International Conference on Computing and Systems, pp: 263-269, ISBN: 93-80813-01-5.
[8] Man-in-the-browser. Retrieved June 20, 2013, from https://en.wikipedia.org/wiki/Man-in-the-browser.
[9] Roy, A., Karforma, S. (2012). Object Oriented approach of Digital certificate based E-Governance mechanism. Computational Intelligence and Communication Engineering: International Joint Conference on CIIT, CENT, CSPE and CIITCom Proceedings, LNICST Springer Chennai, INDIA, pp: 360 - 366, ISSN: 1867-8211.
[10] Roy, A., Karforma, S. (2011). A Survey on E-Governance Security. International Journal of Computer Engineering and Computer Applications (IJCECA). Fall Edition, Vol. 08, Issue No. 01, pp: 50-62, ISSN: 0974-4983.
[11] Roy, A., Banik, S., Karforma, S. (2011). Object Oriented Modelling of RSA Digital Signature in E-Governance Security. International Journal of Computer Engineering and Information Technology (IJCEIT), Summer Edition, Vol. 26, Issue No. 01, pp: 24-33, ISSN: 0974-2034.
[12] Roy, A., Karforma, S. (2011). Risk and Remedies of E-Governance Systems. Oriental Journal of Computer Science & Technology (OJCST), Vol. 04 No: 02, pp: 329-339, ISSN: 0974-6471.
[13] Roy, A., Karforma, S. (2012). A Survey on digital signatures and its applications, Journal of Computer and Information Technology, Vol. 03 No: 1 & 2, pp: 45-69, ISSN: 2229-3531.
[14] Roy, A., Karforma, S., Banik, S. (2013). Implementation of authentication in e-governance- an UML based approach. Lap Lambert Academic Publishing, Germany, ISBN 978-3-659-41310-0.
[15] Lee, J.K., Ryu, S.R., Yoo, K.Y. (2002). Fingerprint-based remote user authentication scheme using smart cards. Electronics Letters (Vol. 38, Issue: 12), pp: 554 – 555, ISSN: 0013-5194.
[16] Ku, W.C., Chang, S.T., Chiang, M.H. (2005). Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards. Electronics Letters (Vol. 41, Issue: 5), pp: 240 – 241, ISSN: 0013-5194.
[17] Yoon, E.J., Yoo, K.Y. (2005). Secure Fingerprint-Based Remote User Authentication Scheme Using Smartcards. Internet and Network Economics, Lecture Notes in Computer Science Vol. 3828, pp: 405-413, Print ISBN: 978-3-540-30900-0.
[18] Lin, C.H., Lai, Y.Y., A flexible biometrics remote user authentication scheme. Retrieved June 15, 2013, from http://www.csie.thu.edu.tw/csiethu/files/paper/ISLab/islab_92_18.pdf.
[19] Mitchell, C.J., Tang, Q., Security of the Lin-Lai smart card based user authentication scheme. Retrieved June 16, 2013, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.62.3957&rep=rep1&type=pdf.
[20] Fan, C-I., Lin, Y-H., Hsu, R-H. (2006). Remote Password Authentication Scheme with Smart Cards and Biometrics. Global Telecommunications Conference, GLOBECOM '06. IEEE, pp: 1 – 5, ISSN: 1930-529X, E-ISBN: 1-4244-0357-X, Print ISBN: 1-4244-0356-1.
[21] Ziauddin, S., A Two-Factor Mutual Authentication Scheme Using Biometrics and Smart Card. Retrieved June 16, 2013, from http://link.springer.com/chapter/10.1007%2F978-3-642-10847-1_26.
[22] Yoon, E.J., Yoo, K.Y. (2005). A New Efficient Fingerprint-Based Remote User Authentication Scheme for Multimedia Systems. 9th International Conference on Knowledge-Based & Intelligent Information & Engineering Systems, LNAI 3683, pp: 332-338, Print ISBN- 978-3-540-28896-1.
[23] Lee, Y., Kwon, T., An Improved Fingerprint-Based Remote User Authentication Scheme Using Smart Cards. Retrieved June 17, 2013, from http://link.springer.com/chapter/10.1007%2F11751588_95.

[24] Fan, C-I., Lin, Y-H., Provably Secure Remote Truly Three-Factor Authentication Scheme with Privacy Protection on Biometrics. Retrieved June 17, 2013, from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5238635.
[25] Mathew, H.M., Gundapu, P. S. J., Raj, S. B. E., Angeline, S. J. F. (2011). An Improved Three-Factor Authentication Scheme Using Smart Card with Biometric Privacy Protection. Proceedings of 3rd International Conference on Electronics Computer Technology, Vol. 3, pp- 220-223, Print ISBN- 978-1-4244-8678-6.
[26] Wang, X., Zhang, W. (2008). An efficient and secure biometric remote user authentication scheme using smart cards. Proceedings of Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, pp: 913 – 917, Print ISBN: 978-0-7695-3490-9.
[27] Mutlugün, M., Soğukpinar, I. (2009). Multi-level Authentication Scheme Utilizing Smart Cards and Biometrics. Third International Conference on Emerging Security Information, Systems and Technologies, pp: 93 – 98, Print ISBN: 978-0-7695-3668-2.
[28] Li, C.T., Hwang, M.S. (2010). An efficient biometrics- based remote user authentication scheme using smart cards. Journal of Network and Computer Applications, Volume 33 Issue 1, pp- 1-5, ISSN: 1084-8045.
[29] Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards. Retrieved May 25, 2013, from http://www.sciencedirect.com/science/article/pii/S1084804510001657.
[30] Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards. Retrieved May 26, 2013, from http://eprint.iacr.org/2011/676.pdf.
[31] Das, A.K. (2011). Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. Information Security: IET (Vol. 5, Issue: 3), pp: 145 – 151, ISSN: 1751-8709.
[32] Security Analysis and Enhancements of an Effective Biometric-Based Remote User Authentication Scheme Using Smart Cards. Retrieved May 28, 2013, from http://downloads.hindawi.com/journals/jbb/2012/519723.pdf.
[33] Brindha, S., Vennila, Ila. (2011). Hiding Fingerprint in Face using Scattered LSB Embedding Steganographic Technique for Smart card based Authentication system. International Journal of Computer Applications (0975 – 8887), Vol. 26, No.10, pp: 51-55.
[34] Yoon, E-J., Yoo, K-Y. (2013). Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. The Journal of Supercomputing, Vol. 63, Issue: 1, pp: 235-255, Print ISSN: 0920-8542, Online ISSN: 1573-0484.
[35] A Novel Biometric-Based Remote User Authentication Scheme Using Quadratic Residues. Retrieved 02, 2013, from http://www.ijiee.org/papers/348-I20002.pdf.
[36] Yang, C., Ma, W., Huang, B., and Wang, X. (2007). Password-Based Access Control Scheme with Remote User Authentication Using Smart Cards. 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), Vol. 2, pp: 448-452, Print ISBN: 978-0-7695-2847-2.
[37] Kim, H-S., Seo, S. and Choi, J-Y. (2010). Security Analysis of Smart Card based Password Authentication Schemes. 3rd International Conference on Information Sciences and Interaction Sciences (ICIS), pp: 352 – 356, E-ISBN: 978-1-4244-7386-1, Print ISBN: 978-1-4244-7384-7.
[38] Gao, Z., Tu, Y. (2008). An Improvement of Dynamic ID-Based Remote User Authentication Scheme with Smart Cards. Proceedings of the 7th World Congress on Intelligent Control and Automation (WCICA), pp: 4562 – 4567, E-ISBN: 978-1-4244-2114-5, Print ISBN: 978-1-4244-2113-8.
[39] Khan, M.K. (2009). Enhancing the Security of a 'More Efficient & Secure Dynamic ID-based Remote User Authentication Scheme'. Third International Conference on Network and System Security (NSS), pp: 420 – 424, E-ISBN: 978-0-7695-3838-9, Print ISBN: 978-1-4244-5087-9.
[40] Wei, Y-Z., Hu, Y-P. (2006). Security Analysis of Timestamp-based Remote User Authentication Scheme Using Smart Cards. International conference on communications, circuits and systems proceedings, Vol. 3, pp: 1580 – 1582, E-ISBN: 0-7803-9585-9, Print ISBN: 0-7803-9584-0.
[41] Wang, Y., Li, J. (2004). Security improvement on a timestamp based password authentication scheme. IEEE Transactions on Consumer Electronics, Vol. 50, Issue. 2, pp: 580-582, ISSN: 0098-3063.
[42] Kai, H., Qingyu, O., Xiaoping, W., Yexin, S. (2009). Cryptanalysis of a remote user authentication scheme using smart cards. 5th International conference on Wireless Communications, Networking and Mobile Computing (WiCom), pp: 1 – 4, E-ISBN: 978-1-4244-3693-4, Print ISBN: 978-1-4244-3692-7.
[43] Liaw, H.T., Lin, J.F., and Wu, W.C. (2006). An efficient and complete remote user authentication scheme using smart cards. Mathematical and Computer Modelling, Vol. 44, Issues. 1-2, pp: 223–228, ISSN: 0895-7177.

[44] Smart cards and Biometrics. Retrieved June 10, 2013, from http://www.smartcardalliance.org/resources/pdf/Smart_Cards_and_Biometrics_030111.pdf.
[45] Being smart with Biometrics & Smart cards. Retrieved June 15, 2013, from http://www.giac.org/paper/gsec/2188/smart-biometrics-smart-cards/103722.
[46] Smart Card. Retrieved June 20, 2013, from https://en.wikipedia.org/wiki/Smart_card.
[47] An Introduction to Smart cards. Retrieved July 2, 2013, from http://artofconfusion.org/smartcards/docs/intro.pdf.
[48] Cryptographic Coprocessor. Retrieved June 20, 2013, from http://encyclopedia2.thefreedictionary.com/cryptographic+coprocessor.
[49] Types of Smart card. Retrieved June 20, 2013, from http://www.smartcardbasics.com/smart-card-types.html.
[50] Contactless Smart Card. Retrieved June 25, 2013, from http://en.wikipedia.org/wiki/Contactless_smart_card.
[51] Storing Data on ID Cards. Retrieved June 28, 2013, from http://www.idwholesaler.com/learning-center/articles/id-cards/data-storage.htm.
[52] Smart card Readers and Terminals. Retrieved June 30, 2013, from http://www.smartcardbasics.com/smart-card-reader.html.
[53] Smart Cards Applications. Retrieved June 30, 2013, from http://www.smartcardalliance.org/pages/smart-cards-applications.
[54] Smart Card Overview. Retrieved July 02, 2013, from http://www.smartcardbasics.com/smart-card-overview.html.
[55] Drygajlo, A. (2011). Biometrics for Identity Documents and Smart Cards: Lessons Learned. Biometrics and ID Management: COST 2101 European Workshop, BioID 2011, Brandenburg (Havel), Proceedings, Vol. 6583, pp: 1-12, Print ISBN: 978-3-642-19529-7, Online ISBN: 978-3-642-19530-3.
[56] Different Ways to Authenticate Users with the Pros and Cons of each Method. Retrieved July 05, 2013, from http://publications.nr.no/Authentication_atFHI.pdf.
[57] Authentication, Tokens, Smart Cards and Biometrics: An Overview. Retrieved July 06, 2013, from http://www.pctools.com/guides/article/id/10/.
[58] Strong Authentication using smart card technology for Logical Access. Retrieved July 06, 2013, from http://www.smartcardalliance.org/pages/publications-strong-authentication-using-smart-card-technology-for-logical-access.
[59] Authentication Techniques for Smart Cards. Retrieved July 06, 2013, from http://www.osti.gov/bridge/servlets/purl/10141490-M8bQpq/native/10141490.pdf.
[60] The Pros and Cons of Advanced Authentication. Retrieved July 07, 2013, from http://www.esecurityplanet.com/hackers/the-pros-and-cons-of-advanced-authentication-.html.
[61] Multi-factor Authentication. Retrieved July 07, 2013, from https://en.wikipedia.org/wiki/Multi-factor_authentication.
[62] One-time Password. Retrieved July 07, 2013, from http://en.wikipedia.org/wiki/One-time_password.
[63] One Time password (OTP). Retrieved July 08, 2013, from http://www.gemalto.com/techno/otp/.
[64] Design and Implementation of Public Key Infrastructure on Smart Card Operating System. Retrieved July 08, 2013, from http://www.cse.iitk.ac.in/users/moona/students/Y3167022.pdf/.
[65] Henniger, O., Franke, K. (2004). Biometric user authentication on smart cards by means of handwritten signatures. First International Conference on biometric authentication (ICBA) Proceedings, pp: 547-554, Print ISBN: 978-3-540-22146-3, Online ISBN: 978-3-540-25948-0.
[66] Biometric matching thresholds. Retrieved July 08, 2013, from http://biometrics.zzl.org/Biometric%20Matching%20Thresholds.pdf.
[67] EMV. Retrieved July 08, 2013, from http://en.wikipedia.org/wiki/EMV.
[68] The Electronic Purse: An Overview of Recent developments and Policy issues. Retrieved July 08, 2013, from http://www.bankofcanada.ca/1996/01/publications/research/technical-report-no74/.
[69] Biometric passport. Retrieved July 09, 2013, from https://en.wikipedia.org/wiki/Biometric_passport.
[70] Smart Cards and Biometrics in Healthcare Identity Applications. Retrieved July 09, 2013, from http://www.smartcardalliance.org/pages/smart-cards-applications-healthcare.
