# A Generic Framework to Enhance Two-Factor Authentication in Cryptographic Smart-card Applications

G.Prakash [#1], M.Kannan [*2]

[#] Research Scholar, Information and Communication Engineering, Anna University
[#]Associate Professor, Information Technology Department, Sona College of Technology,
TPTC Main Road, Salem – 636005, TamilNadu, India
[1] gprakas74.h@gmail.com
[*] Professor, Information Technology Department, Sri Ramakrishna Institute of Technology
Pachapalayam, Coimbatore – 641 010, TamilNadu, India
[2] kannankrish68@yahoo.com

***Abstract*—Today, most authenticating applications using passwords are being compromised and the risk is becoming higher because it's becoming easier to download tools that will crack them. Passwords are no longer sufficient, as threats against them increase in large quantity. With the growing use of internet to access information resources, government and private agencies are now moving to replace password-based user authentication with stronger, Two-factor authentication systems that strengthen information security. Two-factor authentication requires that two parts of data be accessible, each being from a different category. It is a secure identification process in which the user provides two means of recognition, one of which is normally a physical token, such as a card, and the other of which is typically something memorized, such as a password or PIN number. In general Cryptographic Smart Cards provide a secure, portable platform for this type of Two-factor authentication systems. However, these smart card cryptographic systems are vulnerable to traditional mathematical attacks such as Differential and Linear Cryptanalysis attacks. These attacks explore weaknesses in cryptographic algorithms that are represented as mathematical objects. Other form of cryptographic attacks like Differential Power Analysis (DPA) attacks, fault attacks, replay attacks, side channel attacks, etc also exists. Hence to overcome these attacks, a new generic framework "Smart Crypto-Stegano Card" is proposed in this paper to enhance Two-Factor Authentication that gives users a better way to provide enhanced security for different smart card applications.**

**Keyword-Two-Factor Authentication, Linear Cryptanalysis attacks, Differential Power Analysis attacks, Smart Crypto-Stegano Card**

## I. Introduction

Information Security is one of the most important applications of computer systems and has been integrated into Information Technology sector tightly. Modern commodity computers demand secure storage strongly as they deal with highly classified information and the system protects the secrecy, authenticity, and integrity of the information it stores. The existing technologies for secure storage are password based protection systems. However, passwords are vulnerable to impersonation. Passwords can be stolen from memory, from virtual memory backing store, in transit through networks, or can be guessed with dictionary attack. Today, most authenticating applications using passwords are being compromised and the risk is becoming higher because it's becoming easier to download tools that will crack them. Passwords are no longer sufficient, as threats against them increase in large quantity. The increasing expertise of attacks and the professionalism of cyber criminal gangs have led organizations to make passwords longer, or to change them more often. But this will make authorized users act in response by not remembering passwords, or writing them down in a diary or notepad that will compromise security in a different way.

With the growing use of internet to access information resources, government and private agencies are now moving to replace password-based user authentication with stronger, Two-factor authentication systems that strengthen information security. The design behind two-factor authentication is to provide a dual-layered security protection that allows authorized users to securely access their accounts while preventing unauthorized users from illegally accessing other peoples' accounts. Theoretically, this is a good method that many of today's financial organizations use to authenticate their customers over various banking channels. Two-factor authentication requires that two parts of data be accessible, each being from a different category. It is a secure identification process in which the user provides two means of recognition, one of which is normally a physical token, such as a card, and the other of which is typically something memorized, such as a password or PIN number. PIN number [2].

## II. SMART CARD BASED TWO-FACTOR AUTHENTICATION

In this perspective, the two factors involved are considered as “something you have” and “something you know”. A familiar example of two-factor authentication is a bank card: the card itself is the physical entry and the personal identification number (PIN) is the data that goes with it [7]. Smart Cards provide a secure, portable platform for this type of Two-factor authentication systems. Smart Cards could able to carry and operate significant amounts of data, particularly an individual's personal digital identity in a high secure network. Java's portability allows Smart Cards to function as a general-purpose computing platform and makes possible to have a huge market potential for application software and development [5]. With this ability, Smart cards provide a special mechanism to secure access to network based applications within an organization, they help ensure that only individuals with the proper authority can get access to specific network resources, and they reduce the likelihood that hackers can break into a system.

Initially, Public Key Infrastructure (PKI) is the preferred technology for reducing these risks in Smart cards. PKI uses a pair of strong cryptographic keys. With public key cryptography, the private key is always kept in a secure location, while its counterpart, the public key, may be published. Security is maintained as long as the private key is kept secure. Today’s state-of-the-art Internet security techniques such as Secure Sockets Layer (SSL), Digital Signature are all based on public key cryptography. Modern smart cards improve the security and performance through Public Key Cryptography mechanisms by providing secure storage for private keys and accelerating cryptographic operations.

However, these smart card cryptographic systems are vulnerable to traditional mathematical attacks such as Differential and Linear Cryptanalysis attacks. These attacks explore weaknesses in cryptographic algorithms that are represented as mathematical objects. Other form of cryptographic attacks like Differential Power Analysis (DPA) attacks, fault attacks, replay attacks, side channel attacks, etc also exists [3]. Organizations implementing smartcard solutions must realize that these attacks should be counter measured which is an ongoing research that requires more than just a few actions. Hence, a new state-of-the-art design is needed for stipulating the security solutions and to countermeasure the threats.

## III. RELATED WORK

Santhosh Baboo *et al.*[4] have proposed a new scheme to enhance and ensure the remote authentication through secure and dynamic authentication using a smart card. This scheme introduced a dynamic authentication scheme, which includes a number of factors, among which the password, password index, and date of modification were the important factors, which decide the dynamicity in authentication. This dynamic authentication scheme ensures the authentication, confidentiality, reliability, integrity and security in network communications. The security and performance factors to ensure the dynamic mutual authentication and to enhance the security features in authentication for smart card based networks were analyzed using this scheme.

Karen Lu *et al.* [10] have proposed a new online authentication framework that provides security, usability, and ease of deployment. This framework combines the proven hardware security of smart cards and the universal ease of web access through browsers, without imposing the deployment and usability complexities generally ssociated with conventional smart card systems. The resulting authentication solution is applicable to existing smart cards already deployed, intuitive for users and convenient for service provides to both develop and maintain.

Balakumar *et al.*[11] have proposed a secure key generation scheme for cryptography by combining two biometrics features. The biometrics used in this scheme was fingerprint and iris. These two features were combined with the help of a fusion algorithm. From the combined features, cryptographic key was generated.

Yasir Ahmad [12] has proposed a scheme for the implementation of elliptical curve cryptography in smart cards using the concept of Galois Finite Field. With Elliptic Curve Cryptography the time required to produce a key pair is so small that even a component with a very limited computing smart card power can produce the key pair offered a better random number generator is possible.

Guomin Yang et al. [13] proposed a new two-factor smart-card-based password mutual authentication scheme which defines a set of desirable properties to protect against various attacks such as Offline guessing attack and Impersonation attack.

## IV. SECURITY ISSUES ON CRYPTOGRAPHIC SMART CARDS

### A. *RSA Public Key Cryptographic Smart Cards*

The cryptographic strength of the key pairs generated in Smart cards is not very high. Due to lack of computing power, a relatively weak random number source as well as a relatively weak algorithm for selecting large prime numbers is used in RSA Public Key Cryptography based Smart cards. In general, RSA public key cryptosystems involve complex computation such that a separate hardware crypto coprocessor is required. These co-processors took up precious space which adds about 20 to 30% of the cost of the cards.

### B. *Logical Attacks*

With new generation Smart cards and trusted personal devices increasingly connected to networks and providing execution support for complex programs, the prospect of logical attacks has urged the trusted personal devices industry to improve the quality of their software, as logical attacks are potentially easier to launch than physical attacks (for example they do not require physical access to the device, and are easier to replicate from one device to the other), and may have a much wider impact.

An adversary who can introduce computational errors into a smart card can deduce the values of cryptographic keys hidden in the smart card. The surprising part is that an attacker can do this even without precisely controlling the nature of the errors or even the exact timing of the errors. By comparing the result of an erroneous encryption with the result of a correct encryption of the same data, the attacker can learn something about the correct encryption key. By doing enough of these comparisons, the attacker can learn enough information to deduce the entire encryption key.

As the brute-force attack can be performed in most of the standard encryption algorithms, the security of the smart cards become liable. And also, the secrecy is preserved only with the Public and Private keys and not on the encryption algorithms. Therefore, the Smart card security could not be effectively implemented with cryptographic systems. Hence, an alternative approach is to be considered.

## V. PROPOSED GENERIC FRAMEWORK

Even though Cryptographic systems are specifically designed for smart card security, there is no such thing as perfect security. Every new security design will eventually face its threats. There is no easy recipe to counteract smartcard security threats, but it is possible to minimize the risks.

Our research proposes a Cryptographic Smart card technology embedded with Steganographic techniques and a stronger two-factor authentication, which are now considered more secure than Cryptographic Smart card. The challenging factor of Steganography is that the existence of hidden key or password in the image is not known by perceiving it with the naked eye [14]. The generic framework for the first factor authentication is shown in the Fig. 1 as an integrated Smart Crypto-Stegano Card. The first step of process is based on a One-Time Password (OTP) created with a Random Number Generator. The OTP is unique for each individual user and is generated from the PIN given by the user. The user ID and this OTP are then encrypted with the standard public key encryption algorithm – Elliptic Curve Cryptography [12] using the public key of the receiver. The encrypted data (Enciphered Password) are then hidden into the digital photo image of the user with a new data hiding technique – Replacement of Selective pixels. The resultant photo image i.e. Stego-image is then embedded into the Smart card.

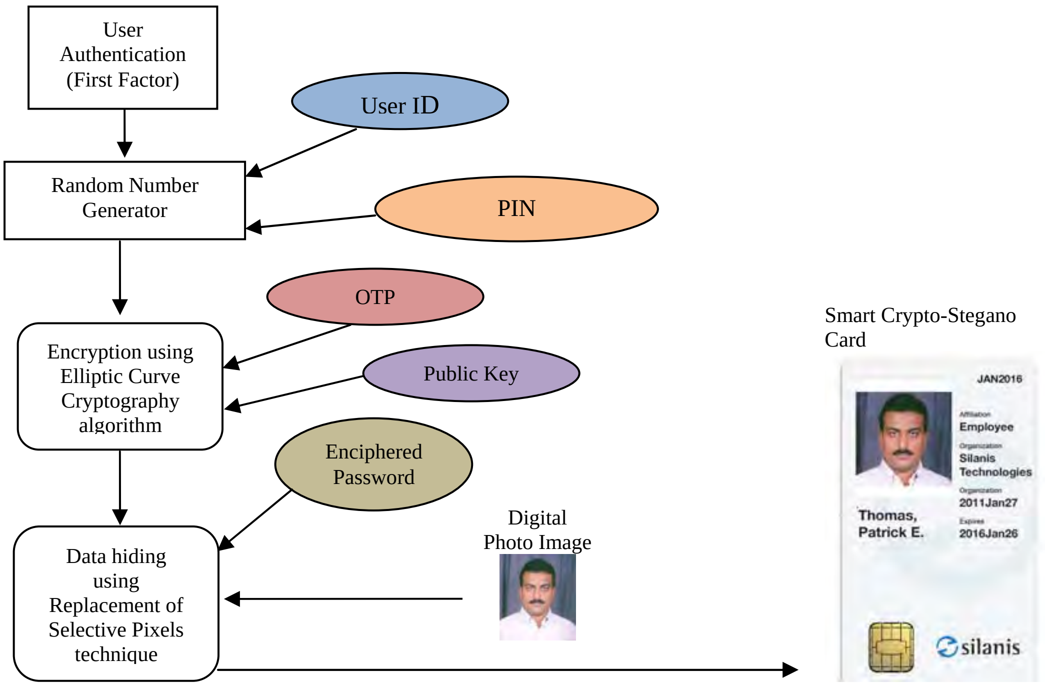
User Authentication (First Factor)
User ID
Random Number Generator
PIN
OTP
Smart Crypto-Stegano Card
Encryption using Elliptic Curve Cryptography algorithm
Public Key
Enciphered Password
Digital Photo Image
Data hiding using Replacement of Selective Pixels technique
JAN2016
Employee
Silanis Technologies
2011Jan27
Thomas, Patrick E.
2016Jan26
silanis

Fig.1. First Factor Authentication – Process of creating Smart Crypto-Stegano Card

The digital stego-image of the users are now stored in the smart card chip. The second factor authentication integrates a biometric sensor with a smart card reader as shown in Fig. 2, which provides additional level of security to the system [11]. The biometric sensor takes a digital photograph of the user and then the captured digital image is compared with the stego-image stored on the smart card. If the captured biometric matches the biometric stored on the card, the smart card then extracts the secret information required to log the user onto the network. Smart card technology – typically used in conjunction with steganography makes logical access more secure. Two-factor authentication with smart cards provides stronger security than simply entering valid credentials. The smart cards provide non-repudiation – two-factor security authenticates user unambiguously – and therefore guarantee integrity and security.

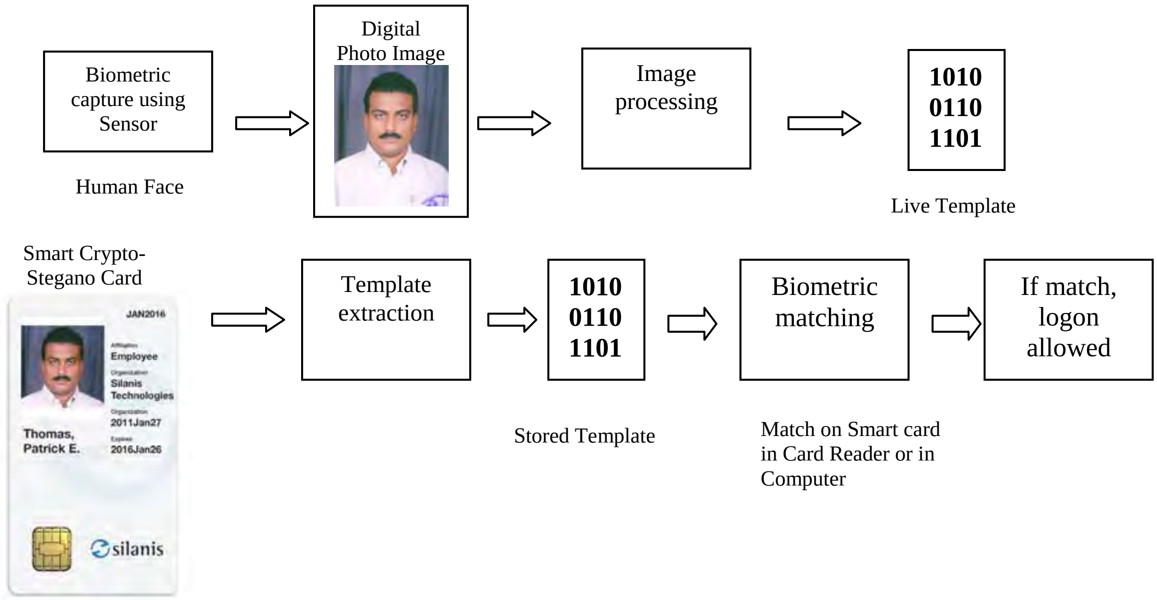

Fig.2. Second Factor Authentication – Integration of Biometrics system

## VI. Conclusion

The expected outcome is a new Smart Crypto-Stegano card with a strong Two-factor authentication. Smart card technology – typically used in conjunction with steganography makes logical access more secure. Two-factor authentication with smart cards provides stronger security than simply entering valid credentials. The smart cards provide non-repudiation – two-factor security authenticates user unambiguously – and therefore guarantee integrity and security. As the encryption algorithm and the data-hiding technique are new, any malicious users and hackers could not attack the security system.

However some issues will arise which relates to the complex infrastructure and Token life-cycle cost. The future work proceeds with the multi-function capability of the smart card and to provide Credential security for biometric template. Currently there is no smart card support available with the Linux kernel. The open source world provides greater choice for implementing high-level functionality, but many of the tools are somewhat duplicative. It is proposed to develop a supporting tool for Linux based Smart card Security Systems and the research effort would took place in future for a more appropriate solution.

## References

[1] K C Leung, L M Cheng, A S Fong, C K Chan, "Cryptanalysis of a Modified Remote User Authentication Scheme Using Smart Cards," *IEEE Trans. Consum. Electron*, vol. 49, pp. 1243-1245, Nov. 2003. .

[2] Available: http://www.howtodothings.com/business/how-to-learn-about-two-factor-authentication

[3] Thomas S. Messerges, Ezzat A. Dabbish, Robert H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks", *IEEE Transactions on Computers*, vol. 51, No. 5, pp. 541-552, May 2002.

[4] S. Santhosh Baboo, K. Gokulraj, "An Enhanced Dynamic Mutual Authentication Scheme for Smart Card Based Networks", *International Journal of Computer Network and Information Security*, Vol. 4, No. 4, pp.30-38**,** May 2012.

[5] Available: http://people.cs.uchicago.edu/~dinoj/smartcard/applications.html

[6] Available: http://www.smartcardalliance.org/newsletter/february_2005/feature_0205.html

[7] Available: http://searchsecurity.techtarget.com/definition/two-factor-authentication

[8] Zuowen Tan, "An Authentication and Key Agreement Scheme with Key Confirmation and Privacy-preservation for Multi-server Environments", *Journal of Computers*, vol. 6, No. 11 (2011), pp. 2295-2301, Nov 2011.

[9] Wenbo Shi and Peng Gong, "A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", *International Journal of Distributed Sensor Networks*, Vol. 2013 (2013), Article ID 730831, 7 pages.

[10] Karen Lu, Asad Ali, Kapil Sachdeva and Ksheerabdhi Krishna, “A Pragmatic Online Authentication Framework using Smart Cards,” in *Proc. SERVICE COMPUTATION’11*, 2011, p. 84-91.

[11] Balakumar and Venkatesan, “Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris,” in *Proc. IJCSI’11*, 2011, p. 349-356**.**

[12] Yasir Ahmed, “A study on the application of Elliptic - Curve Cryptography in implementing smart cards,” *International Journal of Modern Engineering Research*, vol. 2, pp. 155-159, 2012.

[13] Guomin Yang, Duncan S.Wong, Huaxiong Wang and Xiaotie Den, “Two-factor mutual authentication based on smart cards and passwords”, *Journal of Computer and System Sciences*, vol. 74, pp. 1160–1172, 2008.

[14] Graeme Bell and Yeuan-Kuen Lee, “A Method for Automatic Identification of Signatures of Steganography Software**”,** *IEEE Transactions on Information Forensics and Security*, vol. 5, No. 2, pp. 354-358, June 2010.

[15] Antonio Savoldi and Paolo Gubian, “Data Hiding in SIM/USIM Cards: A Steganographic Approach,” in *Proc. SADFE'07, IEEE Computer Society*, 2007.