Implementation of Security in FPGA using Hybrid Combination of AES and Simple biometric Key

M. Vasantha
faculty; Electronics and Commmunication
dept-University college of Engineering-Ariyalur.

S.Anantharaj
Electronics and Commmunication
dept-University college of Engineering-Ariyalur.

M.Chandrasekar
Electronics and Commmunication
dept-University college of Engineering-Ariyalur.

P.Kalimuthu
Electronics and Commmunication
dept-University college of Engineering-Ariyalur.

Abstract— The objective of this research proposal is to design new bio metric security protocol using hybrid encryption system. The hybrid encryption technique is a combination of both symmetric and asymmetric cryptographic techniques. The security of bio-metric information transfer through unreliable channel is challenging, because of external attacks. Therefore, Security of biometric information is essential requirement in this current trend and technology. The various protocols such an AES, DES, 3 DES are currently using biometric solution. But, the key distribution and encryption and decryption cycle is major problem. The new protocol solves make more secure an easy to encrypt and decrypt the data. Thus, in this paper, we propose new efficient and effective mechanism for confidentiality and authentication for biometric security system by using AES and simple symmetric key algorithm. Also it examines the possibility of using a combination of biometric attributes to overcome common problems in having a biometric scheme for authentication. It also investigates possible schemes and features to deal with variations in Biometric attributes.

Keywords— Biometric, RSA, AES, DES, Triple DES, SSK, Encryption, Decryption

I. INTRODUCTION

Cryptography is the science and art of secret writing that it cannot form without creativity actions with entrepreneurial talent . It studies some mathematical techniques and provides mechanisms necessary to provide aspects related to information security like confidentiality, data integrity, entity authentication, and data origin authentication. Biometric cryptography comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. Hybrid model biometric system offers several advantages compared to other symmetric security systems. First, any bird system can increase the reliability of the verification process. Second, a hybrid system can capture the unique, biometric characteristics of a much larger and more varied target population. Third, the system is much more difficult to spoof than a single biometric system. Symmetric algorithms are cryptosystems that either a secret key will be shared for both encryption and decryption .The algorithms of symmetric cryptosystems are very strong against possible attacks, but mainly weakness of symmetric cryptosystems is brute- forcing the secret key. This characteristic creates the biggest critical act in any cryptosystem that uses symmetric algorithms which is distribution of the shared secret between the two parties like DES algorithms .Asymmetric algorithms use different values for encryption and decryption and do not need to share secret between two parties. Each party only has to keep a secret of its own. The earliest foundation of asymmetric algorithms known as public key cryptosystems comes from key exchange problem of symmetric algorithms. AES is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. AES stands for Advanced Encryption Standard who first publicly described the algorithm in 1977. The AES cryptography algorithm using in various application in the security aspects.

II. PREVIOUS WORKS

The main problem of asymmetric cryptography is the management of private key. No one should be able to access Someone else's private key. They need to store in such a place which is protected from unauthorized accessing. This is vulnerable for attacking by hackers. This creates big problem in asymmetric cryptography. Thus it can be solved by the use of biometric template. Private Key can be generated directly by the biometric template. Since private key can be generated dynamically from one's biometric template, so there is no need to store private key anymore and network becomes more secure and safe. But there are very little work has been done in the field of AES with the help of biometric. Some of the suggested approaches are given. However these biometrics have lots of issues regarding training, capturing image, easily obscured by eyelashes, eyelids, lens and reflections from the cornea, lack of existing data deters ability, cost, voice can be captured while uttering the password, a camera can photograph an iris from across the room, and fingerprints left on surfaces can be lifted hours later etc. For some individuals, the iris image capturing is very difficult. Iris recognition system requires lots of memory to be stored. It is easily absurd by eyelash, eyelids, lens and reflection from the cornea. People are not much familiar with iris recognition system yet, so there are lots of myths and fears related to scanning the eye with light source. Iris recognition system works on the basis of

acquisition of iris image, but acquisition of an iris image needs more training and attractiveness than most other biometrics. It cannot be verified by human too. The most problem with iris recognition system is its expensiveness. I have generated cryptographic key from user's face features and then the key has been applied in DES algorithm for encryption and decryption purposes and same way it have generated cryptographic key from user's voice while speaking a password[13], but no further implementation of key has been described on their paper. Related application are as palm vein print is extremely difficult to forge and therefore contributes to a high level of security, because the technology measures hemoglobin flow through veins internal to the body. We are generating cryptography keys from user's palm vein and then the generated key are used as user's secret keys for AES. Hence in proposed method we are using palm vein as a secret key instead of the biometric.

III. Biometric Security Consideration

While potentially offering significant security benefits, a biometric system is only one of many security tools available. Depending on the application, an environment or circumstance may or may not benefit from a biometric system. Understanding the operational requirements of the situation is necessary to determine if a biometric system can be used to meet a security need. The use of biometrics will not solve all of a system's security problems, but when properly implemented, a biometric system should be one part of overall security architecture. There is no single biometric modality that is best for all applications. Many factors must be taken into account when implementing a biometric system including location, security risks, task, expected number of users, user circumstances, existing data, etc. It is also important to note that biometric modalities are in varying stages of maturity and therefore may offer varying levels of security, ease of implementation, and user convenience. Biometric systems alone do not currently provide adequate security for high assurance applications. When biometric systems (something you are) are combined with other security mechanisms (something you have and something you know), those systems can provide significant security benefits. However, the biometric system must be implemented correctly for the specific application.

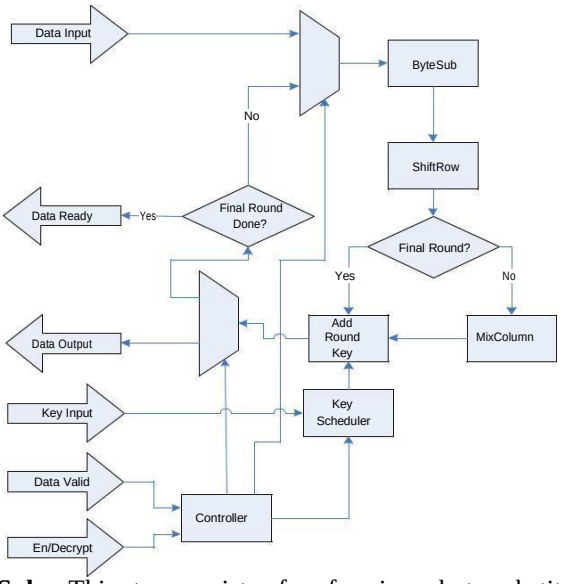
IV. Biometric-based Security Approaches for Data Authentication

Biometric is a technique commonly known as the automatic identification or verification of an individual by his or her physiological or behavioural characteristics. Biometric approach uses an intrinsic characteristic of the human body as the authentication identity to secure the distribution of a cipher key within NOC communications. Because of the data that are detected, collected and transmitted in NOC is comparatively sensitive, an ideal biometric trait should present 100% reliability, user friendly, fast operation and low cost. Besides, itis postulated that the utilized biometric should satisfy the following properties indicated in TABLE 1.

TABLE 1 BIOMETRIC PROPERTIES

Properties	Description
Universal	Possessed by the majority, if not the entire population.
Distinctive	Sufficiently different in any two individuals.
Permanent	Sufficiently invariant, with respect to the matching criterion, over a reasonable period of time.
Collectable	Easily collected and measured quantitatively.
Effective	Sufficiently invariant, with respect to the matching criterion, over a reasonable period of time.
Acceptable	Yield a biometric system with good performance that is given limited resources in terms of power consumption, computation complexity and memory storage, the characteristic should be able to be processed at a fast speed with recognized accuracy.
Invulnerable	Relatively difficult to reproduce such that the biometric system would not be easily circumvented by fraudulent acts.

V. Proposed System



ByteSub – This step consists of performing a byte substitution using an S-box. The substitution is defined as a transformation on GF(2^8), but will be implemented in hardware using a lookup table.

ShiftRow – This step performs a cyclical shift over the four rows of data. Each row is shifted by a different amount, depending on the block length.

MixColumn – The step performs operations on the columns of data. Each column is multiplied with a fixed vector and the result is computed mod $x^4 + 1$.

Add Round Key – This step is simply the XOR combination of the data with the current round key. The round key is computed from the encryption key based on the key scheduler algorithm.

Key Scheduler – The key scheduler uses the encryption key generate several different keys used for the different rounds of encryption. The key scheduler consists of two parts, key expansion and round key selection. Key expansion is used to generate a much longer expanded key from the encryption key. The round key selection is used to extract bits from the expanded key during each round to be used for the round key. The expanded key is long enough that the key selection is able to pull different bits from the expanded key for each round.

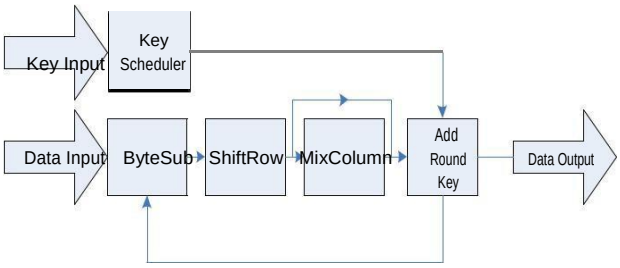
Controller – The controller will be responsible for tracking the current round of encryption/decryption, controlling the

order of the keys produced by the key scheduler, and for selecting what source to accept data from at the beginning of each round (either from the user supplied data or the output of the previous round.) The controller will wait until the data valid signal is received to begin operating, and will make sure that the data ready signal is set after the operations have been completed.

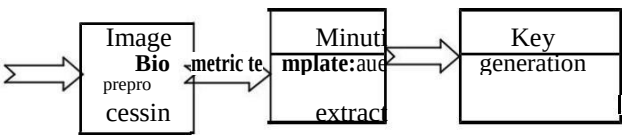
Simplified Block Diagram

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi resolution TIFF or EPS file with all fonts embedded) because this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on your frame, use the MSWord ―Format ‖ pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.



Simple block for key generation:



The image received from the biometric scanners.

Image pre-processing: The template from the biometric scanner is undergoes to Histogram equalization, Wiener filter, image enchancement, normalization, binarization, thinning.

Minitiau extraction: From local 2D field Estimation,the ridge and bifurcation from template is identified.

Key generation: By using cross number method,,the key is generated from the template image.

VI. Conclusion

In this paper, a biometric-FPGA based security framework is proposed for data authentication within NOC. Specifically, the sender's key feature is selected as the biometric key for data authentication mechanism within NOC system. The main goal of the current research is to develop new methods, algorithms and software tools for designing biometric based high level security systems. The security system in NOC must be implemented with low computational complexity and high power efficiency. In this proposed approach, low cost authentication challenges are addressed specifically by using biometric information instead of cryptographic key distribution. Thus, it will certainly save resources while adequate security measures are employed.

References

1) Sonam Shukla,Pradeep Mishra, ―A Hybrid Model of Multimodal Biometrics System using Fingerprint and Face as Traits‖,

2) Arun Rossa, Anil Jaina, James Reismanb, "A hybrid Fingerprint matcher", 2003 Published by Pattern Recogninition, Elsevier Science Lt
36 (2003) 1661 – 1673, Elsevier Publication.

3) Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi, "Implementation ofSecurity through simple symmetric key algorithm based on modulo 37", International Journal of Computers & Technology www.ijctonline.com ISSN: 2277-3061 Volume 3 No. 2, OCT, 2012.

4) Shweta Malhotra, Chander Kant Verma , "A Hybrid Approach for Securing Biometric Template", International Journal of Engineering and Advanced Technology (IJEAT),.

5) Lin, H. S., "Cryptography and Public Policy, Journal of Government Information", (1998) 135–148.

6) Alia, M.A., Yahya, A., "Public–Key Steganography Based on Matching Method", European Journal of Scientific Research,(2010) 223-231.

7) S. Mohammadi, S. Abedi, *"ECC based Biometric Signature: A new approach in electronic banking security"*, International Symposium on Electronic Commerce and Security (ISECS'07), doi:10.1109/ISECS.2008.98, pp. 763-766, 2008.

8) William Stallings, *"Cryptography and Network Security Principles and Practices"*, PEARSON Prentice Hall, Edition Fourth, 2007.

9) C. Nandini and B. Shylaja, *"Efficient Cryptographic key Generation from Fingerprint using Symmetric Hash Functions"*, International Journal of Research and Reviews in Computer Science (IJRRCS), Vol.2, No. 4, August 2011.

10) H.X.Mel,Doris Baker, *"Cryptography Decrypted"*, Addision-Wesley, Edition 2011.

11)SNAC, *"Biometrics Security Considerations"*, Systems and Network Analysis Center Information Assurance Directorate, www.nsa.gov/snac.

12)C. C. Y. Poon, Y.-T. Zhang, and S.- D. Bao, *"A novel biometrics method to secure wireless body area sensor networks for telemedicine and mhealth"*, IEEE Communications Magazine, vol. 44, no. 4, pp. 73–81,2006.