International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Bio-Key Generation for Integrity Checking Using Elliptic Curves in Fingerprint Verification System

V. Rekha, V. Kavitha

Abstract*: This paper proposes a Bio-key generation method for integrity checking in fingerprint verification system. A major drawback in traditional cryptography is random key generation and those keys need to be remembered by the user. To overcome such drawback the crypto-Bio-key generation system is introduced. In this system, there are three process to follow. Initially, a revocable transformation of the compressed fingerprint feature data using transformation key for security enhancement. Secondly, the key exchange technique using Elliptic curve cryptography (ECC) to generate secret key. Finally SHA256 hash function generates the Bio-key for high level integrity checking.

***Index Terms*: Bio-key, ECC, key exchange, revocable transformation, SHA256.**

I. INTRODUCTION

A. Background

Bio-key generation strengthen the security of the verification system. Traditionally, the crptography is an efficient approach for secure transmission but it faces difficulties in memorizing the random keys. The key generation from the biometric data overcome such limitations. Fingerprint is one of the type of biometric system to achieve best verification as compared to iris, face etc. With the widespread use of data exchange across the net, and also the storage of sensitive information on open networks, cryptography is changing into associate degree progressively vital feature of knowledge security several cryptologic algorithms are out there for securing information E.g. RSA, DES, AES etc. A crypto graphical approach ties knowledge protection mathematically to the key that's used to guard it [1]. This enables data owner to possess complete management over one's personal information while not hoping on, or relinquishing management to a third party authority [2].The key generation of biometric cryptosystem combines a high level security that's provided by cryptography and non-repudiation provided by bioscience [3-4]. It produces a stable crypto graphical key that's extracted from biometric knowledge although, a number of the intruders may try and hack the bio-key throughout identification and verification method [5-8]. Thus, it's not a pure authentic system. So, it needs a complicated Bio-key generation for security. Therefore, in our analysis work, the Elliptic Curve Cryptography (ECC) Bio-key generation is employed for removing all the constraints that are listed above. Biometric recognition systems may be known by eight attainable attack. These impact points, are wide divided into 2 main groups: - Direct attacks and indirect attacks. Key generation could be a vital a part of recognition system. The biometric system is reliable one, thanks to the distinctiveness within the individual options. The biometric system is a lot of correct and secure one. Additionally to, the biometric system could be a sensible quantifiability mechanism during which the login method may be created by such quite biometric system that can't be hacked by somebody. The user's identity are lost if the user compromises the first biometric info. Biometric systems that mix statistics with cryptography key generation are referred to as Bio-key generation. To ensure secure transmission, cryptological key plays a serious role [9,10]. If we have a tendency to introduce biometric with the key, it guarantee a lot of authentication throughout transmission. The integrity checking is applied mistreatment computer code Bio-key generation

B. Related Works

A Fuzzy vault crypto-biometric system was developed by Enbo et al. [11] to save the stored fingerprint. The sharing operation taken over based on geometric hashing. To ensure security, a new decoding algorithm along with Fuzzy vault was proposed, which protect the fingerprint template. Their work uses non-invertible transformed version on the biometric data for biometric authentication [12]. Instead of password, the smart system uses fingerprint for authentication. Here also, the authors used fuzzy vault system for security system. Both the security level and verification accuracy are taken into account. The fingerprint alignment problem is rectified with the help of geometric hashing [13]. Barman et al. [14] used Crypto-biometric system to avoid remembering the key in the user side. For that, the keys are generated from the biometric data. So the user no need to remember his random key. It is called as revocable key generation. The same principle is carried out by Neethu and Ali Akbar [15] but keys are generated from the fingerprint template. Shuffle key and hash function are also used for increasing security.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
V. Rekha*, Department of Computer Science, Ponjesly College of Engineering, Anna University, Chennai 600025, India
Dr. V. Kavitha, Department of Computer Science, University College of Engineering, Tamil Nadu, India

A blind authentication scheme was proposed by Upmanyu et al. [16] to provide security, privacy and revocability.

C. Contributions

The significant contribution of this integrity checking security system is the Bio-key generation. In order to generate the Bio-key, revocable transformation, key exchange based on ECC and hash function are contributed. This significantly improves the security of the system.The remaining section of the manuscript is prepared as follows. In section II, the system for integrity checking is elaborated with scientific representations. It describes mainly the Bio-key generation using ECC. Section IV illustrates the result and discussion for the proposed integrity system model. Finally the paper concludes in section V.

II. ECC KEY EXCHANGE AND BIO-KEY GENERATION FOR INTEGRITY CHECKING

Secure communication is the most prominent means in every day to day circumstances. Fingerprint verification system is our study area. In order to improve the security system, integrity checking is the most secular way to communicate between a client and the server. During communication, there may be some possibility to hack user's genuine public key. At that time, replay attack plays a role in such situation and the attacker derive the keys. In order to overcome such situation, deriving keys from biometric data can avoid the possibility of replay attack. In our work, the cryptographic key exchange and the Bio-key generation from the cryptographic keys and fingerprint data extremely makes the integrity checking and performs secure transmission.

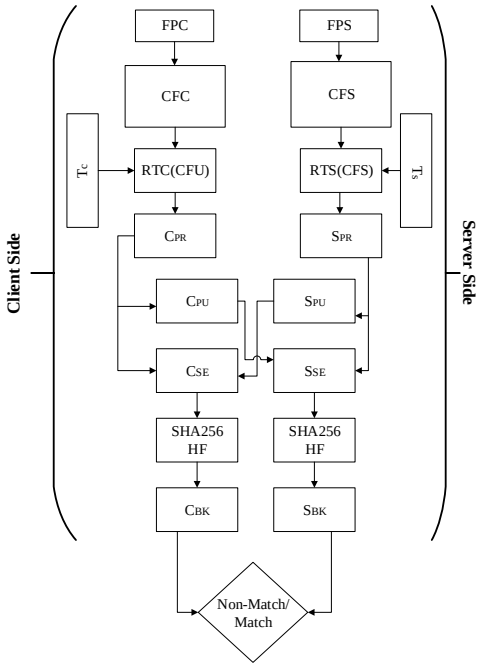

Fig. 1.Flow chart of integrity checking via Bio-key.

Fig.1 shows the flow of the proposed system for integrity checking. The variables given in the flow chart is given as follows: FPC-Finger print of client, FPS-Fingerprint of server, CFC-Compressed Fingerprint feature data obtained from client fingerprint, CFS-Compressed fingerprint feature data of server, T_C-Transformation key of client, T_S-Transformation key of server, RTU(CFU)-Revocable transformation in the client side, RTS(CFS)- Revocable transformation in the server side, C_{PR}-Private key of client, S_{PR}-Private key of server, C_{PU}-Public key of client, S_{PU}-Public key of server, C_{SE}-Secret key of client, S_{SE}-Secret key of server, SHA256 HF-SHA256 Hash Function, C_{BK}-Bio-key of client, and S_{BK}-Bio-key of server. In both the client and server side, the following process is carried out. First the given fingerprint input data is applied to an average filtering, after filtering the ridge features can be extracted. Those feature data is compressed using Pattern Optimization from Subset Tree (POST) compression scheme []. The compressed fingerprint feature data is taken for the integrity checking. The procedure for the integrity checking is detailed in the subsections.

A. Revocable Transformation

A transformation key is used to shuffle the compressed fingerprint feature data. Instead of processing the original feature data, the revocable transformation increase the security. The reversible transformation is applied on compressed fingerprint feature knowledge on the user-specific key to supply a resuscitate to the feature data. This user-specific key's aforesaid to be a change key for the user. The transformation key's used because the seed price to create the approximate range of the alternate feature knowledge. The bits related to this random range begin from the start and are changed with bits within the levels that increase with every random number.

B. ECC Key Exchange

ECC is an asymmetric cryptographic algorithm uses both the private and public key to ensure authentication. A private key is generated from the revocable transformed compressed fingerprint data *RT(CF)*. From that private key, a public key is generated. By exchanging the public key between the client and the server along with their own private key, a secret key is generated.

1) *Private Key and Public key:* The private key C_{PR} and $S_{PR}$of the client and server are produced from the RT(CF). From the private key and the generator point P generated from the elliptic curve, the public keys C_{PU} and S_{PU} are generated as:

$$P \times C_{PR} = C_{PU} \quad (1)$$

$$P \times S_{PR} = S_{PU} \quad (2)$$

2) *Secret Key:* The secret key is generated by exchaning the keys. Thus the secret keys produced are C_{SE} and S_{SE}.

$$S_{PU} \times C_{PR} = C_{SE} \quad (3)$$

$$C_{PU} \times S_{PR} = S_{SE} \quad (4)$$

ECC provide excellent key exchange than the RSA algorithm in terms of attacks.

C. SHA256 Hash Function

The secret key generated from the ECC is given to SHA256 hash function for Bio-key generation. Initialization, padding and hash calculation are the steps of hash function.

D. Bio-key

The output of the hash function is the bio-key. This keys can be used for integrity checking.Thus the proposed integrity system model will avoid the replay attack and provide secure communication.

Algorithm 1: Bio-key integrity checking
Input: CF
Output: Bio-key
Revocable Transformation of CF: RT(CF)
Key Exchange and Secret Key Generation
Step 1: Choose C_{PR} & S_{PR} from RT(CF)
Step 2: Choose C_{PU} & S_{PU} from C_{PR} & S_{PR} and P
Secret key generation by key exchange
Step 3: Exchange C_{PU} to S_{PU} & S_{PU} to C_{PU}
Step 4: Generate Secrete key of client and server C_{SE} & S_{SE} from C_{PR}* S_{PU} & S_{PR} & C_{PU}
SHA256 for Bio-key generation
Input: Secrete key of client and server C_{SE} & S_{SE}
Step 1: Initialize hash values
Step 2: Initialize array of spherical constants
Step 3: Pre-processing (Padding)
Step 4: Method the message in consecutive 512-bit chunks
Step 5: Extend the primary sixteen words into the remaining forty eight words
Step 6: Initialize operating variables to current hash worth
Step 7: Add the compressed chunk to the present hash worth
Step 8: Manufacture the ultimate hash worth (256-bit message digest (Bio-key))

III. EXPERMENTAL RESULTS AND DISCUSSION

The evaluation for the key exchange and Bio-key generation is simulated in the MATLAB platform. To ensure the security of the Bio-key, it is verified by two possible attacks. Attack 1 called as fake fingerprints and attack 2 called as real fingerprints. Two flat sensors known as optical and capacitive and one sweep sensor, so totally three sensors are considered with the two attacks.

A. Detection Error Tradeoff (DET) Analysis

The DET performance curve is plotted to show the performance of the Bio-key integrity checking for different sensors. The error between the false acceptance rate and the false rejection rate is measured in terms of DET curves.

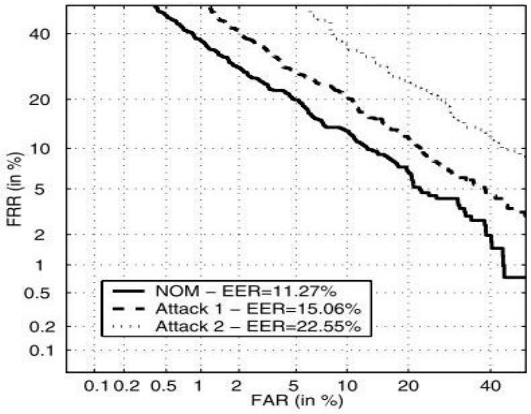

Fig. 2.Performance Interms Of DET Curves For Testing In Optical Sensor.

Fig. 2 shows the Equal Error Rate (EER) performance of our proposed integrity checking in optical sensor. As compared to the normal operation mode (NOM), EER performance for the attack 2 is almost minimum near to the NOM. But it fails in attack 2.

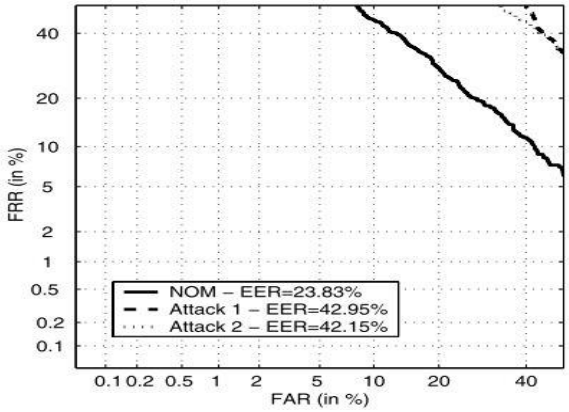

Fig. 3.Performance interms of DET curves for testing in Capacitive sensor

Capacitive sensor have more error value as compared to the optical as given in Fig.3. The NOM of optical is 11.27% but the capacitive have NOM very high in the range 23.83%. The performance is almost similar for both the attacks.

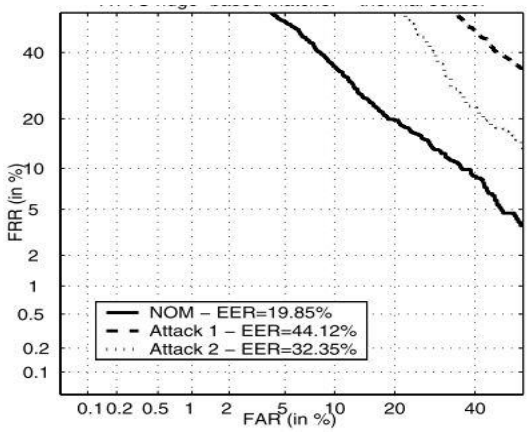

Fig. 4.Performance interms of DET curves for testing in Thermal sensor

The noise component in Thermal is low as compared to capacitive but high than optical. Attack 2 achieves better than that of attack 1 is shown in Fig. 4. The possible types of attacks are limited using the proposed Bio-key.

IV. CONCLUSION

Key generation and its security analysis are the primary issues to be follow in a security system. In this way, our system proposes a Bio-key generation method for integrity checking. The combination of revocable transformation, key exchange and hash function generated a Bio-key to overcome the security issues. The Bio-key has the capacity to avoid the replay attack.

REFERENCES

1. S. Barman, S. Chattopadhyay and D. Samanta, "An approach to cryptographic key distribution through fingerprint based key distribution center," 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, 2014, pp. 1629-1635.
2. S. Barman, S. Chattopadhyay and D. Samanta, "Fingerprint based symmetric cryptography," 2014 International Conference on High Performance Computing and Applications (ICHPCA), Bhubaneswar, 2014, pp. 1-6.
3. R. Ranjan and S. K. Singh, "Improved and innovative key generation algorithms for biometric cryptosystems," 2013 3rd IEEE International Advance Computing Conference (IACC), Ghaziabad, 2013, pp. 943-946.
4. A. Bhatega and K. Sharma, "Secure cancelable fingerprint key generation," 2014 6th IEEE Power India International Conference (PIICON), Delhi, 2014, pp. 1-4.
5. A. S. Andalib and M. Abdulla-Al-Shami, "A novel key generation scheme for biometric cryptosystems using fingerprint minutiae," 2013 International Conference on Informatics, Electronics and Vision (ICIEV), Dhaka, 2013, pp. 1-6.
6. A. Sarkar and B. K. Singh, "Cancelable biometric based key generation for symmetric cryptography," 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 2017, pp. 404-409.
7. G. Panchal and D. Samanta, "Comparable features and same cryptography key generation using biometric fingerprint image," 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2016, pp. 691-695.
8. Lin You, Guowei Zhang and Fan Zhang, "A fingerprint and threshold scheme-based key generation method," 5th International Conference on Computer Sciences and Convergence Information Technology, Seoul, 2010, pp. 615-619.
9. A. Sarkar and B. K. Singh, "Cryptographic key generation from cancelable fingerprint templates," 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Dhanbad, 2018, pp. 1-6.
10. A. Sarkar, B. K. Singh and U. Bhaumik, "RSA Key Generation from Cancelable Fingerprint Biometrics," 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, 2017, pp. 1-6.
11. F. Enbo, H. Caiyun and L. Jiayong, "Auto-aligned sharing fuzzy fingerprint vault," in China Communications, vol. 10, no. 10, pp. 145-154, Oct. 2013.
12. Daesung Moon, Sungju Lee, Yongwha Chung, Sung Bum Pan and Kiyoung Moon, "Implementation of automatic fuzzy fingerprint vault," 2008 International Conference on Machine Learning and Cybernetics, Kunming, 2008, pp. 3781-3786.
13. H. Choi, S. Lee, D. Moon, Y. Chung and S. Pan, "Secret Distribution for Secure Fingerprint Verification," 2008 International Conference on Convergence and Hybrid Information Technology, Daejeon, 2008, pp. 535-540.
14. S. Barman, D. Samanta and S. Chattopadhyay, "Revocable key generation from irrevocable biometric data for symmetric cryptography," Proceedings of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT), Hooghly, 2015, pp. 1-4.
15. C. Neethu and Ali Akbar N, "Revocable Session Key Generation Using Combined Fingerprint Template," 2018 International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT), Kannur, 2018, pp. 584-588.
16. M. Upmanyu, A. M. Namboodiri, K. Srinathan and C. V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 255-268, June 2010.
17. V. Rekha, V. Kavitha, "Efficient low bit rate image coder for fingerprint image compression", Journal of Information Science and Engineering, vol. 34, no. 6, pp. 1561-1578, 201

AUTHORS PROFILE

V. Rekha received her B.Sc, M.C.A. and M.Phil degrees in Computer Science, Computer Applications and Computer Science from Manonmaniam Sundaranar University, Tirunelveli, Anna University, Chennai and Manonmaniam Sundaranar University, Tirunelveli in 2003, 2006 and 2007 respectively. She joined Pon- jesly College of Engineering as a Lecturer in 2006 and then became an Assistant Professor in 2007. She is currently working towards Ph.D. degree in Computer Science at Ponjesly College of Engineering. Her research work includes biometrics, image compression, cryptography.

V. Kavitha obtained her B.E. degree in Computer Science and Engineering in 1996 from the Noorul Islam College of Engineering and M.E. degree in Computer Science and Engineering in 2000 from Mepco Schlenk Engineering College. She received Ph.D. degree in Computer Science and Engineering from Anna University, Chennai in the year 2009. Right from 1996, she is in the Department of Computer Science and Engineering under various designations. Presently she is working as an Professor and Head in the Department of Computer Science and Engineering at University College of Engineering, Kancheepuram, Tamil Nadu, India. Her research interests are network security and cloud computing.