

Cryptography based Internet Security ATM System using Fingerprint for securing PIN

Richa Agrawal^[1], Dr. Brajesh Kumar Singh^[2], Dr. Lavkush Sharma^[3]

^[1] M. Tech.Scholar, ^[2] Professor, C.S.E. Department, R.B.S. Engineering Technical Campus, Bichpuri, Agra, U.P., India, ^[3] Associate Professor, C.S.E. Department, R.B.S. Engineering Technical Campus, Bichpuri, Agra, U.P., India

ABSTRACT

Today, ATMs (automated teller machines) are used in a variety of ways, including: you can withdraw cash, transfer cash, check your balance, get an account summary, and more. The main component here is security, to maintain the security we prefer cryptography and biometrics. Cryptography is a state-of-the-art technique for increasing security. Using cryptography and biometrics together creates a bio cryptographic system. Since the private key is an important component of encryption, here one is the main task to secure the private [1] key. To overcome this issue, we use a biometric fingerprint image. However, biometrics cannot protect anyone's fingerprint template because of the many suspected attacks. Therefore, we use a fuzzy vault system that combines cryptography [2] and biometrics [4] to ensure that only authorized users can use their passwords and PINs with the legal data.

Keywords: Biometrics, Cryptography, Fuzzy vault system, IP security, Java Applets.

1. INTRODUCTION

In today's era, we have three security goals called CIA: Confidentiality, Integrity and Availability. However, our security will be becoming challenging that time when any intruder tries to create some noise or try to induce the error bits. Today's era requires reliable data protection and identity management mechanisms. Cryptography is one of modern techniques which provide security. There are two types of attacks that impostors do, in the passive attack the intruder can steal the information but in the active attack the intruder can modify the details of the user. We use encryption techniques on one side and decryption [1] at the other side to prevent such kinds of frauds. We have techniques like: traffic Padding, Digital signature, stenography, encipherment, access control etc.

We have two types of keys to prevent these fraudulent activities mentioned in the below figures:

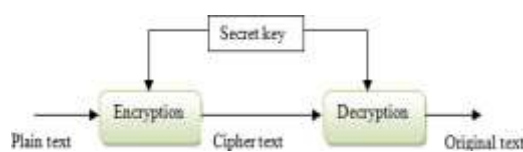


Figure 1: Symmetric Cryptography

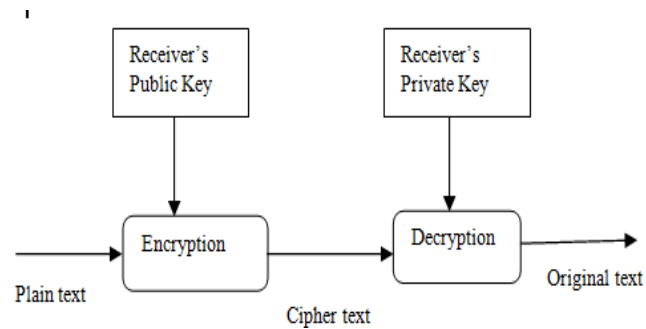


Figure 2: Asymmetric Cryptography

Symmetric key cryptography is also known as secret key cryptography. We use one secret key at both ends as illustrated in figure 1. On the other hand, figure 2 depicts the asymmetric key cryptography, we use two keys: public at one end and private at another end.

There is an RSA algorithm for asymmetric key cryptography that builds the mathematical foundation; on the other hand we use DES and AES algorithms in the symmetric key cryptography which tells about the substitution and permutations of the information bits.

RSA is more complex than the DES and AES however it provides more security than the DES and AES.

Furthermore, if we needed the higher security then the keys could be random, unique and long so that the inducer can't identify the pattern of the key. However, this makes it difficult for users to remember such long keys, so they need to be stored on computers, mobiles, smart cards and so on. Therefore, you can get the key through pass code protected data. Pass codes could easily be guessed, identified and shared. Biometric property is something which has the physiological and behavioral characteristics of an individual's identity. Biometrics uses human fingerprints, irises, faces, and veins. Biometrics uses the user's fingerprint pattern and is more secure than password-based authentication because each user has a unique pattern. We use biometric authentication and cryptography for information security. However, now the intruder steals the fingerprint pattern by the attack and they are replacing their pattern to access the information.

Thus, biometrics and cryptography each have their strengths and weaknesses, and to overcome this problem, a bio-crypto system that combines cryptography and biometrics to provide a high level of security is realized. Fuzzy Vault uses both biometrics and cryptography together. Today, people have multiple ATM pins and passwords in multiple accounts, and to protect these pins and passwords, the new fuzzy vault system is a system that works with both biometrics and encryption.

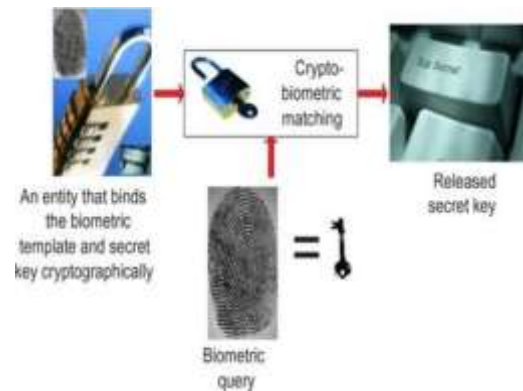


Figure 3: Key binding mode of bio cryptosystem.

In key binding mode as per figure 3, firstly the key will be generated by the RSA algorithm, and public key will be combined with the biometric query and with the user's PIN. When all three entities will be combined then the system will be more secure and only the authorized user can access the ATM.

However, to enhance the security of the cryptography keys, we will use the Internet Security protocol which is divided into two parts: Authentication header and Encapsulation security protocol. Likewise, we will use the encryption algorithm in the ESP protocol and authentication protocol in AH. At a time, when both will be approved, we can get the Identifier in domain of Interpretations (DOI). Hence, our system will be completely secured and no intruder can hack the user's personal data.



Figure 4: Variation of the fingerprints.

Figure 4, represents two dissimilar images of the same finger on two distinctive days. Due to translation, distortion, and rotation, the position of the feature points will be different in both images. Since key release is easy to implement however the security of biometric templates is the main thing. Biometric template can easily be stolen, once the template is stolen, it is impossible to revoke hence if we compare all three modes, it turns out that the key binding / generation mode is highly safe than the other, but it is not easy to contrivance due to large unpredictability of fingerprint pattern.

2. LITERATURE REVIEW

Many researchers have been working on bio cryptographic systems. Juels and Wattenberg[11] were used to hide secrets using a set of biometric data, but worked with an ordered set. If work is presented on an unordered set or a noisy system, the system will either fail or the idea will be rejected.

Juels and Sudan[3] have adapted this old method of fuzzy commitment to present a bio crypto system. This fuzzy vault system provides protection for each of two secret keys and biometrics. Therefore, bio crypto systems, unlike fuzzy commitment systems, work with unordered datasets. They both are joined and put in the vault. C and G are added together to maintain the security of the biometric data. That secures the Secret Key S and fingerprint data of the user from the Intruder.

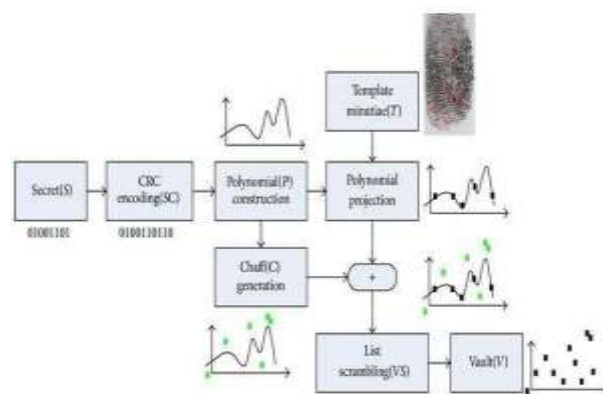


Figure 5: Encryption of fuzzy vault for fingerprint

Here we can see in figure 5 that at the time of registration, private key K is hooked by U. Whereas U is a disordered pair of genuine points G selected from a personal fingerprint design. The polynomial [5] P is created by encrypting private key S. P is measured by all elements. Now to unlock the vault, the user's need to supply the query biometric template Q'. By this Q', another un-ordered pair of genuine points G' is selected. Therefore, many numbers of genuine points and chaff points are stored in vault V. If the genuine points G' and G overlap each other and the secret is decoded, the polynomial can be reconstructed.

This system is called fuzzy. That means anything which is faulty and untruthful. Biometric is known as fuzzy since the templates of the identical person and even of the same fingers are not similar.

Ratha et. Al[23] proposed different techniques of cancelable template generation as if the original template will be used in one application and that application will be compromised then the other applications will also be compromised. Hence, to overcome this problem, they proposed the technique of cancelable template of the biometric pattern of the user. Cartesian transformation technique is used to displace the original location of the minutiae with the help of mapping Matrix. By this same transformation function with a different transformation key can be generated a new cancelable template of the same finger.

N. Lalithamani and K.P. Soman[20] also approached the technique of cancelable template. They calculated the distance between two minutiae points and unique distances are considered. They stored the distance as a vector. Also, they applied another approach called discrete exponential function. There are two coordinates (x and y) and the next prime number of each vector is computed and stored in another vector. If the resultant vector would be prime that would directly append to that vector, the next prime number will append to the third vector.

Hao et al. [24] Proposed an approach to combine the cryptography with Iris, in their approach a random key is generated by the iris and the key is encoded with error correction codes. This encrypted key is XORed with the iris image to lock the reference code with encoded key and the locked iris key is being stored in the smart card. Now a new query iris code is generated and it's XORed with the locked iris key and stored in the smart card. They are able to extract 140 keys correctly with 0.47 % FRR and 0% FAR.

S. Dutta et al[21] proposed an approach to create a cryptography key from the biometric data. In this method, fingerprint data of sender and receiver are shared without transformation and the 128 bits long cryptographic key will be generated. Hence, at the sender's end the key will be generated and it will be transmitted at the receiver's end with the encrypted message. Hence, the data will be secure and cannot disclose to each other.

3. PROPOSED SYSTEM

The below diagram shows the overall proposed fuzzy vault system based on cryptography and biometric. It is completely based on the encryption and decryption and fingerprint template.

System Description: To maintain the confidentiality of the pin and password of the user, we will combine the cryptography keys and fingerprint together that create a fuzzy vault system as illustrated in figure 6.

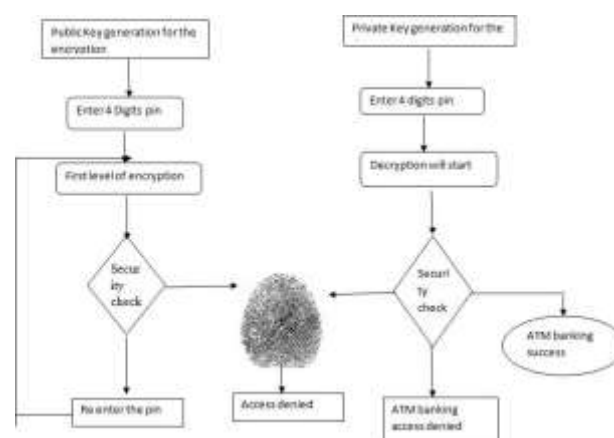


Figure 6: Proposed system block diagram Algorithm design steps:

First, we will generate a key with the help of RSA algorithm for the encryption with the help of two prime numbers.

Steps: Choose 2 prime numbers m & n .

1. Compute: $r=m*n$

$\Omega(r)= \Omega(m) \times \Omega(n)$ (Euler totient function)

$= (m-1) \times (n-1)$

2. Choose e ; $1 \leq e < \Omega(r)$, co prime of $\Omega(r)$ $\hat{O}(e, r) =$ public key

3. Determine, s as $e*s=1 \pmod{\Omega(r)}$ $s= 1/e \pmod{\Omega(r)}$ (s is multiplicative inverse of e)

4. $\hat{O}(s, r) =$ private key

5. $D=(\Omega(r) \times I) + 1/e$ ($e*s= 1 \pmod{\Omega(r)}$)

Once the key will be generated, user will enter his 4 digits pin number, the public key will be combined with the user's pin and the process of encryption will start. After the security checks, if the pin would be correct then it will further proceed and user needs to put the fingerprint data in the system.

If all the data would be correct, the process will be continuing for the decryption. If security checks fails then user needs to enter their pin again, the process will be continuing till the user can't enter the correct pin.

Same process will start for the decryption and private key will be generated for the decryption, now once the user will enter his 4 digits pin then the decryption process will start, if in the security checks the fingerprint data and the correct pin would have been entered by the customer, the user will be able to withdrawal the money from the ATM otherwise it will be access denied.

We will here use the RSA algorithm for generation of public and private keys for the encryption and the decryption process. The system will be highly secured from the attackers and we added the fingerprint and keys both as fingerprint of the user will be unique of every user.

Here the main question here arises that how can we secure our cryptography keys and fingerprint data. So that, the attacker cannot hack the secure keys.

To maintain the security of the cryptography keys, we used Internet security protocols. That is divided into two parts: Authentication header and Encapsulation security protocol as shown in the figure 7.

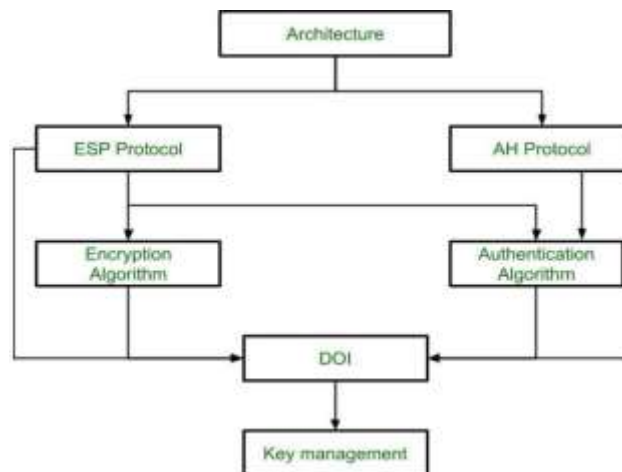


Figure 7: IP security Architecture

In Authentication protocol, it decides whether the authorized user is accessing or not. In the Encapsulating security protocol, we can use the Encryption algorithms like DES, AES and RSA. Hence, which authentication and encryption algorithms are approved, we can get the Identifier in domain of interpretations (DOI). Once is the major module here is the key management which manages the key. Therefore, keys can be handled by the two ways: IPsec key command is the manual way and the second way that is automated way is Internet key exchange (IKE) protocol.

4. COMPARATIVE ANALYSIS AND DISCUSSION

Table 1: Comparison of RSA, AES and DES

Factors	RSA	DES	AES
Created by	In 1978 by Rivest, Shamir, and Adleman	In 1975 by IBM	In 2001 by Vincent Rijmen, Joan Daemen
Cipher Type	Asymmetric	Symmetric	Symmetric
Key Length	>1024 bits	56 bits	128, 192, or 256 bits

Known Attack	Factoring the public key	Brute Forced, Linear and differential cryptanalysis attack	Side Channel Attack
Block Size	Minimum 512 bits	64 bits	128 bits
Simulation speed	Faster	Faster	Faster

Table 1, represents the comparison of AES, DES and RSA, we can determine the strong algorithm on the basis of security level.

DES: Security is the major concern in the DES algorithm due to 56 bit key length, the security of the DES algorithm can be easily cracked by the brute force, linear and cryptanalysis attack.

RSA: We will generate the public and private key with the help of RSA algorithm, it will take more number of bits than DES and AES algorithm, finding the public key with the help of two prime numbers, we will use the Euler totient function to determine the keys. But, basically it is not possible to find the key because of the polynomial time hence it proves that RSA is a strong algorithm.

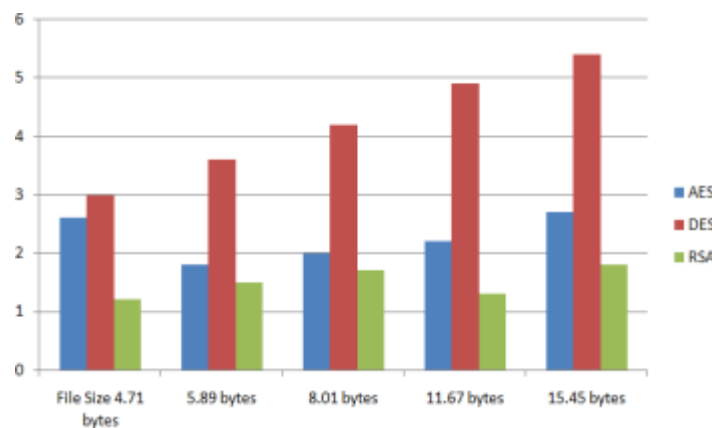


Figure 8: Computation time values

As illustrated in figure 8, we can compute the time values with the help of file size in bytes, for the various file sizes; we are getting the different values of DES, AES and RSA. DES is taking the maximum time in comparison of RSA and AES however it is the minor time difference between the AES and RSA.

5. EXPERIMENS & RESULTS

The proposed system is implemented by the Java applets and swing packages. We have inserted a fingerprint sensor in the system and when the

AES: AES algorithms provide the highest security level as we can use the key length up to 256 bits also it performs the same operations like RSA arithmetic operations however it could be mathematically inverted. The security of the key depends upon that how much time and cost it will take to identify the key by the imposter. No attack can crack the security of the AES algorithm.

customer will try to touch the sensor to put his fingerprint image that will be bind with the cryptography keys and with the unique pin if all the necessary conditions will be matched only then the user can access the ATM.

The combination of cryptography key, user's secure pin which he can get from the financial institution and fingerprint image of the user create a fuzzy vault system as per figure 9.

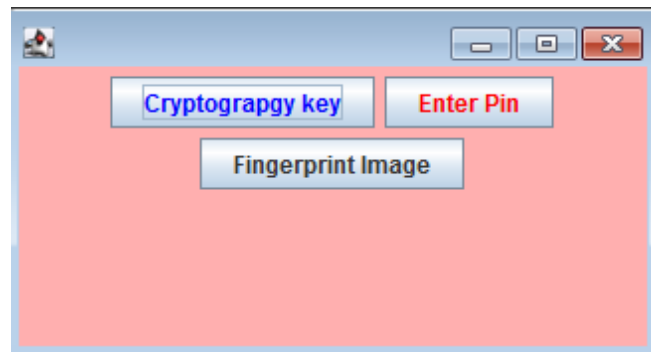
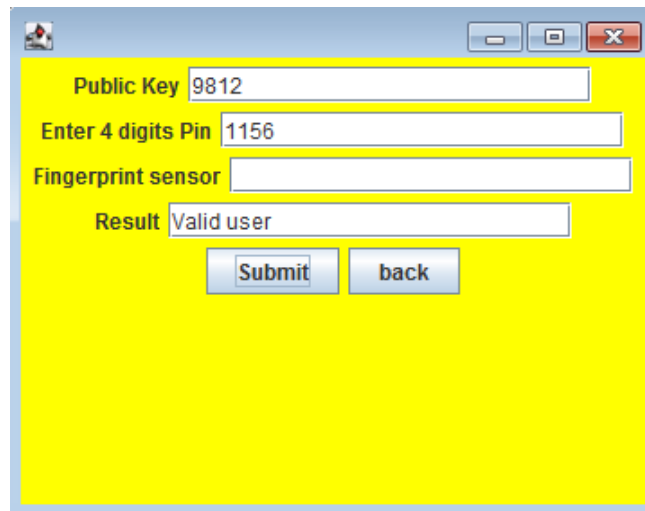


Figure 9: Fuzzy Vault System

In the Initial phase, the public key will be combined with the customer 4 digits Pin, the public key will also be the 4 digits as same of pin digits, hence the encryption process will starts and if after the security check all the data will be matched then it will proceed further and system will check the fingerprint module of the user as well. If the valid fingerprint would be there then it will start decryption phase and user will be able to access the ATM successfully else access denied will occur.

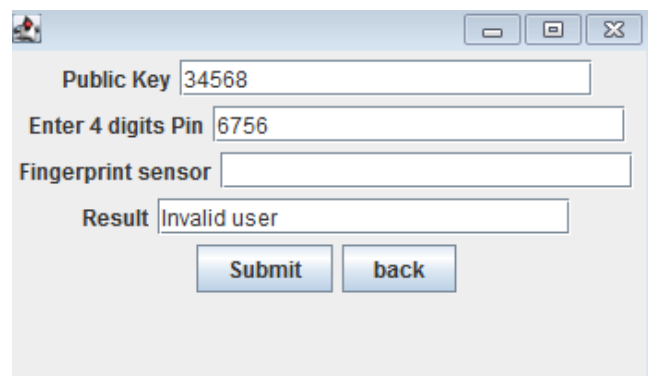
The verification of the valid or authorized user is depicted in figure 10. Here, public key will contain the same number of digits as the user's pin or password. If data will be matched, user will be accessible or the user will be valid user.



A screenshot of a web application window with a yellow background. It contains the following fields and buttons:

- Public Key: 9812
- Enter 4 digits Pin: 1156
- Fingerprint sensor: (empty)
- Result: Valid user
- Buttons: Submit, back

Figure 10: Verification of the valid user.



A screenshot of a web application window with a light gray background. It contains the following fields and buttons:

- Public Key: 34568
- Enter 4 digits Pin: 6756
- Fingerprint sensor: (empty)
- Result: Invalid user
- Buttons: Submit, back

Figure 11: Invalid user after security check

If in the security checks, the authentication is failed the user will not be able to access the data as shown in the above figure 11.

6. CONCLUSION & FUTURE WORK

Traditional fuzzy commitment system was unable to secure the data, hence we modified the system and used cryptography and biometric together to secure the authentication process. We were facing some issues to maintain the security of the biometric traits hence we used the crypto biometrics to maintain the safety of the fingerprint data here we used the dummy fingerprint modules of few patterns of the users. Also to provide more security of the cryptography keys, we used internet security protocol.

Now it is impossible to guess or break the key within a specific time period. If the attacker has both cancelable templates, the attacker can generate a key. The sender's fingerprint data is shared in an encrypted format and requires a real recipient fingerprint and private key to decode it. Recipient fingerprint data is not shared over insecure channels. The key is not saved and is not sent to the recipient. Therefore, this approach protects key management.

User can get the pin or password from the financial institution that is a secure password but

also our system will fail if an intruder hacks the customer phone number, they can change the user's pin and can verify their data with the help of the user's personal details. Hence, in the future we can design a system that will secure the user's pin and OTP.

REFERENCES:

- [1] W. Stallings, 3rd ed., *Cryptography and Network Security, Principles and Practices*, Prentice Hall, 2003.
- [2] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," in *Proc. Audio-Video-Based Biometric Person Authentication*, 2005, pp. 310–319.
- [3] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symposium. Information Theory*, 2002, pp. 408
- [4] A. Jain, K. Kumar and A. Nagar, "Biometric Template Security", *EURASIP Journal on Advance in Signal Processing*, 2008.
- [5] K. Nandakumar, A. Jain and A. Pankanti, "Fingerprintbased fuzzy vault: Implementation and Performance", *IEEE Transactions Information Forensic Security*, Vol. 2, No.4, pp. 744-757, 2007.
- [6] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symposium. Information Theory*, 2002, pp. 408
- [7] Y. Feng and P. Yuen, "Protecting face biometric data on smartcard with Reed–Solomon code," in *Proc. CVPR Workshop Privacy Res. Vis.*, 2006.
- [8] M. Freire-Santos, J. Fierrez-Aguilar and J. Ortega- Garcia, "Cryptographic key generation using handwritten signature," in *Proc. Def. Security Symposium, Biometric Technology Human Identification*, 2006, pp. 225–231.
- [9] Y. Chang, W. Zhang and T. Chen, "Biometric- based cryptographic key generation," in *Proc. IEEE International Conference on Multimedia Expo.*, 2004, pp. 2203–2206.
- [10] Y. Lee, K. Park, S. Lee, K. Bae and J. Kim, "A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System", *IEEE Transactions On Systems, Man, And Cybernetics— Part B: Cybernetics*, Vol. 38, No. 5, 2008, pp. 1304- 1313.
- [11] A. Jules and M. Wattenberg, "A fuzzy commitment scheme", in *Proc. 6th ACM conference on computer and communication security (CCS '99)*, pp. 28-36.
- [12] M. Khalil-Hani, M. Marsono and R. Bakhateri, "Biometric Encryption based on a fuzzy vault scheme with a fast chaff generation algorithm", *Future generation Computer Systems*, 2013, pp. 800-810.
- [13] R. Hooda and S. Gupta, "Fingerprint Fuzzy Vault: A Review", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, Issue 4, 2013.
- [14] R. Ferrer, L. Carneiro, J. Bessa, J. Moraes, E. Neto and A. Alexandria "Techniques of Binarization, Thinning and Feature Extraction Applied to a Fingerprint System", *International Journal of Computer Applications*, Vol. 103, No. 10, 2014.
- [15] Y. Chen, S. C. Dass, and A. K. Jain, "Fingerprint quality indices for predicting authentication performance," in *Proc. AVBPA*, 2005, pp. 160–170.

- [16] Hazewinkel, Michiel, "Lagrange interpolation formula", Encyclopedia of Mathematics, Springer, 2001.
- [17] B. Persis Urbana Ivy, Purushothaman Mandiwa, Mukesh Kumar, 'A Modified RSA cryptosystem based on 'n' prime numbers', International Journal of Engineering and Computer Science, ISSN:2319-7242 Vol 1 Issue 2, Nov 2012 page no. 63-66.
- [18] Rajan S Jamgekar, Geeta Shantanu Joshi, 'File Encryption and Decryption Using Secure RSA', International Journal of Emerging Science and Engineering, ISSN: 2319-6378 Vol 1 Issue 4, Feb 2013.
- [19] N. Lalithamani and K.P. Soman, "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme," European Journal of Scientific Research, vol.31, no.3, pp.372-387, 2009.
- [20] N. Lalithamani, K.P. Soman, "An Effective Scheme for Generating Irrevocable Cryptographic Key from Cancelable Fingerprint Templates," International Journal of Computer Science and Network Security, Vol.9, No.3, pp: 183- 193, 2009.
- [21] S. Dutta, A. Kar, B. N. Chatterji and N.C.Mahanti, "Network Security Using Biometric And Cryptography," Lecture Notes in Computer, Springer, 2008. ISBN978-3-540-88457-6: 38-44.
- [22] S. Dutta, S. Chakraborty, N.C.Mahanti, "Fingerprint Based Cryptography Technique for Improved Network Security," Journal of Computer Science and Engineering vol. 5, issue 2, February 2011.
- [23] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating Cancellable Fingerprint Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561-572, April 2007.
- [24] Feng Hao, Ross Anderson, and John Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081-1088, 2006.
- [25] Gary C. Kessler, "An Overview of Cryptography" [Online]. Available: <https://www.garykessler.net/library/crypto.html> , 2021.
- [26] William Stallings's book "Cryptography and Network Security: Principles and Practice," 6th Ed, 2013, ISBN-13: 9780133354690.
- [27] Taylor Onate Egerton Victor T, "Comparative Analysis of Cryptographic Algorithms in Securing Data," International Journal of Engineering Trends and Technology (IJETT) – Volume 58 Issue 3 – April 2018.
- [28] JDK1.8.0_291 [Online]. Available: <https://www.oracle.com/in/java/technologies/javase/javase-jdk8-downloads.html> , 2021.
- [29] Karthik Nandkumar, Anil K. Jain,, "Fingerprint- Based Fuzzy Vault: Implementation and Performance," IEEE Transactions on Information Forensics and Security (Volume: 2, Issue: 4, Dec. 2007.