IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Security Improvement Algorithm for online Fingerprint Authentication

Vinutha C D[1], Dr. Devaraju R[2]

[1] Dayananda Sagar College of Engineering, Student, Bangalore, India

[2] Dayananda Sagar College of Engineering, Associate Professor, Bangalore, India

Abstract— The data privacy issues for an individual is of more concern due to the high sensitivity of the data. The Confidential information pertaining to the user data must be kept safe. The access and usage of the data should abide with Organization for Economic Co-operation and Development (OECD) principles. We present a privacy-preserving policy called Improved Security Fingerprint Authentication (ISFA) scheme. The ISFA scheme consists of three parts i.e., Trusted0Authority (TA), Online Authentication Servers of Internet service (OASers) and Consumers. TA is similar to the government agency, booting up the system initialization by generating and sending system parameters (private and public keys) to the registered OASers and the consumers. TA is in charge of fingerprint template encryption and storage. OASers are similar to businesses like Amazon, Flipkart etc., and they should register in TA ahead of time. OASers will receive the consumers registration details and request TA for the related fingerprint templates. After registering, consumers will log in using their fingerprint, which has already been authorized by a trusted authority, and then consumers will be able to access the website. Our system generates an ECC over prime number algorithm for encryption, and a fingerprint matching mechanism compares the current fingerprint picture to the image stored in the database. The consumers will be able to access the portal if the image matches without any differences.

Keywords-Data security, Elliptic curve cryptography, Online authentication, fingerprint.

1. INTRODUCTION

Biometric-based identification, which is based on a person's biological or behavioral features, is gaining popularity as a practical way to identify them[1]. Because of the universality, uniqueness and permanence of biometric data, biometric identification systems have been widely used in a range of applications. They offer greater convenience than traditional techniques, such as PINs, passwords, and ID cards, and can be lost, stolen, or forgotten. More banks have recently increased their efforts to integrate biometric technology (iris scanners, fingerprint readers, and so on) into their systems [2]. Fingerprint identification is widely utilized in criminal investigations and law enforcement, but it can also be employed in civilian applications such as access control, online payment verification, and driver license applications [3][4]. Despite the widespread use of fingerprint authentication, there are growing worries about the privacy and legal difficulties that come with it, because fingerprint data is highly sensitive and cannot be cancelled or replaced once it has been exposed [5][6]. For example, fingerprints cannot be altered like traditional passwords, if a fingerprint is used as a password once, it can never be used again. In this regard, considering the requirements of actual systems on security and efficiency, privacy-preserving online fingerprint authentication remains a difficult task. Because fingerprint recognition allows for some degree of uncertainty or distortion, fingerprint data should not be encrypted using the Hash method, which has a very high "avalanche effect." To address the problem, various common approaches have been offered, such as Fuzzy Vault and Bio-Hashing [7][8], which can keep templates private during the storing and matching process. The servers, on the other hand, are trusted in the foregoing schemes, and these privacy-preserving strategies will have an impact on the correctness of the underlying identifying system. To tackle the problem, homomorphic encryption and searchable encryption techniques are also developed [9]. These related schemes have significant temporal complexity or only enable simple arithmetic, making them unsuitable for the various complex computations required by an online fingerprint matching service. Some approaches use matrix-based encryption to prevent excessive computing overhead while allowing the cloud to find the best match without decryption in the outsourced situation [10].

2. RELATED WORK

Data privacy issues have recently sparked increased concern. Some relevant efforts on privacy-preserving fingerprint-authentication are briefly reviewed in this section.

In recent advances in biometric recognition and the increasing use of biometric data prompt significant privacy challenges associated with the possible misuse, loss or theft of biometric data. Biometric matching is often performed by two mutually suspicious parties, one of which holds one biometric image while the other owns a possibly large biometric collection. Neither party is prepared to provide its data due to privacy and liability concerns. This necessitates the development of secure biometric data computation algorithms in which no information is provided to the parties other than the result of the comparison or search. In order to solve the problem, G. P. Blanton M [2], proposes a method to develop and implement the first privacy-preserving identification protocol for IRIS codes. In addition, the author also designs and implement a secure fingerprint recognition technique based on Finger Codes that outperforms existing methods significantly. The author demonstrates how novel methodologies and optimizations used in this study allow us to build highly efficient protocols suitable for big data sets and produce significant performance gains when compared to previous work that was considered state-of-the-art.

Jin [3] proposed a novel algorithm for human authentication security, where the objective of the task was to limit access to only those with authority have access to physical sites or computer networks. This is accomplished by providing passwords, tokens, or biometrics to authorized users. Unfortunately, the first two suffer from a lack of security because they are easily forgotten and stolen; biometrics, too, has inherent limitations and security dangers. Combining two or more factor authenticators to gain security benefits is a more realistic strategy. This work proposed a novel two factor authenticator based on iterated inner products between tokenized the

integrated wavelet and Fourier–Mellin transform provide a pseudo-random number and a user-specific fingerprint feature. The transformed user specific compact code is coined as Bio-Hashing. With the same user fingerprint data, Bio-Hashing is very tolerant of data capture offsets, resulting in strongly correlated bitstrings. Furthermore, without both the token with random data and the user fingerprint feature, there is no deterministic way to acquire the user specific code. For example, this approach would protect us from biometric fabrication, which can be accomplished by just altering the user particular credential, which is as easy as changing the token holding the random data. The Bio-Hashing algorithm has significant functional advantages by combining two or more factor along with biometrics decreases the occurrence of false reject rates.

Juels and Sudan [4] describes a simple and novel cryptographic construction called fuzzy vault. User A may place a secret key *k* in a fuzzy vault and locks it using a set elements/features with specific length related him from some public domain U. If user B tries to unlock the vault using his elements/features set of similar length, he obtains *k* only if B features are close enough to A features, i.e., only if A features and B features overlap substantially. This fuzzy vault concept provides a provable security against a computationally unbounded attacker.

B. M. R. Dellys H N, Benadjimi N [7], proposed, In the fingerprint fuzzy vault, there are numerous abscissae creation methods for chaff points. An experimental comparison of the squares-method and threshold-methods is undertaken in this work. The experimental results show that the squares-method is far better than threshold-method. But detailed representation in squares-method uses 2D representation while threshold-methods are represented by composite representation. The authors propose to implement squares-methods using composite representation and conducted same experiments which executed in less time.

A. A. Nasiri and M. Fathy [8], addressed the significance of fingerprint template protection in fingerprint recognition systems. For this aim, fuzzy vault is a promising and practical scheme. It has the ability to preserve biometric templates as well as execute secure key management. The process of aligning the query fingerprint sample in the encrypted domain with the template fingerprint sample is difficult. In this work, an alignment-free fingerprint cryptosystem based on multiple fuzzy vaults is experimented. In the proposed method, the registration phase conducts multiple vaults construction for one fingerprint and the secret will be recovered if at least two of the vaults are successfully decrypted by the query fingerprint during the verification phase. To test the performance of the proposed fingerprint cryptosystem, experiments are done on the FVC2002-DBla and FVC2002-DB2a data sets.

J. Hartloff and V. Govindaraju [9], talks about the traditional work on fingerprint verification using a cryptographic framework and the fuzzy vault approach. This work demonstrates that the breaking of a fuzzy vault leads to random error decoding of Reed-Solomon codes, which has been considered as a challenging problem in the cryptography field. Most current research gauges the strength of the fuzzy vault in terms of its resistance to pre-defined assaults or by the vault's entropy. This paper proposed a security parameter for the fuzzy vault in terms of the decoding problem, which provides context for the breaking of the fuzzy vault. The author continues to follow our security parameter and provides ROC statistics with it. This research also aims to be more conscious of the nature of fingerprints when storing them in the fuzzy vault, noting that detailed distribution is far from random. The results show that the fuzzy vault can be a viable approach for secure fingerprint verification.

Z. J. F. Q. HE Kang, LI Mengxing [10] explains how to handle the challenge of securing remote identity authentication privacy via fingerprints by presenting a novel approach based on Finger code and homomorphic encryption. The server's template is encrypted in the proposed scheme, whereas the server's templates in previous schemes were plain, ensuring its security. The “packing” mechanism is used in the protocol to effectively reduce the computational and communication load between the server and the customer. The proposed technique is secure and practical, according to analysis and experiment results.

M. Barni, T. Bianchi, D.Catalano, and M. D.Raimondo [11], introduces the privacy protection of biometric data as a key research area, particularly in the context of distributed biometric systems. It is important in this case to ensure that biometric data cannot be stolen by anybody and that biometric clients are unable to collect any information other than the single user verification/ identification. The server that conducts the biometric matching should not learn anything from the database, and it should be impossible for the server to abuse the matching values to extract any information about the user's presence or behavior in a biometric system with a high level of privacy compliance. Within this conceptual framework, the author proposes a novel complete demonstrator based on a distributed biometric system capable of protecting individual privacy through the use of cryptosystems in this study. Using homomorphic encryption and Finger code templates, the implemented system computes the matching task in the encrypted domain. The demonstrator's design technique is described in this work, as well as the results collected. The demonstrator has been fully developed and tested in real-world scenarios. Experiments show that this strategy is feasible in situations where data privacy is more important than system correctness and the processing time obtained is acceptable.

Biometrics-based verification, particularly fingerprint-based identification, has received a lot of attention since it was proposed by A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti [12]. Traditional techniques to fingerprint representation have two significant flaws. The representations based on explicit identification of entire ridge structures in the fingerprint are challenging to extract automatically for a significant portion of the population. The frequently used minutiae-based representation ignores a large portion of the rich discriminating information contained in fingerprints. The details of local ridge formations are insufficient to fully define them. Furthermore, minutiae-based matching struggles to match two fingerprint photos with varying numbers of unregistered minutiae points efficiently. A bank of Gabor filters is used in the proposed filter-based technique to capture both local and global features in a fingerprint as a compact fixed length Finger Code. Because it is based on the Euclidean distance between the two corresponding Finger Codes, fingerprint matching is extremely rapid. The accuracy of the authors' verification is just marginally inferior to the best results of minutiae-based algorithms published in the open literature. Our method outperforms a state-of-the-art minutiae-based system where the application system's performance requirement does not entail a very low false acceptance rate. Finally, the matching performance can be improved by combining the matchers' findings based on complementary (minutiae-based and filter-based) fingerprint information.

The fundamental disadvantages of the methods described above is their poor performance when an impostor takes a party's pseudo-random numbers and attempts to authenticate as the party. If the sensitive data is encrypted, the security issues with outsourced databases can be overcome. However, this raises the question of how the storage system can process encrypted data. Other issues include how the storage system may process encrypted data. The homomorphic encryption approaches described are not practicable for random arithmetic computation over encrypted data, and so are not suited for online use, due to the so-called bootstrapping that results in increased processing overhead. Unlike the previous approaches, the proposed IFSA scheme is based on ECC over prime number and aims to improve efficiency and privacy. The privacy transition, in particular, will have no effect on the accuracy of the underlying fingerprint identification system.

3. PROPOSED SYSTEM

We focus on how servers provide accurate and efficient fingerprint authentication with encrypted consumer queries and templates in the proposed system. As indicated in Fig. 1, the system is made up of three parts: a Trusted Authority (TA), Online Authentication Servers of Internet Services (OASers), and Consumers.

TA is a Trusted Authority, this generates and sends system parameters to registered OASers and consumers, respectively, to initialize the system setup. The encryption and storage of sensitive fingerprint templates collected from consumers is the responsibility of TA. Moreover, TA sends certain encrypted templates to registered OASers with consumers authorization. TA performs two functions: system initialization and encrypted template authorization.

- OASers provide personal authentication, such as enterprises like Amazon, Flipkart, etc. To be qualified to perform fingerprint authentication service, OASers need register with TA ahead of time. OASers receive consumers register information and requests to TA for related templates. After receiving the encrypted fingerprint templates, OASers can provide personal authentication by using fingerprint matching technique.

Users can register in OASers and query the privacy-preserving online fingerprint authentication service using their fingerprints after having their fingerprints taken by TA. Because fingerprints contain sensitive data about consumers, and sending the query in plaintext to OASers could result in privacy breaches, TA should use ECC over prime number encryption during the query generation process.

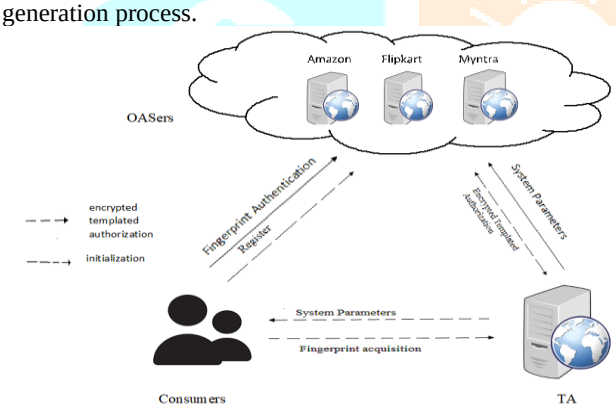

Fig 1. System Model

4. SECURITY REQUERIMENTS

In our security paradigm, TA is trusted, whereas OASers are trustworthy but suspicious. In particular, OASer will carry out the activities honestly in order to verify the identity of the consumers, but it will also attempt to decrypt the encrypted templates received from TA and the inquiries received from consumers in order to get the original fingerprint data. Furthermore, an OASers may engage in malevolent conduct, such as attempting to mimic another OASers in order to provide service or engaging in coordination with other OASers. For the success of a privacy-preserving fingerprint authentication technique, the security of fingerprint data in storage, transmission, and calculation is important. As a result, the following security standards must be met in order to ensure the protection of sensitive data and communication packages.

Privacy: When an OASers or opponent acquires all of the requests from consumers, it will not be able to obtain the original fingerprint information under the proposed scheme. Furthermore, an OASers can only acquire the matching result while doing the computing process to see if the query fingerprint and the fingerprint template match. In addition, the outcome of the matching should be safe from attackers.

Confidentiality: The sensitive fingerprint templates assets should be preserved under the proposed ISFA scheme. Even if an OASers or adversary keeps all of the consumer data obtained via TA, it will not be able to obtain the original fingerprint information for the corresponding template. Furthermore, the method should prohibit OASers from colluding or leaking templates; even if one unlawful OASers obtains encrypted templates assets from another, it will not be able to provide fingerprint authentication services.

Authentication: Authenticating an encrypted query/response provided by licensed OASers/consumers and not altered during transmission, for example, if an unauthorized consumer forges a query or response, this harmful behavior should be recognized. In this sense, only lawful inquiries and responses are acceptable.

5. PRELIMINARIES

- **Proposed ISFA Scheme**

System Initialization, Encrypted Template Authorization, Authentication Query Generation, and Fingerprint matching are the four key aspects of the proposed ISFA, which is an efficient and privacy-preserving online fingerprint authentication technique. In the System Initialization phase, TA starts the system and provides consumers and OASers registration, as well as collecting the registered consumers fingerprints as matching templates. In the Encryption Template Authorization step, TA encrypts the collected templates and transmits the templates of registered consumers to OASers with consumer authorization. In the Query Generation phase, registered consumers create queries for OASers. Finally, in the Fingerprint Matching phase, when OASers receives the consumers inquiry, it does the matching computation to determine whether the fingerprints match and responds to the consumers with the results.

- **Registration:**

Initially, OASers must use the fingerprint matching technology to register with the Trusted Authority with their fingerprint. After the Trusted Authority approves the request, OASers can add products to the website. OASers will require Trusted Authority for the relevant templates when customers register with them. If the fingerprint is matched after receiving the related templates from the authority, it will display as 'fingerprint matched,' and consumers will be able to enter the website and view the products; if it is not matched, it will display as 'fingerprint mis-matched,' and consumers will be unable to enter the website and view the products.

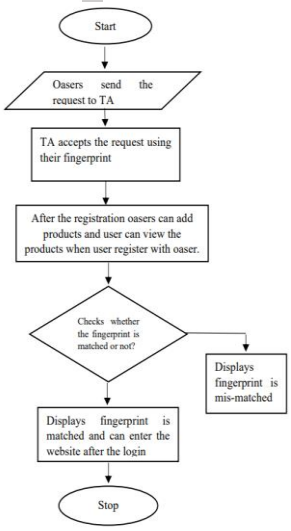

Fig 2: Flowchart of Registration

- **Authentication:**

Consumers can securely send their inquiry requests to OASers after registering with them. The Message-Digest Algorithm is a cryptographic hash function that is utilized. The static function get Instance is used to initialize these algorithms (). The message digest value is calculated when the algorithm is chosen, and the

results are transmitted to a byte array. With the help of base64, the convert text technique is used to transform text into by code. After the picture has been encoded and decoded, it is transmitted to the byte array, which converts the text into an image.

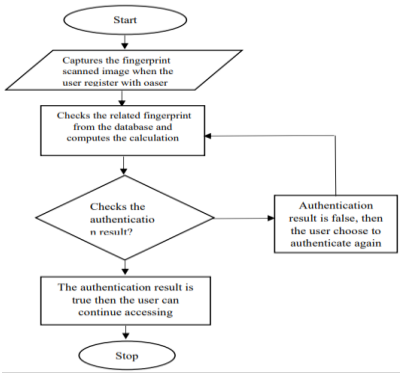

Fig 3: Flowchart of Authentication

- **Encryption:**

The signature method and the verify method are two alternative ways for ECC over prime numbers. In the signature method, the given data is transformed to ECC, which then encrypts it and handles the tiny keys. The data that is signed should be validated in the verify method. In Java, there is a pre-defined class called EC Parameter Spec. The ECC over prime number is specified as prime192v1 in this EC parameter spec, and it is passed to the ECC initialization procedure when it is created. The Sun security provider will use a 192-bit prime field Weierstrass curve to implement this type of encryption process, which will allow the private and public key pairs to be generated. The data is then calculated and stored in a database, with the image format consisting only of 0's and 1's.

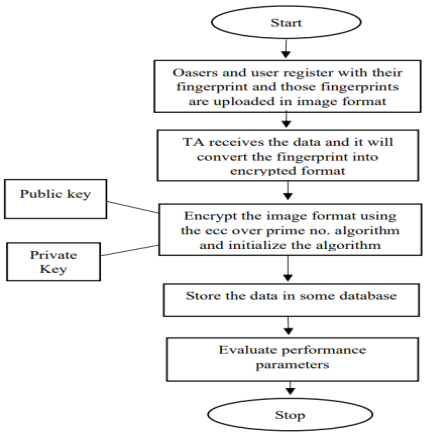

Fig 4: Flowchart of Encryption

- **ECC over Prime Number Algorithm**

Step 1: The ECC over prime numbers has two methods, one for signatures and the other for verifications.
Step 2: In the signature method, the given data is turned into the ECC, which is then encrypted, and it handles small keys with a size of 192 bits prime field weierstrass curve.
Step 3: The EC parameters spec is a predefined class, and the ECC over prime number is given as prime 192v1 in the EC spec, which is passed to the initialization process once it is created.
Step 4: Sun security is enabled, and an add provider is imported from the upper class, which mentions a specific library that uses prime numbers.
Step 5: The ECDSA and BC are mentioned in order to load our method from the bounce castle supplier and build a keypair.
Step 6: The process is started with EC Spec, which generates a security random key before generating a private and public key and storing the item.
Step 7: Data get byte will generate a file containing a byte array that will be transmitted to the input data.
Step 8: The input data and private key are transmitted to the sign method to start the signing process, and everything is saved in a specific repository.
Step 9: In the verification method, the data that is signed is checked and validated using the public key. The input data, public key, and sign data are then sent into the verify method, which checks and verifies the data.

- **Fingerprint matching Algorithm**

Step 1: Pixel by pixel, the fingerprint image will be compared. The first and second images will be compared; if the pixels do not match, an error will be displayed; otherwise, the difference percent will be calculated.
Step 2: Using RGB, divide the pixels pixel by pixel to calculate the difference percent.
Step 3: Calculate the pixel difference by comparing the first image pixel to the second image pixel, and the second image pixel to the first image pixel.
Step 4: Using the for loop and the pixel values of each image, the largest difference is determined.
Step 5: The result is saved in a value that will be examined to see if the image matches without any differences. If it does, authentication is successful; otherwise, authentication is unsuccessful.

- **Java Implementation Details**

Java Big Integer class is used to implement the ECC operations. The Big Integer object in Java offers methods for working with huge numbers (primes and non-primes), which are required for all cryptographic techniques. Its Prime() method most likely generates prime numbers with a specified number of bits. Big Integer objects can be added, subtracted, multiplied, and so on using other methods. The mod Pow() method, which allows you to raise a number to a power and then execute the mod operation, is one of the most commonly used ways. Mod Inverse (), which allows you to do a mod operation on the inverse of a number, is another frequently used method. We can make an ECC Point object out of the Big Integer object. We may use this object to conduct Point additions based on the attributes of EC. This object allows us to conduct numerical operations that take into account the point at infinity. This object has two major functions: one to add two points and another to multiply a Point by a scalar.

6.RESULTS

The proposed project uses the NetBeans IDE for web page development and the SQLyog Community for MySQL database management. Created a web website for OASers, consumers and Trusted Authority.

Fig 5: Web Page

The Trusted Authority, which is in charge of encrypting and storing sensitive information templates obtained from consumers, is mentioned on the web page. OASers will register with Trusted Authority ahead of time in order to be qualified to perform fingerprint authentication services; OASers will receive consumers registration information and will register with Trusted Authority for associated templates. Consumers can then register with OASers and use their fingerprint to query the privacy-preserving online fingerprint acquisition service. After registering, OASers can add their products to the website using their fingerprint; if the fingerprint matches, they can enter the

website; else, the fingerprint will be mis-matched. The consumers will then login with their fingerprint to purchase things from the website; if the fingerprints match, they will be able to access the website; otherwise, the fingerprints will be mismatched, as shown in the diagram below.

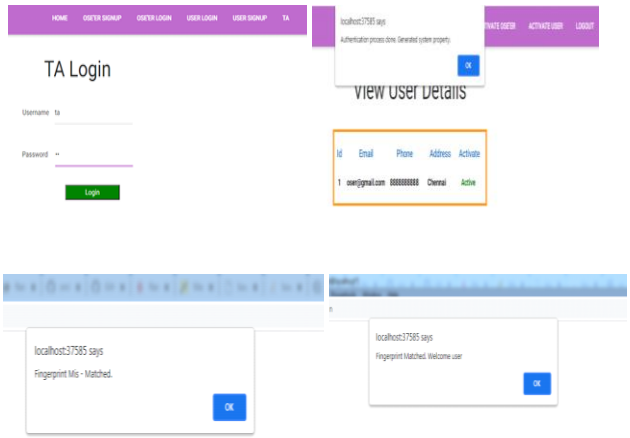

Fig 6: Login credentials

Furthermore, a link is established between the ISFA method and PRFS, with PRFS being a fingerprint recognition system based on homomorphic encryption and FingerCode templates. Figure 7 shows the computation overhead of ISFA and PFRS as a function of the number of FingerCode dimensions, and we can see that as the number of dimensions increases, the computation overhead of PFRS increases dramatically, and it is much greater than that0of our suggested scheme. In the suggested approach, the average cost time of inquiry and answer in a work area is a few seconds, which is acceptable for online applications. When compared to PFRS, IFSA is more=efficient and secure in outsourcing settings.

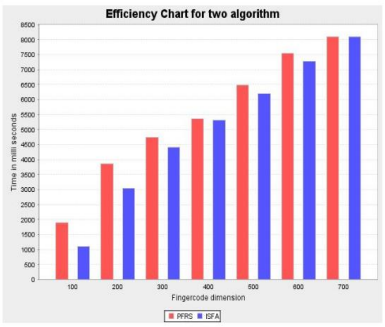

Fig 7: Efficiency chart

According to the suggested project, the computing complexity determines the scheme's performance in OASers, TA and consumers. The dimension of FingerCode, which impacts the length of a template and a consumer's inquiry, and further affects the computation difficulty in OASers, Trusted Authority, and consumers, is one of the elements that may affect the computation complexity in OASers. With the growing dimension of FingerCode, the computing cost of OASers, Trusted Authority, and consumers will linearly increase. The reason for this is that as the dimension of FingerCode grows, OASers will spend more time in the matching process, and TA will publish the dataset of a consumer's fingerprint templates to OASers, who will spend more time with the increasing of the dimension of FingerCode, and consumers will spend more time with the increasing of the dimension of FingerCode. As a result, our proposed scheme can achieve privacy-preserving fingerprint verification with low computation complexity in OASers, TA and consumers, and the overall overhead for a single whole fingerprint authentication service query and response time is estimated to be a few seconds, as shown in fig 8.

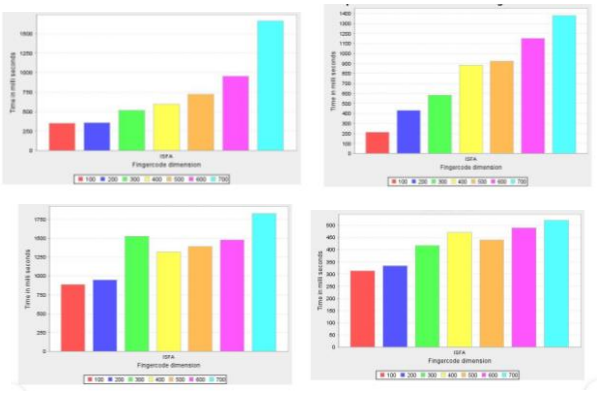

Fig 8: Computation Complexity

7.CONCLUSION

For online fingerprint authentication, the suggested solution is an ISFA-compliant security improvement mechanism. The Trusted Authority(TA), online authentication servers of internet services (OASers), and consumers are the three components of the ISFA approach. TA, which is similar to a government agency, is in charge of fingerprint template encryption and storage. OASers are similar to businesses like Amazon, Flipkart etc., and they should register in TA ahead of time. OASers will receive the consumers registration details and request TA for the related fingerprint templates. Consumers will be able to visit the website after registering and logging in with their fingerprint, which has previously been authorized by a trusted authority. The proposed technique can protect consumers fingerprints while also maintaining the confidentiality of matched templates. The underlying fingerprint identification system's accuracy will not be compromised. Consumers can obtain safe and accurate fingerprint authentication without disclosing fingerprint information in this way.

REFERENCES

[1] H. Zhu, X. Liu, R. Lu, and H. Li, "Efficient and privacy-preserving online medical prediagnosis framework using nonlinear svm," IEEE journal of biomedical and health informatics, vol. 21, no. 3, pp. 838–850, 2017

[2] G. P. Blanton M, "Secure and efficient iris and fingerprint identification," Biometric Security, 2015.

[3] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognition, vol. 37, no. 11, pp. 2245–2255, 2004

[4] A. Juels and M. Sudan, "A fuzzy vault scheme," Designs, Codes and Cryptography, vol. 38, no. 2, pp. 237–257, 2006.

[5] A. B. J. T. Ngo, David Chek Ling, Biometric Security. Cambridge Scholars Publishing, 2015.

[6] J. Pagliery, "Hackers stole 5.6 million government fingerprints - more than estimated," http://money.cnn.com/2015/09/23/technology/ opm-fingerprinthack/, September 2015.

[7] B. M. R. Dellys H N, Benadjimi N, "Fingerprint fuzzy vault chaff point generation by squares method," in 2015 7th International Conference of Soft Computing and Pattern Recognition (SoCPaR). IEEE, 2015, pp. 357–362.

[8] A. A. Nasiri and M. Fathy, "Alignment-free fingerprint cryptosystem based on multiple fuzzy vaults," in Artificial Intelligence and Signal Processing (AISP), 2015 International Symposium on. IEEE, 2015, pp. 251–255.

[9] J. Hartloff and V. Govindaraju, "Security analysis for fingerprint fuzzy vaults," Proceedings of SPIE - The International Society for Optical Engineering, vol. 8712, no. 4, pp. 1–12, 2013.

[10] Z. J. F. Q. HE Kang, LI Mengxing, "Fingercode based remote fingerprint authentication scheme using homomorphic encryption," Computer Engineering and Applications, vol. 49, no. 24, pp. 78–82, 2013.

[11] M. Barni, T. Bianchi, D. Catalano, and M. D. Raimondo, "A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates," in IEEE BTAS 2010, 2010, pp. 1–7.

[12] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," Image Processing, IEEE Transactions on, vol. 9, no. 5, pp. 846–859, 2000.

[13] Q. Wei, H. Zhu, R. Lu, and H. Li, "Achieve efficient and privacy preserving online fingerprint authentication over encrypted outsourced data," in 2017 IEEE International Conference on Communications. IEEE, 2017, pp. 1–6.

[14] M. Shen, B. Ma, L. Zhu, R. Mijumbi, X. Du, and J. Hu, "Cloud-based approximate constrained shortest distance queries over encrypted graphs with privacy protection," IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 940–953, 2018

[15] Details on the 192-bit prime field Weierstrass curve are accessible at https://neuromancer.sk/std/x962/prime192v1