

Next-Gen Authentication: Secure Login System Using Dynamic Biometric Passwords

Prof. Nikita Saindane¹, Pooja Vishwakarma², Kalyani Ghodake³, Manish Marndi⁴

¹ Professor, Dept. of Computer Engineering, PHCET, Maharashtra, India

^{2,3,4} UG student, Dept. of Computer Engineering, PHCET, Maharashtra, India

Abstract - With the accelerated development of digital technologies, user authentication has become a crucial requirement for ensuring both security and seamless access in modern web and mobile systems. Conventional authentication, including passwords and fixed credentials, are becoming susceptible to security attacks, such as, data breaches, replay attacks, and identity theft. To overcome these setbacks, this project will suggest a new generation authentication system which incorporates biometric authentication with mammoth cryptographic methods. This system encodes raw biometric data into a secure non-reversible template so that there should never be any sensitive user data stored or sent in plaintext. Moreover, the secure pairing mechanism is also applied to create trusted communication between the user devices and the authentication server. The solution proposed will increase the security level, ensure users privacy and enhance resistance to common attacks by cyber criminals but still be usable. It has been proven through experimental analysis that the system can deliver high authentication throughput with low computation cost and will also be useful in real-world use in security critical systems.

Key Words: Biometrics, Authentication, Passwords, One-Time Passwords (OTPs), SHA-256, Cyber Attacks, Phishing, Identity Theft

1. INTRODUCTION

User authentication is now a paramount issue with the rapid development of online services. Conventional password-based authentication methods are common and much susceptible to hacks like phishing on the internet, brute force and stealing of credentials. There is also an additional threat of unauthorized access and identity theft by vulnerable password practices and password reuse. In order to address these shortcomings, currently, authentication systems integrate passwords with other security appliances like One-Time Passwords (OTPs) and cryptographic hash functions. Nonetheless, these systems are also dependent on knowledge-based credentials that can be hacked or breached. The biometric authentication method is more secure as it is based on the personal characteristics of the user, however, it also has its privacy and security problems in terms of biometric data storage. This project is focused on the next generation authentication system and involves the application of biometrics combined with the use of safe cryptography systems to enhance security without violating user

privacy. The proposed system can provide enhanced security to cyber-attacks and the validity of identity verification. The current project is devoted to the next-generation authentication process that consists of a highly secure cryptography system and biometrics to enhance the security level and avoid any invasion of the user privacy. The proposed system can enhance its ability to check the identity and its ability to with-stand cyber-attacks.



Fig -1: Various types of existing Authentication Systems

2. BACKGROUND

The traditional process of user authentication has been with the help of using passwords. Password-based systems have been found wanting over years due to increasing complexity of cyber-attacks, including phishing, keylogging and brute-force attacks. Despite other security mechanisms such as hashed passwords and the use of One Time Password (OTPs), hackers still find exploitation in the vulnerability of the system and human factor. Biometric authentication systems are now in widespread use such as fingerprint and facial recognition, to enhance security verification. In spite of the fact that biometrics are more reliable because of their uniqueness, privacy issues, data leaks and irremovable biometric welfare are challenges. As a result of such limitations, advanced authentication systems that offer solid cryptographic technology and biometrics are currently needed in an attempt to guarantee high security and privacy of the users.

3. MOTIVATION

The rise in the rate of cyber-attacks and cases of identity theft has greater awareness of the inadequacy of old traditional authentication systems using passwords. Weak passwords are frequently reused by the users and they are easy targets of phishing and credential thefts. Even such improved techniques like OTPs and hashed passwords cannot stop advanced attacks completely. Biometric authentication is more secure though it also raises some issues regarding privacy and storage of biometric data in a safe manner. These issues influenced the creation of a new generation authentication system that integrates biometrics with cryptographic to improve security and at the same time provides user privacy, as well as minimize the use of passwords.

4. FUNDAMENTAL CONCEPTS

The main objective of this project is to provide a robust authentication mechanism by integrating biometric verification with cryptographic security methods.

Literature Review of the research papers:

1. Random Hash Code Generation for Cancelable Fingerprint Templates using Vector Permutation and Shift-order Process:

In their study, S. M. Abdullahi and S. Sun present a method for protecting fingerprint templates through the generation of random hash codes using vector permutation combined with a shift-order transformation process [1]. The proposed technique focuses on improving the security of biometric systems by generating cancelable fingerprint templates instead of storing original biometric data. In this method, fingerprint features are transformed into randomized hash values, making it difficult to recover the original biometric information from the stored templates and thereby enhancing data confidentiality.

Advantages: The proposed architecture enhances the protection of biometric data because of the absence of the necessity to store raw fingerprint data. Also, the mechanism of transformation allows the creation of new templates in case a template has been stored in the system previously, which enhances the privacy of the user and the flexibility of the systems.

Limitations: The method has several drawbacks despite the benefits of security since it adds extra processing overhead by including several steps of transformation in generating templates and in matching them. Besides, the methodology primarily focuses on securing biometric templates and

lacks the mechanisms of time-based authentication or suppressing replay attacks.

2. A Cancelable Templates for Secure Face Verification based on Deep Learning and Random Projections:

In the study conducted by A. Ali et al., a privacy-preserving face verification method is introduced that combines deep learning techniques with random projection mechanisms to generate cancelable biometric templates [2]. The proposed approach extracts deep facial feature representations and transforms them into protected templates through random projection operations. This transformation makes non-invertible representations, assuring that the templates stored cannot be used to reconstruct the original facial images. As a result, the method significantly increases the safeguarding of the biometric information even in situations where stored data could be compromised. Advantages: The framework increases security of Face-based authentication systems by eliminating the need to store unprocessed biometric features. The integration of deep learning contributes to improved feature extraction and recognition performance – Random projection provides template revocability and user privacy by producing transformed, cancellable representations. Limitations: The dependence on deep neural network models increases the computational requirements and may require higher processing power. Furthermore, the proposed method mainly deals with face verification security and does not account for any other authentication layers like multi-factor authentication or time-based authentication mechanisms.

3. A New Fuzzy Vault based Biometric System Robust to Brute-Force Attack:

In their work, A. F. De Abiega-Leglisse et al. present a biometric authentication framework based on the fuzzy vault cryptographic scheme to make it more resistant to brute-force attacks [3]. The proposed method for securing biometric information by linking biometric features with cryptographic keys in a fuzzy vault structure. This design conceals the true biometric data within many chaff points making it extremely difficult for an attacker to retrieve meaningful information even though the vault data is exposed. By combining cryptographic protection with biometric authentication: the system seeks to strengthen the security of biometric storage and verification (Overall) processes.

Advantages: The approach improves biometric protection by combining cryptographic key binding with biometric characteristics. The construction of the fuzzy vault increases resistance against brute force attempts and prevent direct exposure of original biometric information stored in the system.

Limitations: Although the technique requires complicated procedures for vault generation and decoding, which could yield an increased computational overhead. In addition, differences in the quality of biometric input data can impact on the reliability of the unlocking process. Possibly decreasing the accuracy of authentication.

4. Cancelable Biometric Template Generation Using Random Feature Vector Transformations:

In this study, R. S. P. Ragendhu et al. propose a technique for development of cancelable biometric templates via the application of random feature vector transformation methods [4]. The key concept of the approach is to protect biometric information by converting extracted biometric features into transformed representations that cannot be reversed to get the original data. By generating such protected templates, the system ensures that biometric credentials can be revoked and replaced if template is compromised, whilst still supporting dependable authentication performance

Advantages: The proposed method enhances the privacy of biometric systems – by avoiding the storage of raw biometric characteristics. The use of random feature transformations permits the creation of revocable templates, which reduces the likelihood of misuse of biometric data and enhances overall security.

Limitations: Transformed operations may increase computational demands at the time of template generation and verification. Furthermore, authentication performance might decline if the transformed feature space is not carefully designed/optimized, which may affect recognition accuracy.

5. EXISTING SYSTEMS

To enhance security and protect user identities in online applications and a number of studies have concentrated on improving digital authentication systems. The majority of existing solutions use password-based authentication, which is often combined with cryptographic hashing techniques and One-time Password (OTP) to avoid unwanted access. According to research, while these techniques provide some protection, they are still not safe from identity fraud, phishing attacks, and theft of credentials due to human error and credential reuse. Although some research has looked into using biometric authentication to enhance identity verify, problems of safe storing biometric data, privacy concerns, and irrecoverable data compromise still exist. These drawbacks illustrate that in order to successfully combat current

cyber threats; current authentication systems need more secure and more privacy-preserving strategies.

6. PROBLEM STATEMENT

Passwords and OTPs, which are the major constituents of current authentication systems, are extremely vulnerable to online threats such as phishing, identity fraud and credentials theft. System security is further compromised by weak password practices and password reuse, which is still exploited by attackers. Improper management and storage of biometric data is coming with great privacy and security concerns, even though biometric authentication provides more powerful identity authentication. Therefore, to ensure user identity protection and prevent unwanted access, next-generation authentication system that safely integrates the biometrics and cryptographic techniques is required.

7. PROPOSED SYSTEM

To overcome the security and usability issues with standard password and mechanism based on OTP, the proposed system provides a dynamic authentication approach. Based on time reliant credential generation, cryptographic key binding, cancellable biometric template, the system offers a safe authentication process in addition to ensuring that unprocessed biometric in this way data is never therefore revealed. Some of the weaknesses of traditional authentication systems such as password reuse, phishing attacks, replay attacks and in this case irreversible leakage of biometrics. The proposed system design eliminates these problems by ensuring that authentication credentials are dynamic, non-reusable and revocable.

The authentication workflow is divided into four main phases:

1. User registration
2. Device pairing
3. Login and authentication

Each phase performs a specific function to ensure the integrity and confidentiality of the overall authentication mechanism.

7.1. Phase of registration (Generation of Cancelable Biometric Templates)

The process of registration is when the user is enrolled into the system in a secure and private manner. In this step, the user gets to type in a specific identifier, and his/her biologi-

cal fingerprint is scanned with a biometric sensor. The fingerprint captured is handled by the biometric infrastructure and transformed into a standard ANSI fingerprint template which is normally held in the form of a byte array internally.

The format is standard, which means that the system is not reliant on a particular fingerprint sensor. The first step of the system is a cancellable transformation that ensures that this original biometric data can never be re-obtained prior to this fingerprint template being directly stored. To achieve this, a shuffle seed is generated with the help of the SHA-256 hash function. The identifier used by the user is site specific salt and the public key of the mobile device and the identifier is used to generate the hash. Such a combination of the same fingerprint will give different templates despite the possibility of using the same fingerprint on a different platform or device. Based on the generated hash value, a pseudo-random number generator (PRNG) is set up. This Permutation of the template indices in a pre-determined way. Permutation is used to randomize the fingerprint template, which removes the native spatial organization of the fingerprint and makes it difficult to recreate the familiar biometric print.

To create a more tolerant system as to minor differences certain variations during fingerprint capture, the shuffled template is split into a number of fixed-size pieces. Each segment has representative features which are computed by simple algorithms such as taking the highest value or computing a checksum. These values extracted are then pooled with each other to create a fixed length feature vector.

The last step is the encoding of this feature vector using the Base64 encoding algorithm to form the cancellable biometric template, denoted CT_{web}. The resultant template can support secure authentications and cryptographic functions since once it has been created; one can no longer reverse it to extract the original fingerprint and can be repaired in case requirements change.

7.2. Device Pairing Phase (QR-Based Secure Exchange)

The stage of device pairing with the device authentication decides a secure connection between the mobile authentication device of the user and the web application. This system adds a CT_{web} and minimum information on services-related data into a QR code upon generating the cancellable template. The first time the user goes through the setup process, the QR code is displayed to the user. The user uses the mobile authentication application to read the QR code and the pairing protocol is activated. In this process, the mobile device transmits the server the public key and creates or ob-

tains its asymmetric key pair. The server then encrypts CT_{web} with this public key and it sends encrypted information back to the mobile application.

The encrypted template can only be decrypted within the paired device because it has the corresponding private key. The step ensures that authentication credentials cannot be copied or used on other not authorized devices. After being decrypted, the template is stored safely in the mobile application, and this process has been paired.

7.3. Login Phase (Dynamic Password-Based Authentication)

Authentication is done at the stage of logging in without the user being required to recall and use a constant password. The user logs into the mobile application and his/her local fingerprint verification are done. This on-site authentication helps to ascertain that biometric matching is done fully on the trusted device.

The mobile application creates a dynamic authentication password based on the successful verification with the hash function which is the hash-256. The cancellable biometric template, the current time-stamp and the salt that is site-specific are all that is inputted into the hash function. The authentication credential generated is a short-lived value based on the truncated hash value to an alphanumeric format.

The web application takes the generated dynamic password, and the server determines the expected value separately by use of the same parameters. Authentication will only be granted on submission and calculation of values that are equal and the time falls within the stipulated time. This design ensures that each authentication attempt is one-time and can never be duplicated.

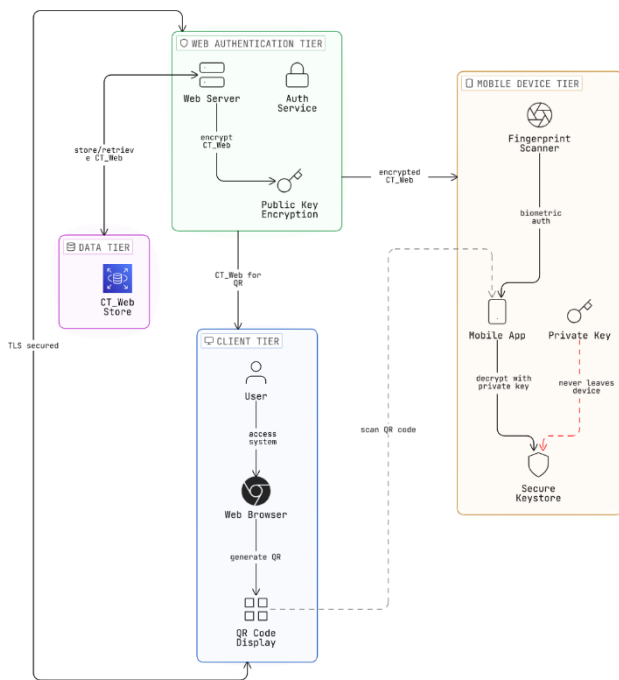


Fig -2: System Block Design

8. METHODOLOGY

The methodology of this work is aimed at developing and testing of the secure authentication system that would exclude the OTP-based verification and unchangeable passwords. The suggested approach will enhance the level of security, at the same time considering the application specific usability and practicality. The development process had several stages. It started on making system requirements, system design, implementation of biometric processing techniques and lastly, by evaluating the security of the proposed system.

1. Requirement Identification:

The first stage involved analyzing commonly used authentication mechanisms and identifying their limitations. Even though password-based authentication systems are widely used, they are vulnerable to phishing attacks, reuse of passwords, and use of weak passwords. OTP-based systems enhance security, but have delays and depend on third-party communication systems such as SMS or email. Biometric authentication is very secure, but it may be a matter of concern to store raw biometric data indefinitely, as doing so may compromise the privacy of the users. These observations were used in defining the requirements of the system. The system must not be reusable of credentials; it must also secure biometric data and must be easy to use by the user. The

other requirement was the ability to revoke and reissue authentication credentials in case of a compromise.

2. Methodology for System Design:

The overall architecture of the system was developed following the definition of the requirements. A mobile based authentication model was selected to enable the biometric verification to be performed on the user device. This method will decrease the vulnerability of biometric information and restrict the size of sensitive data stored in the server.

Some of the independent modules of the system were biometric processing, device pairing and authentication verification. This modular design allows one to easily manage the system and be able to modify or enhance a particular component without having any effect on the whole system.

3. Biometric Processing and Template Generation:

The use of fingerprint biometrics was chosen due to its ability to have a universal application in modern hardware and the ability to offer high-quality identification. When the fingerprint is registered, a standard ANSI fingerprint template is created through transformation of the captured fingerprint image. This will ensure that different fingerprint sensors are compatible. The original template is not stored but a cancellable transformation method is applied. With user and device specific parameters a cryptographic hash is generated, and the value limits the process of shuffling of the templates. In turn, the structure of the original fingerprint is distorted by the modified template. A shuffled template is divided into smaller pieces to ensure that it is made more uniform. Each segment generates representative features which are joined to create a fixed length representation. This last representation is the cancellable biometric template on which authentication is done.

4. Pairing of devices securely:

When the biometric template is created, it should be secured to the mobile device of the user. This is done in the first stage of registration wherein a pairing system is applied using a QR code. The biometric template would be scanned by the mobile application coded in a QR code. Asymmetric encryption is used to protect the data which is being transmitted. The mobile application will decrypt the encrypted data with the associated private key and the template will be encrypted with the public key of the mobile device. This will ensure that the authentication credentials are never related with more than one trusted device.

5. Authentication and Login Process:

There is minimal interaction of the user with the mobile application except when it comes to logging in. The application will first do local fingerprint verification in order to verify the user. A dynamic password is generated after the successful verification is realized using a cryptographic hash function. Password is the combination of cancellable biometric template, up-to-date time and site-specific parameter. The password is time dependent, meaning that it is not valid over a long period of time.

The password generated is then given to the web server to be verified. The server determines the expected value independently and compares it with the received password. In case the values are identified as being the same within the given time slot, access is provided.

6. Security Assessment:

The proposed system was evaluated against several common security threats. Phishing attacks, replay attacks, and the unauthorized reuse of credentials are examples of these. Also looked at were scenarios involving intercepted authentication data. Because the system does not store raw biometric data, the risk of biometric information leakage is significantly reduced. Additionally, the use of cancellable biometrics this means that new templates can be generated if needed, ensuring that compromised credentials can be changed.

9. ALGORITHMIC REPRESENTATION

Algorithm 1: Cancellable Biometric Template Generation

Input: Fingerprint F , User ID UID , Site Salt S , Device Public Key PK

Output: Cancellable Template CT_{web}

1. Convert the fingerprint F to ANSI template T
2. Compute $Seed = SHA-256(UID | S | PK)$
3. Initialize PRNG using $Seed$
4. Generate permutation P
5. Apply permutation P to template T to get $T_{shuffled}$
6. Split $T_{shuffled}$ into fixed-size segments
7. Extract stable biometric features of each segment
8. Combine extracted features into feature vector V
9. Encode V using Base64 to get CT_{web}
10. Return CT_{web}

Algorithm 2: Secure Device Pairing

Input: Cancellable Template CT_{web}

Output: Securely stored template on mobile device

1. Encode CT_{web} into a QR code
2. Scan the QR code using the mobile application
3. Mobile device sends public key PK to the server
4. Server encrypts CT_{web} using the received public key PK
5. Forward the encrypted template to the mobile device
6. Mobile device decrypts the template, using its private key
7. Keep the decrypted template securely on the mobile device

Algorithm 3: Dynamic Authentication Process

Input: Cancellable Template CT_{web} , Timestamp T , Site Salt S

Output: Authentication Result

1. Compute dynamic password
 $DP = Truncate (SHA-256(CT_{web} | T | S))$
2. Submit DP to the authentication server
3. Server calculates expected dynamic password DP_{server}
4. If $DP = DP_{server}$ and timestamp T is between the valid time window
Grant authentication access
5. Else
Reject authentication request

9. SECURITY ANALYSIS

A. Dynamic Credential Generation

In the authentication process, the system calculates a dynamic password (DP) based on the biometric template that can be cancelled and time-based parameters.

Let the cancellable biometric template created at the time of enrolment be indicated as CT . The dynamic credential is calculated using a cryptographic hash function:

$$DP = Truncate (SHA-256(CT \parallel Ts \parallel S))$$

Where,

CT is the cancelable biometric template,

Ts is the current timestamp,

S contains a system specific salt value.

Since the timestamp is constantly changing, the generated credential becomes unique for each authentication session and remains valid only within a predetermined time window, which greatly reduces the likelihood of credential reuse.

B. Biometric Template Protection

The system uses a transformation function to create a cancelable template in place of storing raw biometric data:

$$CT = T(B, s)$$

Where,

s is a transformation seed,

B is the extracted biometric feature vector. This procedure guarantees that the original biometric data cannot be recovered by reversing the stored template. This feature offers template revocability, which is a significant drawback in traditional biometric systems.

In the event of a possible compromise, a new template can be created using a different transformation seed:

$$CT' = T(B, s')$$

This approach enhances the security of the authentication system, it ensures that even if transformed template is exposed, it is not reusable or linked to the original biometric data.

As a result, this system maintains both privacy and security while also supporting authentication of users in a secured locked system.

C. Attack Resistance Analysis

| Attack Resistance Analysis | | | |
|----------------------------|--------------------------------------|----------------------------------|---|
| Attack Type | Password-Based System | OTP-Based System | Proposed NextGen System |
| Phishing Attack | High risk due to credential exposure | Moderate risk if OTP intercepted | Resistant due to biometric verification |

| | | | |
|----------------------|----------------------------------|-------------------------------------|---|
| Replay Attack | Possible if credentials captured | Possible within OTP validity window | Prevented by time-based dynamic password |
| Brute Force Attack | Possible with weak passwords | Limited protection | Extremely difficult due to hash-based credential generation |
| Credential Theft | Password leakage possible | OTP interception possible | No reusable credentials available |
| Device Impersonation | Possible from any device | Possible if OTP accessed | Prevented through secure device pairing |

With the elimination of the stagnant or reusable credentials that are actively used in traditional password and OTP-based systems, the proposed Next-Gen authentication framework improves security.

Alternatively, authentication is performed using cancelable biometric templates and time-sensitive dynamically generated credentials by using cryptographic hash functions. This strategy reduces the chances of replay attacks and the use of credentials since each authentication value can be unique and only last for a given time.

Besides that, the device pairing mechanism also limits unauthorized access to devices unless their account information is exposed, by enabling the authentication of only a registered mobile device.

The proposed system's resistance to common security attacks is compared to that of conventional authentication methods in Table 1.

D. Security Feature Comparison

The suggested system's security features were also contrasted with other conventional authentication methods. The proposed framework combines several security features that together lower the attack surface and improve authentication reliability.

| Security Feature Comparison | | | |
|-------------------------------|-------------------------|--------------------|-----------------|
| Security Feature | Password Authentication | OTP Authentication | Proposed System |
| Static Credentials | Yes | Yes | No |
| Biometric Verification | No | No | Yes |
| Dynamic Credential Generation | No | Yes | Yes |
| Device Binding | No | No | Yes |
| Replay Attack Protection | Low | Medium | High |
| Template Revocability | Not Applicable | Not Applicable | Supported |

E. Authentication Workflow Security Model

The first steps of the authentication procedure are fingerprint collection and obtaining the biometric features. An encrypted copy of the features extracted is stored in a cancellable template on the corresponding mobile device, which is safe.

A hash function and parameter of a timestamp are used

to generate a dynamic password during log in using the template. The generated credential is forwarded to the server before access is granted and the credential is authenticated within a stipulated time.

The multi-stage startup of the authentication process enhances the resistance to common authentication attacks by making the authentication credentials both time-dependent and device-bound and inapplicable.

Security Architecture of Biometric Authentication System

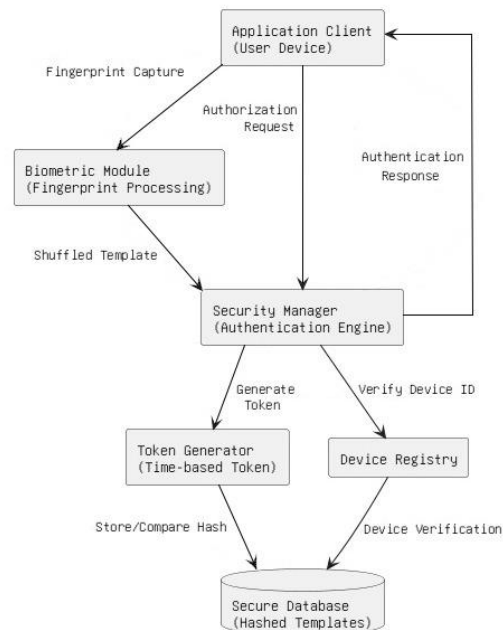


Fig -3: Security Model

10. PERFORMANCE ANALYSIS

Computational efficiency, authentication latency and system overhead of the proposed next generation authentication framework were investigated when using a login process. Authentication algorithm comprises the operations of biometric feature extraction, cancelable template transformation, dynamically generated password by cryptographic hash generation, and server validation. Each of these stages affects the overall time and money used in the computation of the authentication process. The suggested approach does not require any external credential delivery procedures such as SMS or email as compared to traditional authentication protocols such as password-based and

OTP-based authentication. Rather than that, the cancelable biometric template along with time-sensitive parameters is stored and used to form a dynamic password on the paired mobile device. This minimizes the dependency on a network and enhances the speed of authentication as well as ensuring high level of security.

Three evaluation aspects - the comparison of authentication time, the comparison of computational cost, and the distribution of system overhead - were examined in order to gain a deeper comprehension of the system's performance characteristics. The figures that follow provide an illustration of the outcomes.

A. Authentication Time Comparison:

This graph compares the average time of authentication require by the proposed NextGen authentication system, OTP-based authentication and the conventional password-based authentication. Although using OTP based systems increases more delays through network transmission and message delivery, password-based authentication normally consists of small processing time through credential verification. The proposed solution, in contrast, generates advantageous credentials locally on the connected device significantly decreasing the authentication latency, preserving strong security controls.

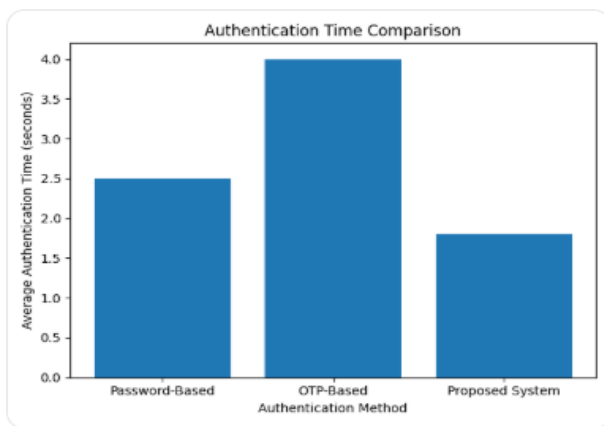


Chart -1: Authentication Time Comparison

B. Computational Cost Comparison:

This chart gives the relative computation cost of different authentication methods at different operating phases. Whereas OTP-like systems introduce an additional network cost, traditional password systems use mostly static credentials and require very little computation. Due to its efficient authentication procedures and Cryptography hashing lightweight, the proposed authentication system supports the biometric processing and low computation complexity. Greater security is thereby achieved by the system without straining computing cost to the system.

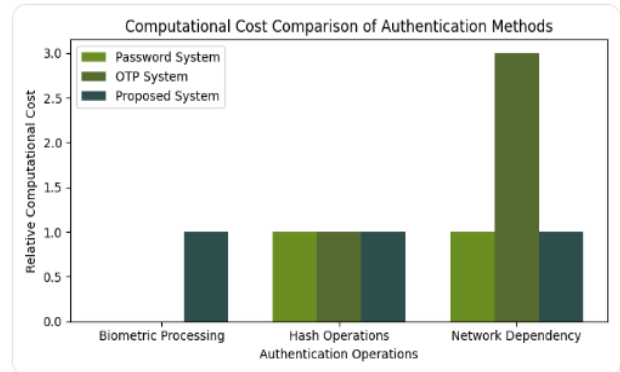


Chart -2: Computational Cost Comparison

C. Authentication Latency Breakdown:

| Authentication Latency Table | |
|------------------------------|-------------|
| Stage | Approx Time |
| Biometric extraction | 2 secs |
| Template transformation | 1.5 secs |
| Dynamic password generation | 2.5 secs |
| Server verification | 1 secs |

D. System Overhead Distribution:

The pie chart presents the distribution of the computational load between the different stages of the proposed authentication process. Biometric feature extraction takes the largest candidates of processing costs since it needs the gathering and address of fingerprint data so as to offer a consistent feature representation. The leftover overhead is further divided into server-side validation, hashing-based dynamic sorting of passwords and template customization. The overall system overhead is at balanced level and suitable in real time authentication where there is an additional biometric processing step

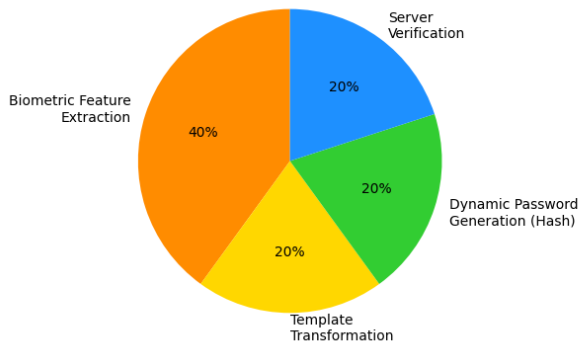


Chart -3: System Overload Distribution

11. RESULT ANALYSIS

Step 1.

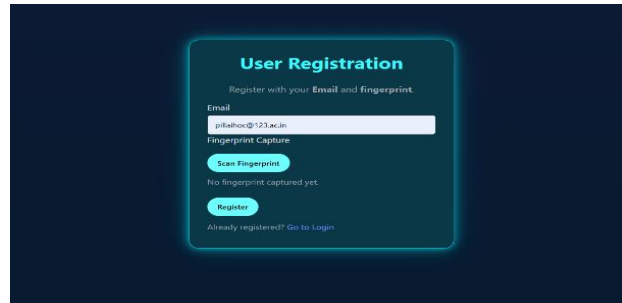


Fig -4: User Registration with Biometric Input

The foregoing figure shows the process of registering with the user having a username and fingerprint input with which the user gains biometric enrollment.

Step 2.

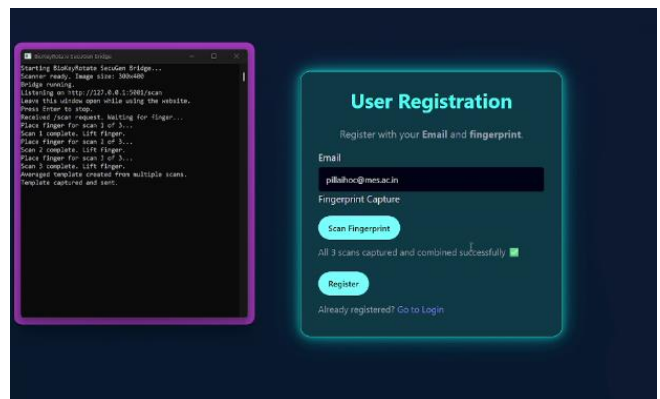


Fig -5: Stable Finger Template Generation

This figure indicates that the fingerprint is scanned thrice to come up with a stable and dependable biometric template that one can be authenticated against.

Step 3:



Fig -6: QR Code Generation for Device Pairing

D. Discussion of Network Dependency and Scalability

Compared to the traditional OTP-based authentication systems, the proposed authentication framework can reduce network dependence to a significant degree. Traditional OTP authentication will require external communication services such as email delivery services or SMS delivery services and this will introduce latency and may fail when network connectivity is low. Conversely, the proposed approach considers parameters based on time and the template of cancellable biometrics to generate dynamic authentication credentials at the local levels of the connected mobile device. This approach will ensure faster authentication even within limited network environments and eliminate the delay in the delivery of messages.

The system in question is, in terms of scalability, sufficient to split computational workload between the authentication server and a client device. Lightweight hash verification and timestamp validation are only done by the server, the mobile device locally generates the dynamic password.

The authentication server can also accept a number of simultaneous authentication requests without a noticeable performance degradation as these processes need not demand much processing units. This design allows the proposed authentication system to be deployed in large-scale applications such as financial applications, business applications and learning systems.

The figure depicts the creation of QR code that is used to securely link the user's mobile device with the web application

Step 4:



Fig -7: Mobile Application Detecting Linked Account

The figure above indicates that the registered account of the user is detected by the mobile application and ready to create a secure device connection.

Step 5:



Fig -7: QR Code Scanning for Secure Connection

This figure demonstrates that the mobile application is scanning the QR code establishing a secure connection with the web server.

Step 6:

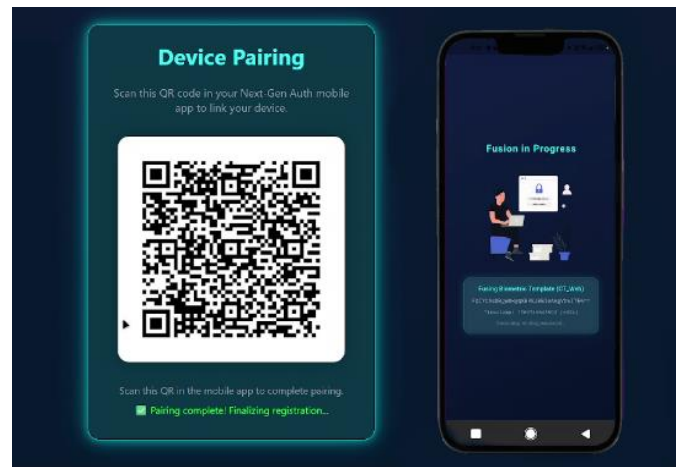


Fig -7: Secure Storage of Encrypted Biometric Template

The above figure depicts the encrypted biometric template being securely stored on the user's mobile device to prevent unauthorized access.

Step 7:

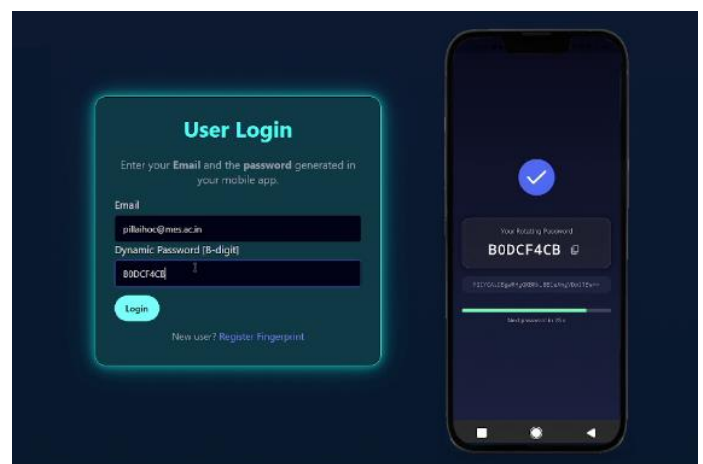


Fig -8: User Login with Dynamic Password

The figure above depicts the log-in procedure to the user involving entering the email and dynamically generated password of the mobile application.

Step 8:

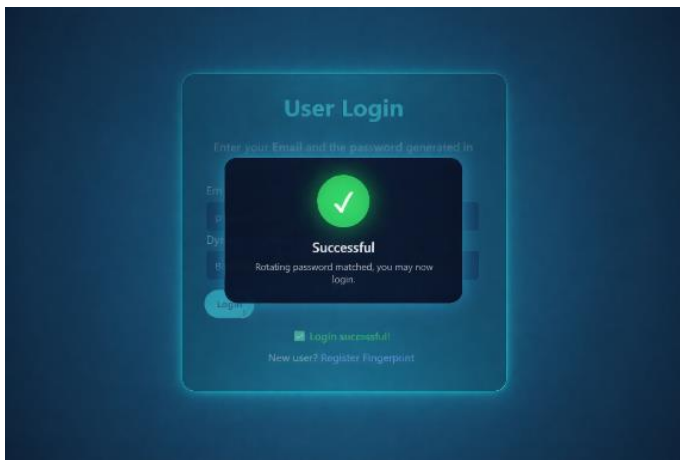


Fig -9: Successful Authentication Verification

Here the figure depicts that authentication succeeded following dynamic password validation on client as well as server side.

11. CONCLUSIONS

The constraints of the conventional password and OTP-based authentication tools were overcome by creating a secure authentication system in this project. The current systems have frequently been associated with security problems that include the reuse of passwords, phishing attacks, and the occurrence of data leakages, therefore, driving the desire to establish a superior solution.

The suggested system applies the applications of biometric data in a privacy-saving manner of transformation in a format of a cancellable and irreversible data format. Raw biometric information is not at any point stored or transmitted, which is an added security to user identity. Security is also enhanced by the device bonding and time authentication which makes sure that the set of the login credentials cannot be reused or abused.

In general, the system shows that the strong authentication may be implemented without the user facing the complexity increment. The method is feasible, safe, and can be applied in the fields where the high level of reliability and security is needed like in a banking systems and educational platforms.

ACKNOWLEDGEMENT

It is a privilege for us to have been associated with Prof. Nikita Saindane our guide, during this project work. We have

greatly benefited from her valuable suggestions and ideas. It is with great pleasure that we express our deep sense of gratitude to them for their valuable guidance, constant encouragement, and patience throughout this work. We are also indebted to our guide for extending the help to academic literature. We would also like to acknowledge Ryan Gosling as a source of inspiration and motivation.

REFERENCES

- [1] S. K. Sahoo, S. C. Das, and S. Bakshi, "Random Hash Code Generation for Cancellable Fingerprint Templates," *IEEE Transactions on Information Forensics and Security*, vol. 20, no. 5, pp. 567–576, May 2025, DOI: 10.1109/TIFS.2025.3399874.
- [2] M. Gomez-Barrero, J. Fierrez, and J. Galbally, "Cancelable Template for Secure Face Verification Based on Deep Learning and Random Projections," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2747–2762, Nov 2018, DOI: 10.1109/TIFS.2018.2833040.
- [3] P. Drozdowski, C. Rathgeb, C. Busch, and A. Uhl, "OTB-Morph: One-Time Biometrics via Morphing," in *Proceedings of the 2023 International Conference on Biometrics (ICB)*, Crete, Greece, 2023, pp. 1–8, DOI: 10.1109/ICB57460.2023.10199205
- [4] A. Juels and M. Sudan, "A New Fuzzy Vault Based Biometric System Robust to Brute-Force Attack," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, Feb. 2006, DOI: 10.1007/s10623-005-6343-z.
- [5] M. El-Abed, M. Gomez-Barrero, and J. Fierrez, "Cancelable Multimodal Biometrics Based on Chaotic Maps," *Pattern Recognition Letters*, vol. 165, pp. 57–65, Apr. 2023, DOI: 10.1016/j.patrec.2023.01.009.
- [6] M. El-Abed, M. Gomez-Barrero, and J. Fierrez, "Cancelable Multimodal Biometrics Based on Chaotic Maps," *Pattern Recognition Letters*, vol. 165, pp. 57–65, Apr. 2023, DOI: 10.1016/j.patrec.2023.01.009.
- [7] A. Kumar and D. Zhang, "Cancelable Palmprint: Intelligent Framework Toward Secure and Privacy-Aware Recognition System," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 54, no. 3, pp. 1182–1195, Mar. 2024, DOI: 10.1109/TSMC.2024.3345612.
- [8] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 1, pp. 1–17, Jan. 2008, DOI: 10.1155/2008/579416.
- [9] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint Image Reconstruction from Standard Templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007, DOI: 10.1109/TPAMI.2007.1097.
- [10] M. Gomez-Barrero, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Cancelable Biometrics: A Comprehensive Survey," *Pattern Recognition*, vol. 82, pp. 93–105, Oct. 2018, DOI: 10.1016/j.patcog.2018.04.023
- [11] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, "Secure Biometrics: Concepts, Authentication Architectures, and Challenges," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 51–64, Sep. 2013, DOI: 10.1109/MSP.2013.2266951.