Global Scientific JOURNALS

GSJ: Volume 13, Issue 3, March 2025, Online: ISSN 2320-9186
www.globalscientificjournal.com

OTP SCAM – SECURITY USING TONGUE PRINT BIOMETRIC AUTHENTICATION

NIVETHA V
Department of Computer Science And Engineering
Dr. M.G.R. Educational and Research Institute
Deemed to be University
nivethav2403@gmail.com

HAARINI M
Department of Computer Science And Engineering
Dr. M.G.R. Educational and Research Institute
Deemed to be University
haarumurugan0@gmail.com

SHEEBA R
Department of Computer Science And Engineering
Dr. M.G.R. Educational and Research Institute
Deemed to be University
sheebafrancy61@gmail.com

DR. S MOHANDOSS
Associate professor
Department of CSE
Dr. M.G.R. Educational and Research Institute
Deemed to be University
mohandoss.cse@drmgrdu.ac.in

DR.E.R RAMESH
Assistant professor Faculty of Center of Excellence in Digital Forensic
rameshvani@gmail.com

MS.MAGNAYADLAPALLI
Assistant professor
Faculty of Center of Excellence in Digital Forensic
magna.coedf@gmail.com

Abstract

Criminals often exploit OTP sharing to access victims' bank accounts. To enhance security, we propose integrating tongue print biometric verification after the OTP session. Like fingerprints or iris patterns, tongue prints are unique and complex, featuring distinct papillae, ridges, and textures that can be captured digitally for secure authentication. Unlike fingerprints, tongue prints are non-invasive and hygienic, as they require minimal contact during imaging. This technology provides a robust layer of security, preventing unauthorized access and enabling its application in banking, secure facilities, and electronic devices.

Keywords—Tongueprint biometric, Papillae, authentication

I. INTRODUCTION

With the increasing reliance on One-Time Passwords (OTPs) for secure transactions in banking, e-commerce, and other online services, OTP scams have become a major cybersecurity concern. Cybercriminals exploit social engineering techniques, phishing, and SIM swapping to intercept or manipulate OTPs, leading to financial fraud and identity theft. Traditional OTP-based authentication methods are vulnerable to such attacks, making it crucial to implement stronger security measures. This project introduces **Tongue Print Biometric Authentication** as an additional layer of security for OTP verification. Tongue prints, like fingerprints, are unique to individuals and provide a non-replicable biometric trait, making them highly secure against spoofing attempts. Unlike fingerprints or facial recognition, tongue prints offer a less exploitable authentication method due to their internal positioning and unique texture patterns.

The primary objective of this project is to develop a **web-based authentication system** that integrates OTP verification with **tongue print recognition** for enhanced security. The system will include a secure sign-up and login process, where users register with their phone number and tongue print data. During authentication, an OTP will be sent via SMS, and the user will be required to verify their identity using a real-time tongue scan via a webcam. Advanced **image processing and machine learning** techniques will be used to analyze and verify tongue prints, ensuring accurate and secure user authentication. A secure **backend database** will be implemented to store encrypted biometric data and authentication logs, safeguarding user information from unauthorized access.

By integrating biometric authentication with OTP security, this project aims to **mitigate OTP fraud** by ensuring that even if an OTP is stolen, only the legitimate user can complete the authentication process. The system will incorporate **encryption, secure communication protocols, and fraud detection algorithms** to protect against potential cyber threats. The significance of this project lies in its ability to enhance cybersecurity by reducing fraud risks associated with **phishing, SIM swapping, and OTP interception**. As biometric authentication continues to evolve, tongue print recognition offers a promising, **non-intrusive, and highly secure authentication method** that can revolutionize secure access systems. This research contributes to the fields of **cybersecurity, biometrics, and user authentication**, paving the way for more advanced and fraud-resistant security mechanisms in digital transactions.

METHODOLOGY

The methodology for implementing **OTP Scam – Security Using Tongue Print Biometric Authentication** involves a structured approach that integrates biometric recognition with OTP-based verification to enhance security. The process begins with the **system design and development**, where a web-based authentication platform is created using frontend technologies like **HTML, CSS, and JavaScript**, while the backend is built with **Python/Django or Node.js**. A secure database, such as **MySQL or MongoDB**, is used to store user credentials and biometric data, ensuring encrypted communication between the client, server, and database.

During **user registration**, individuals provide personal details, a phone number, and a password. The system prompts users to capture **multiple tongue print images using a webcam**, which are preprocessed for feature extraction. To verify the authenticity of the registration, an **OTP is sent via SMS** to the registered phone number, and users must enter it for validation. The extracted tongue print features are **encrypted and securely stored** in the database for future authentication, ensuring protection against unauthorized access.

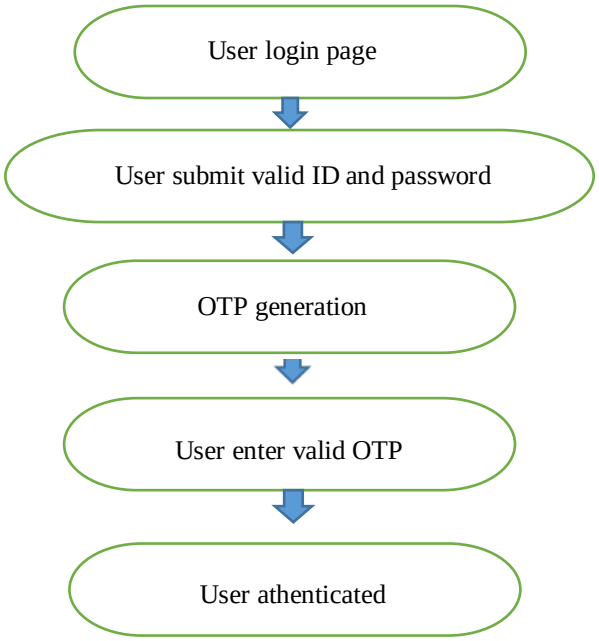
For the **login process**, an **OTP is generated and sent via SMS** to the registered phone number. The user must enter the OTP within a limited time frame to proceed. If the OTP is incorrect or expired, authentication fails, preventing unauthorized logins. After successful OTP verification, the system initiates **tongue print biometric authentication**, prompting the user to capture a **real-time tongue print image using a webcam**. The captured image undergoes **preprocessing techniques** such as grayscale conversion, noise reduction, and edge detection to extract distinct features. A **machine learning model (such as CNN or SVM)** is used to compare the new tongue print with the stored biometric data. If the tongue print matches, authentication is successful, and access is granted. If there is a mismatch, the system denies access, ensuring that even if an OTP is compromised, unauthorized users cannot bypass biometric verification.

To ensure **secure data processing and storage**, all biometric and authentication-related data are **encrypted using cryptographic algorithms** before being stored in the database. The system implements **secure communication protocols (SSL/TLS encryption)** to protect data transmission between users, the server, and the database. Additionally, **fraud prevention mechanisms** such as liveness detection, anomaly detection for unusual login attempts, and multi-layer authentication are incorporated to prevent spoofing attacks and unauthorized access. This

methodology provides a **robust and fraud-resistant authentication system**, ensuring a **high level of security against OTP scams and cyber threats**.

EXISTING SYSTEM

The existing authentication system primarily relies on **OTP-based verification**, where a **One-Time Password (OTP)** is sent via SMS or email and must be entered within a limited time to grant access to online services like **banking, e-commerce, and digital platforms**. While this adds a layer of security, OTP authentication is **highly vulnerable to fraud**, including **phishing, SIM swapping, OTP interception, and social engineering attacks**, where hackers manipulate users into revealing their OTPs or intercept messages using malware. To enhance security, some platforms implement **multi-factor authentication (MFA)** by combining OTP with **fingerprint or facial recognition**, but these biometrics can still be **spoofed using lifted fingerprints, high-resolution images, or deepfake technology**. Additionally, **SMS-based OTPs depend on mobile networks**, making them unreliable in poor connectivity areas, and if a user's phone is **lost, stolen, or hacked**, their accounts become easily compromised. Due to these vulnerabilities, **OTP-based authentication alone is not fully secure**, necessitating the development of a **fraud-resistant system** like **tongue print biometric authentication**, which is **unique, internal, and difficult to forge**, ensuring **stronger security and preventing unauthorized access**.



SYSTEM IMPLEMENTATION

1. **Frontend Development**

   The user interface is built using **HTML, CSS, and JavaScript**, integrating **OTP and biometric authentication** for smooth user interaction.

2. **Backend Development**

   The server-side is developed using **Python (Django/Flask) or Node.js**, handling **user requests, OTP generation, biometric processing, and authentication logic**.

3. **Database Management**

   A secure database (**MySQL/MongoDB**) stores **encrypted user credentials, OTPs, and tongue print biometric data** for authentication.

4. **User Verification**

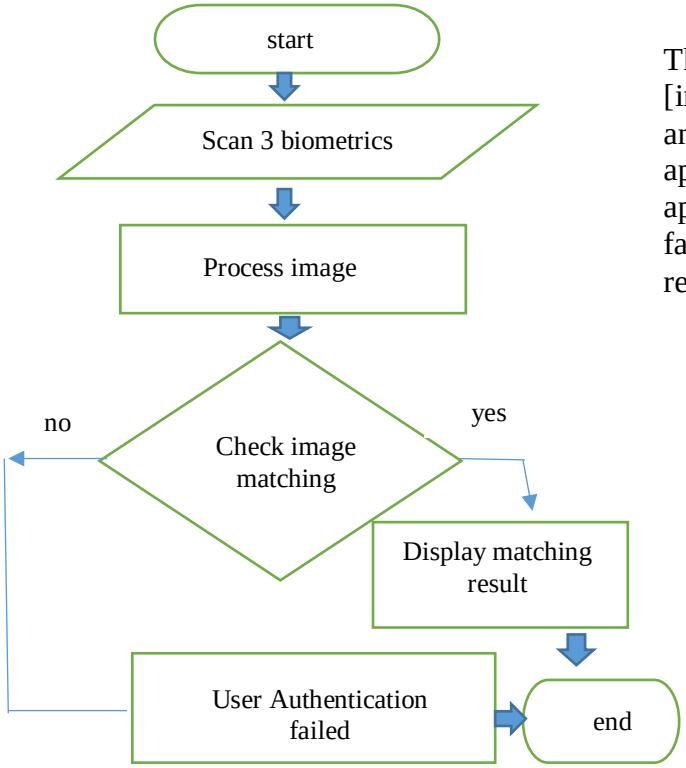
   During registration, users provide **personal details and a phone number**, followed by **OTP verification** to confirm their identity before storing biometric data.

5. **OTP Generation and Verification**

   A **random OTP is generated and sent via SMS**, which the user must enter within a **limited time** for authentication.

6. **Tongue Print Biometric Authentication**

   A **webcam captures a real-time tongue print image**, which undergoes preprocessing and is compared with stored biometric data using **machine learning algorithms** for final verification.



CONCLUSION

In conclusion, tongue print biometric authentication offers a groundbreaking solution to enhance online security, particularly against OTP scams. This project demonstrated the potential of integrating tongue print recognition into a secure login system with OTP verification, adding layers of protection to mitigate unauthorized access. By leveraging the unique and stable features of tongue prints, the system provides a secure, non-invasive, and tamper-resistant authentication method. Testing showcased seamless integration and usability, validating its effectiveness as a credible solution. Future advancements in AI and machine learning can further refine accuracy and adaptability. Widespread adoption across industries like banking, healthcare, and e-commerce could revolutionize identity verification, reducing fraud and boosting trust. Replacing vulnerable OTP methods with tongue print biometrics significantly minimizes interception risks and enhances security. This innovative technology paves the way for a more secure and reliable digital identity verification system, safeguarding online interactions in the modern era.

ACKNOWLEDGMENTS

The authors sincerely thank [institution/organization name] for their support and resources, and [specific individuals, if applicable] for their invaluable guidance. We also appreciate our colleagues for their insights and our families for their encouragement throughout this research.

REFERENCES

1. Caya, M. V., Caringal, M. E., & Manuel, K. A. (2021). Tongue Biometrics Extraction Based on YOLO Algorithm and CNN Inception. 2021 IEEE 13th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM). Manila, Philippines: IEEE
2. Chu, H., Ji, Y., Zhu, D., Ye, Z., Tan, J., Hou, X., & Lin, Y. (2023). Artificial Intelligence in Tongue Image Recognition. International Journal of Software Science and Computational Intelligence.
3. Narang, B., Palaskar, S., Patil, S., & Bartake., A. R. (2020). Tongue Scanning As a Biometric Tool: A Review Article. International Journal of Health Sciences and Research.
4. Hingad, N., Kumar, G., Singh, K., Mahajan, A., Singh, M. P., & Gambhir, R. S. (2024). Tongue print as a valuable biometric and forensic tool: A digital photographic study. Nigerian Medical Journal,
5. Nimbulkar, G., Patil, R., Nathani, S., Salve, S., Chhabra, K. G., & Reche, A. (2020). Tongue Prints: A Forensic Review. Indian Journal of Forensic Medicine & Toxicology,
6. Obaid, A. S., Kamil, M. Y., & Hamza, B. H. (2023). People identification via tongue print using fine-tuning deep learning. International Journal of Reconfigurable and Embedded Systems
7. El-Din, A. G., El-Meligy, M. G., El-Meligy, O. A., & El-Bialy, A. H. (2023). Digital Personal

Identification: Tongue as a Forensic Gratuity. *Egyptian Dental Journal*

8. *Manna, A., & Khan, T. (2023). Tongue prints—Unique as well as potential forensic tool for biometric authentication. Archives of Dental Research*
9. *Bhattacharyya, A., Koley, S., Dash, K. C., & Mahapatra, N. (2020). Tongue print: A unique biometric and potential forensic tool: A review. Oral Maxillofac Pathol J*
10. *Venkatesh, S. B., Kamath, V., Hasbullah, N. B., & Mutalib, N. S. S. B. A. (2020). A preliminary study of tongue prints for biometric authentication. Shiraz E-Medical Journal, 21(1), e96049*