IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

TRUSTFACE: A FACIAL RECOGNITION BASED SECURE DIGITAL TRANSACTION SYSTEM USING AWS REKOGNITION

[1]Abhijeet Dutta, [2]Ms. J. Buvana

[1]Student, [2]Mentor

[1]Artificial Intelligence and Data Science,

[1]Sri Venkateswara College of Engineering, Chennai, India

Doi: https://doi.org/10.56975/ijcrt.v14i7.309003

Abstract: With the increasing reliance on digital platforms for financial transactions and secure access systems, ensuring robust user authentication has become a critical challenge. Traditional authentication mechanisms such as passwords and PINs are highly vulnerable to phishing, credential theft, and replay attacks. While facial recognition provides a convenient biometric alternative, it remains susceptible to spoofing attacks using images, videos, or deepfake content. This paper presents TrustFace, a cloud-native, AI-powered face liveness detection system designed to verify real-time human presence during authentication. The system integrates multi-factor authentication using credential validation, facial recognition, and real-time liveness detection to prevent spoofing attacks. Built on Amazon Web Services (AWS), the architecture leverages serverless computing, secure identity management, and AI-based facial analysis to deliver scalable and low-latency authentication. Experimental evaluation demonstrates that TrustFace effectively detects spoofing attempts while maintaining near real-time performance, making it suitable for modern secure digital systems.

Index Terms - Face Liveness Detection, Biometric Authentication, AWS Rekognition, Multi-Factor Authentication, Anti-Spoofing, Cloud Security.

I. INTRODUCTION

The rapid evolution of digital systems, particularly in financial transactions and online services, has significantly increased the demand for secure authentication mechanisms. Traditional methods such as passwords and PINs are no longer sufficient due to their vulnerability to cyberattacks, including phishing, credential theft, and session hijacking. Biometric authentication, especially facial recognition, has emerged as a promising alternative due to its non-intrusive nature and ease of use. However, conventional facial recognition systems are not entirely secure, as they can be deceived using spoofing techniques such as photographs, recorded videos, or deepfake-generated content.

To address these limitations, authentication systems must not only verify identity but also confirm the physical presence of the user in real time. This requirement introduces the concept of face liveness detection, which ensures that the captured input originates from a live human rather than a spoofing artifact. This paper proposes TrustFace, a secure authentication framework that combines credential-based authentication, facial recognition, and AI-driven liveness detection. Additionally, the system extends authentication beyond login by enforcing verification during sensitive operations, ensuring continuous security.

The novelty of this research is the integration of real-time AI-based liveness detection within a serverless cloud architecture, enabling secure, low-latency authentication while effectively mitigating spoofing and replay attacks that conventional facial recognition systems fail to address.

II. RELATED WORK

Authentication systems have evolved significantly over the years, transitioning from traditional password-based mechanisms to more advanced biometric approaches. Early authentication methods relied heavily on knowledge-based techniques such as passwords and PINs, which, although simple to implement, were highly vulnerable to phishing, credential theft, and brute-force attacks. With the increasing adoption of digital payment systems, the need for more secure and user-friendly authentication mechanisms became evident. Facial recognition technology emerged as a promising biometric solution due to its non-intrusive nature and ease of use. Recent studies have explored its application in digital payment systems, highlighting its ability to enhance user experience and engagement. For instance, Gao et al. [1] demonstrated that facial recognition-based payment systems improve user adoption due to their perceived convenience and innovation. However, the study also identified major concerns related to security risks, particularly the susceptibility of such systems to spoofing attacks and privacy issues.

To further strengthen authentication mechanisms, multi-biometric systems have been introduced. Anwar et al. [2] proposed a multi-biometric authentication framework that combines multiple biometric traits using fuzzy logic to improve accuracy and reduce false acceptance rates. While such systems enhance reliability, they often introduce increased computational complexity and may still lack real-time verification of user presence. In the context of fraud detection, facial recognition has been applied to banking systems to prevent unauthorized access. P.K. et al. [3] developed a face recognition-based fraud detection system capable of operating under masked and unmasked conditions, improving robustness in real-world scenarios. However, these systems primarily focus on identity verification and do not adequately address the problem of spoofing using static or replayed media.

Beyond financial applications, facial recognition has also been integrated with IoT systems for security purposes. Pathak et al. [4] proposed an intelligent vehicle surveillance system that combines IoT with facial recognition for real-time monitoring and theft prevention. While effective in access control scenarios, such systems do not incorporate advanced liveness detection mechanisms to verify real-time human presence. Additionally, the widespread adoption of facial recognition technology has raised significant ethical and regulatory concerns. Robles et al. [5] discussed the global challenges associated with the governance of facial recognition systems, including issues related to privacy, bias, and misuse of biometric data. These concerns highlight the need for secure and responsible implementation of such technologies.

Despite these advancements, existing systems primarily focus on identity verification and lack robust mechanisms to confirm whether the user is physically present during authentication. Most traditional facial recognition systems can be deceived using photographs, videos, or deepfake content, making them vulnerable to spoofing and replay attacks. The TrustFace system aims to address these limitations by integrating real-time liveness detection with facial recognition and credential-based authentication within a cloud-native architecture. By combining AI-driven facial analysis with session-based verification and secure cloud services, the proposed system ensures both identity validation and real-time human presence verification, resulting in a more secure and reliable authentication framework.

III. SYSTEM ARCHITECTURE

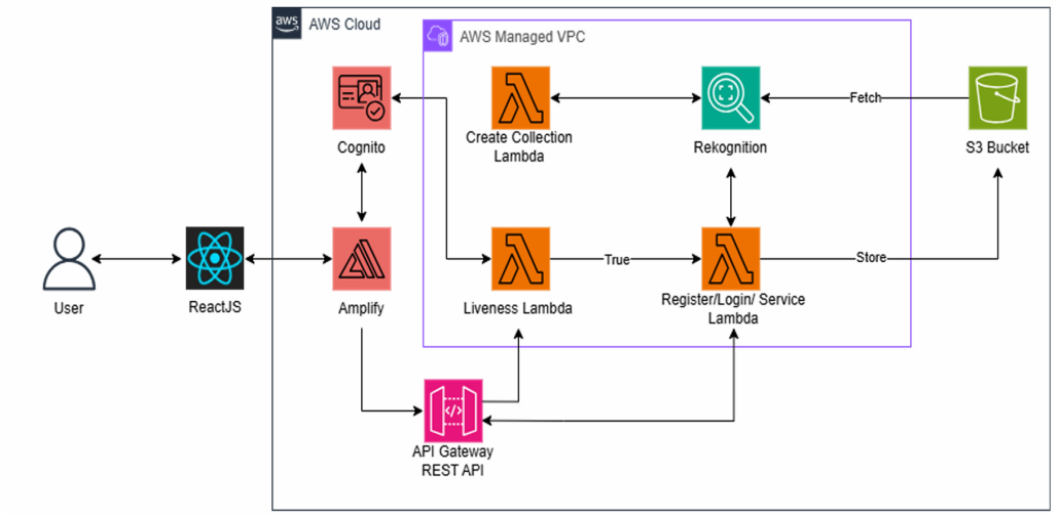

Fig. 1. Aws Cloud Architecture of the Proposed TrustFace System

3.1 Overview

The TrustFace system is designed using a cloud-native, serverless architecture that enables secure, scalable, and real-time authentication. The architecture follows a multi-layered microservice model, consisting of a frontend layer for user interaction, an API layer for request handling, a processing layer for authentication logic, and an AI layer for biometric analysis.

Unlike traditional monolithic authentication systems, TrustFace decomposes functionality into independent components that operate collaboratively. This modular design improves scalability, fault isolation, and system maintainability while ensuring low-latency processing.

The system is built on Amazon Web Services (AWS), leveraging services such as AWS Amplify, Amazon Cognito, API Gateway, AWS Lambda, and Amazon Rekognition. Each component performs a dedicated role within the authentication workflow, enabling seamless integration between user interaction, backend processing, and AI-based verification.

3.2 Application Functionalities

The system comprises four primary functionalities:

The Authentication module validates user credentials using a secure identity management system. It ensures that only registered users can initiate the authentication process, acting as the first layer of security.

The Liveness Detection module is the core component of the system, responsible for verifying real-time human presence. It uses AI-based facial analysis to detect motion, depth, and interaction patterns, preventing spoofing attempts such as photos or videos.

After liveness verification, the face recognition module performs identity validation by comparing captured facial data with stored reference images. A confidence score is generated to determine the similarity between the input and stored data.

The Verification and Decision module evaluates the outputs of all previous stages and applies decision logic. Authentication is successful only if all conditions - valid credentials, confirmed liveness, and high-confidence face match - are satisfied.

3.3 Authentication Flow and System Interaction

The TrustFace system follows a secure and streamlined authentication flow that enables real-time interaction between the frontend, backend services, and AI-based verification components. When a user initiates authentication, the request is processed through the frontend and securely transmitted via an API layer to serverless backend functions.

After credential validation, a unique liveness session is created, allowing the system to capture and analyze real-time facial data using AI-based models. The system evaluates facial motion, depth, and interaction patterns to verify human presence and prevent spoofing attempts. Once analysis is complete, the backend applies decision logic based on confidence thresholds and returns the authentication result to the frontend.

Throughout this process, secure communication protocols, temporary credentials, and role-based access control mechanisms ensure data protection and system integrity, enabling a reliable and scalable authentication workflow.

IV. IMPLEMENTATION

4.1 Backend Services

The backend is implemented using AWS serverless services:

- AWS Lambda: Executes core logic (session creation, verification)
- API Gateway: Exposes REST APIs
- Amazon Rekognition: Performs AI-based liveness detection
- IAM: Controls access permissions

Every single Lambda function can be individually deployed, versioned, and secured using AWS IAM role permissions. Isolated execution environments are used for higher safety and protection from data leaks between agents. Few of the lambda functions:

- createLivenessSession.py : Initializes liveness session
- verifyLiveness.py : Retrieves and evaluates results
- login.py : used for authentication and authorization
- verify.py : Retrieves the image and checks whether the user is the one who is logged in or not

4.2 Frontend Application

The front end is built using React 18+ with TypeScript, while Vite has been used for bundling of the assets for efficient production build purposes. Tailwind CSS has been used for styling using a utility-first approach. Authentication has been handled through AWS Amplify along with Amazon Cognito for session handling based on OAuth 2.0. The FaceLivenessDetector component is used to capture and process facial data in real time.

4.3 Technology Stack

The complete technology stack is summarized in Table 1.

Table 1. Technology Stack Components

Layer	Technology	Purpose
Frontend	React 18 + TypeScript + Vite	UI rendering and state management
Styling	Tailwind CSS	Utility-first responsive design
Auth	AWS Amplify + Cognito	Identity and access management
Backend	AWS Lambda (Python)	Event-driven agent functions
API	Amazon API Gateway	Used for communication
Image	AWS Rekognition	Liveness detection
Storage	Amazon S3	Low cost and easy retrieval
Monitoring	AWS CloudWatch	Used for logging

V EVALUATION AND RESULTS

5.1 Performance Metrics

The system was evaluated under real-time authentication scenarios using simulated user interactions and cloud-based testing tools. Metrics measured included authentication response time, liveness detection accuracy, spoof detection capability, and Lambda execution latency.

The authentication process achieved an average end-to-end response time of approximately 3-4 seconds, covering credential validation, liveness detection, and face verification stages. Liveness detection accuracy was observed to be consistently high under normal conditions, with the system successfully distinguishing between live users and spoof attempts such as static images and pre-recorded videos. Spoof detection tests demonstrated reliable rejection of unauthorized inputs, ensuring robust protection against replay attacks.

The system maintained stable performance during concurrent authentication requests, with no significant degradation in response time under moderate load conditions. The initial Lambda invocation showed an average latency of around 400 milliseconds due to cold start, while subsequent executions reduced latency to below 100 milliseconds. These results indicate that the proposed architecture delivers reliable, secure, and near real-time authentication suitable for practical deployment.

5.2 Security Assessment

The system was evaluated for its robustness against common security threats, including spoofing attacks, replay attacks, and unauthorized access attempts. The implementation incorporates multiple security layers such as session-based validation, temporary credential management, and encrypted communication protocols to ensure secure operation.

Spoofing resistance was tested using static images and pre-recorded videos, where the system consistently rejected non-live inputs due to effective liveness detection mechanisms. Replay attack

prevention was achieved through the use of unique, time-bound session identifiers, ensuring that previously captured data could not be reused for authentication. Additionally, all communication between system components is secured using HTTPS, preventing data interception and tampering.

Access control is enforced through role-based permissions, ensuring that only authorized components can interact with sensitive services. Temporary credentials further enhance security by limiting access duration and reducing the risk of credential leakage. Overall, the system demonstrated strong resilience against common attack vectors, making it suitable for secure real-world authentication scenarios.

Furthermore, the system was assessed for its ability to maintain security during continuous operation and under abnormal usage conditions. Authentication requests containing invalid or expired credentials were correctly rejected, while active sessions were validated before granting access to protected resources. Security events, including authentication attempts and access requests, were logged to facilitate monitoring, auditing, and incident investigation. The combination of secure communication, strict access control, session validation, and continuous monitoring ensures the confidentiality, integrity, and availability of the system, providing a reliable and secure authentication framework for real-world deployment.

5.3 User Interface and Authentication Outcomes

The TrustFace system incorporates an intuitive and user-centric interface that clearly represents both the progress and outcome of the authentication process. As shown in Fig. 2, the registration and verification interface guides the user through structured steps such as session creation, face challenge, and authentication, while also providing real-time liveness tips to ensure optimal capture conditions. Upon successful completion, the system displays a confirmation screen indicating that the user's identity has been verified, along with a smooth redirection process, enhancing user confidence and experience.

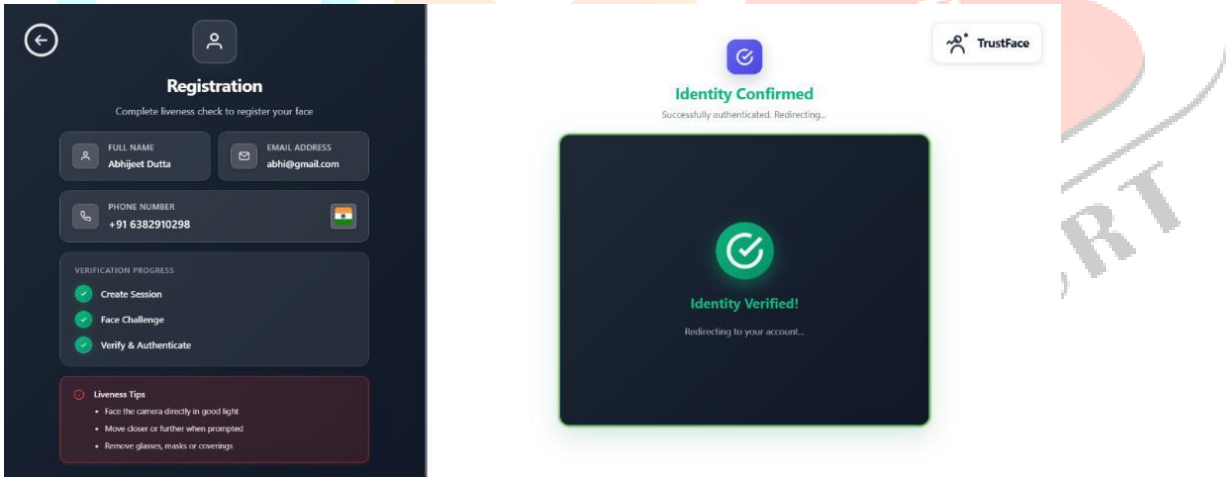

Fig. 2. TrustFace UI - Successful Liveness Verification Result

In contrast, Fig. 3 illustrates the system's response in failure scenarios, where authentication is denied due to insufficient liveness confidence or unfavorable environmental conditions. The interface provides detailed feedback, including confidence scores and corrective suggestions such as improving lighting or adjusting positioning, along with an option to retry the process. This clear distinction between success and failure states, combined with actionable guidance, improves usability while ensuring robustness. Overall, the interface design plays a crucial role in maintaining transparency, reducing user errors, and supporting reliable real-time authentication.

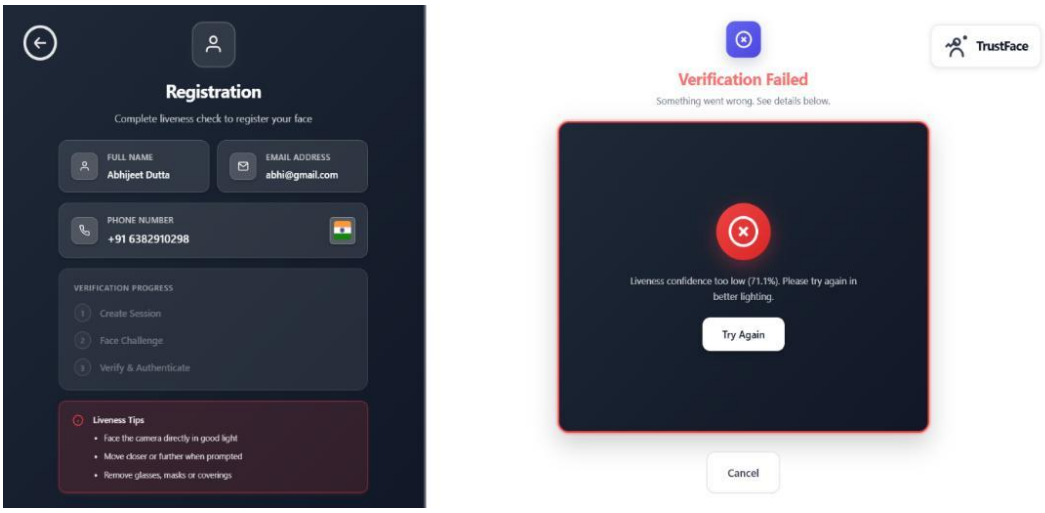

Fig. 3. TrustFace UI - Spoof Detection Result

VI. CONCLUSION

This paper presented TrustFace, a cloud-native authentication system that enables secure and intelligent user verification through real-time face liveness detection. By integrating credential-based authentication, facial recognition, and AI-driven liveness analysis within a serverless architecture, the system delivers a scalable, secure, and low-latency solution capable of mitigating spoofing and replay attacks.

As demonstrated through experimental evaluation, the proposed architecture ensures reliable authentication performance with near real-time response, high liveness detection accuracy, and stable operation under concurrent usage scenarios. Additionally, the modular serverless design allows independent scaling and updates of system components without impacting overall functionality, making it suitable for deployment in modern digital applications.

Future work will focus on enhancing the system with advanced deepfake detection techniques, integrating multi-modal biometric authentication such as voice or behavioral analysis, and improving adaptability under diverse environmental conditions. Furthermore, extending the system toward continuous authentication and fraud analytics can further strengthen security in real-world applications.

VII. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the management of Sri Venkateswara College of Engineering, Chennai, for providing the facilities and support necessary to carry out this research. The authors also thank Ms. J. Buvana for her valuable guidance, continuous encouragement, and constructive suggestions throughout the development of this work. Finally, the authors acknowledge the support of the Department of Artificial Intelligence and Data Science, faculty members, and peers whose assistance and feedback contributed to the successful completion of this research.

VIII. REFERENCES

[1] Gao, W., Jiang, N. & Guo, Q. Facial recognition payment is cool: coolness, inspiration, and customer continuance intention to use facial recognition payment. Financ Innov 11, 31, Springer (2025).

[2] Anwar, N.M., Ahmad, S.S.S., Kausar, N. et al., Multiple biometric authentication for online banking system based on multiple fuzzy approach, Scientific Reports, 15, 32824, Elsevier, 2025.

[3] P.K, R., Khaparde, A., Bendre, V. et al. Fraud detection and prevention by face recognition with and without mask for banking application. Multimed Tools Appl 84, 781-804, Springer (2025).

[4] Pathak, M., Mishra, K.N. & Singh, S.P. An intelligent integrated vehicle surveillance system for controlling the vehicle thefts/hacking using IoT and facial recognition. Int J Syst Assur Eng Manag 16, 468-493, Springer (2025).

[5] Robles, P., Mallinson, D.J., Best, E. et al. Global perspectives on regulating facial recognition technology utilization for criminal justice arrests. Glob. Public Policy Gov. 5, 186-204, Springer (2025).