TouchAuth: A Biometric FIDO2 Key

Nandana Ajilal
Department of Computer Science and Engineering
Rajadhani Institute of Engineering and Technology
Trivandrum, Kerala, India

Aswini Sreekumar
Department of Computer Science and Engineering
Rajadhani Institute of Engineering and Technology
Trivandrum, Kerala, India

Sandhya K. R
Assistant Professor, Department of Computer Science and Engineering
Rajadhani Institute of Engineering and Technology
Trivandrum, Kerala, India

Abstract - TouchAuth: A Biometric FIDO2 Key is a hardware-based authentication system that integrates fingerprint verification with FIDO2 security. The system uses an ESP8266 microcontroller and a fingerprint sensor to authenticate users before enabling access to a USB security module implemented using an RP2040 Pico. Upon successful biometric verification, the ESP8266 generates a virtual user presence signal via GPIO to the Pico, which then performs secure cryptographic authentication with the host system in compliance with FIDO2 standards. The architecture maintains a clear separation between biometric processing and cryptographic operations, enhancing overall system security. Fingerprint data remains confined to the biometric module, while private keys are securely stored and managed within the FIDO2 device, reducing the risk of data exposure and improving resistance against phishing and credential-based attacks. TouchAuth presents a cost effective, scalable, and secure multi factor authentication solution, demonstrating the practical implementation of biometric enhanced hardware tokens for modern authentication systems.

Keywords - Biometric Authentication, FIDO2, Hardware Security Token, ESP8266, RP2040 Pico, Multi Factor Authentication, Cryptographic Authentication, WebAuthn.

I. INTRODUCTION

TouchAuth is a biometric-enabled hardware authentication system designed to enhance secure user verification using fingerprint recognition. It combines biometric authentication with hardware-based user presence verification to strengthen access control mechanisms. Hardware security keys have been widely recognized as effective second-factor authentication devices that improve protection against phishing and credential theft [1], [3]. By integrating biometric verification with hardware tokens, TouchAuth further strengthens authentication by ensuring that only authorized users can activate the device.

The system implements custom-built FIDO2 firmware over a USB Human Interface Device (HID) interface, enabling secure and seamless communication with host systems without requiring additional drivers or external applications [2].This ensures platform independence and ease of deployment across multiple operating systems and browsers. The device integrates a match-on-sensor fingerprint module, allowing biometric processing and verification to occur locally, thereby improving privacy and reducing the risk of sensitive data exposure. This local processing eliminates the need to transmit biometric data over networks, enhancing overall system security.

Upon successful fingerprint authentication, the system enables cryptographic operations through a dedicated hardware module, aligning with modern authentication infrastructures [3]. TouchAuth supports in-browser authentication using FIDO2/WebAuthn protocols, ensuring compatibility with contemporary web services and demonstrating the practical usability of security keys in real-world environments [4].

Additionally, the ESP8266 microcontroller provides Wi-Fi connectivity for fingerprint enrollment and device management. The use of a USB HID interface minimizes network-related vulnerabilities, while the open-source firmware design enhances transparency and flexibility. Similar USB-based authentication tokens have demonstrated improved security and usability in prior research [5].

II. LITERATURE REVIEW

A. *Security Keys: Practical Cryptographic Second Factors for the Modern Web*

Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas [1] proposed hardware-based security keys as practical cryptographic second factors for modern web authentication. Their work introduced the FIDO U2F protocol, which replaces traditional password-based and one-time password systems with public-key cryptography. Each service generates a unique key pair, ensuring that private keys remain securely stored within the hardware device. The concept of origin binding prevents phishing by restricting authentication responses to legitimate websites. Their study demonstrates improved security, scalability, and usability compared to conventional authentication methods.

B. *U2F HID Implementation: Microprocessor to U2F Key*

Torque (Tareq) El Dandachi, Ashika Verma, and Muhammad Abdullah [2] developed a microprocessor-based U2F hardware token that communicates with host systems through the USB HID protocol, enabling driverless operation and wide compatibility. Their implementation focuses on secure key generation and authentication within embedded systems, ensuring efficient performance even on low-power devices. The design maintains essential security features such as secure key storage and user presence verification, while also leveraging public-key cryptography to resist phishing, replay, and man-in-the-middle attacks. The work highlights a low-cost and efficient design while maintaining essential security features like secure key storage and user presence verification, making it suitable for practical deployment.

C. Building an Authentication Infrastructure: Designing a Two Factor Authentication Hardware Token

Zitao Zhang, Jacob Abbott, Sanchari Das, and L. Jean Camp [3] presented the design and development of a two-factor authentication hardware token as part of a larger authentication infrastructure. Their research emphasizes system architecture, secure integration, and usability aspects of hardware tokens. The study also explores user interaction challenges and the importance of designing authentication systems that are both secure and user-friendly, ensuring better adoption in real-world applications.

D. Security Keys: An Empirical Study of FIDO2 Security Keys in Practice.

A study conducted by the University of Gothenburg [4] investigated the real-world usage of FIDO2 security keys, focusing on their effectiveness, usability, and deployment challenges. The research highlights that hardware security keys provide strong resistance against phishing and credential theft, while also identifying practical issues such as user awareness, device management, and adoption barriers that can affect widespread implementation.

E. Modified USB Security Token for User Authentication.

Wala'a M. AlOmari and Hesham Abusaimeh [5] proposed a modified USB security token aimed at improving user authentication mechanisms. Their work focuses on enhancing token architecture, strengthening security controls, and minimizing vulnerabilities associated with traditional authentication techniques. The study demonstrates how improved token design can provide more secure, reliable, and efficient authentication, contributing to the advancement of hardware-based security solutions.

III.SYSTEM DESIGN AND ARCHITECTURE

A. Design Overview

The system is designed as a hardware-based biometric security key that integrates fingerprint verification with FIDO2/WebAuthn authentication to provide secure, passwordless access to computers and web services. It enhances traditional hardware tokens by incorporating biometric validation, ensuring that only authorized users can initiate authentication.

The system combines a fingerprint-controlled user-presence mechanism with a dedicated USB FIDO2 authenticator to emulate a modern hardware security key. A microcontroller interfaces with the fingerprint sensor to capture and verify the user's biometric data. Upon successful verification, a secure signal is sent to the FIDO2 authenticator, which then performs cryptographic operations such as challenge-response authentication using stored private keys.

This design strengthens security by eliminating reliance on passwords, reducing vulnerability to phishing and credential theft. Additionally, it ensures that sensitive cryptographic keys remain securely stored within the hardware, making the system resistant to software-based attacks and unauthorized access.

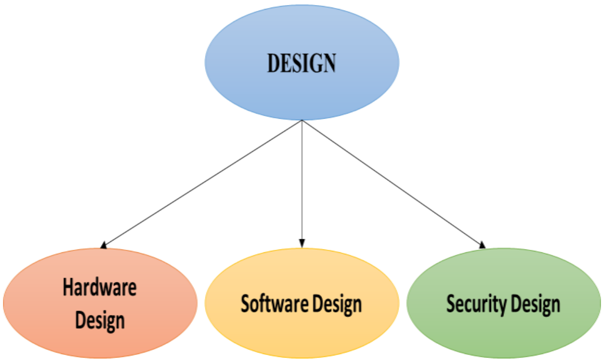

Fig 1: Block Diagram of TouchAuth System Design

B. Hardware Architecture

The proposed system adopts a biometric-gated authenticator model, wherein fingerprint verification serves as the user-presence mechanism required for FIDO2 authentication. This design ensures that cryptographic operations are executed only after successful biometric validation, thereby enhancing system security.

The hardware architecture consists of the following components:

1. **RP2040 Pico (Pico-FIDO):** The RP2040 Pico functions as the primary USB security key, implementing FIDO2/U2F protocols. It communicates with the host system via the USB Human Interface Device (HID) protocol and performs cryptographic operations, including secure challenge-response authentication using internally stored private keys.
2. **ESP8266 (Biometric Controller):** The ESP8266 acts as the biometric control unit, responsible for processing fingerprint verification results and generating the user-presence signal. It also supports auxiliary functionalities such as LED-based status indication.
3. **R307 Fingerprint Sensor:** The R307 sensor is utilized for biometric data acquisition and matching. It supports fingerprint enrollment and verification, enabling reliable user authentication.
4. **USB Host (PC/Browser**): The host system operates as the FIDO2 client, interfacing with the RP2040 Pico through WebAuthn-compatible browsers. It

initiates authentication requests and validates responses via the relying party.

5. **Mode Selection Switch**: A hardware switch is incorporated to toggle between operational modes, such as registration and authentication, thereby improving system usability.

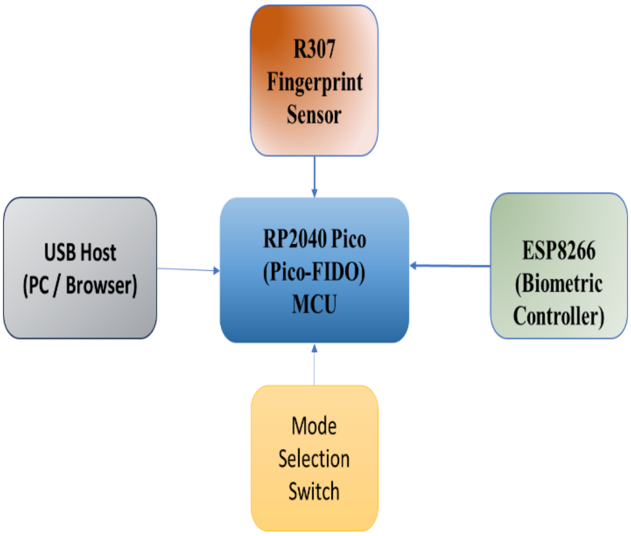

Fig 2: Hardware Architecture of TouchAuth Biometric FIDO2 Key

C. Hardware Interconnections (Design Level)

The hardware interconnections of the system are designed to ensure efficient communication between components. The R307 fingerprint sensor is connected to the ESP8266 microcontroller via a UART interface, enabling reliable transmission of biometric data for fingerprint verification. The ESP8266, acting as the biometric controller, communicates with the RP2040 Pico through a GPIO interface to transmit a virtual user-presence signal upon successful authentication. Finally, the RP2040 Pico is connected to the host system (PC or browser) via a USB interface, where it operates as a FIDO2 authenticator to perform secure cryptographic authentication. This structured interconnection enables seamless integration of biometric validation with hardware-based security mechanisms.

Table I Hardware Interconnection Details of the Proposed System

Component	**Interface**	**Purpose**
Fingerprint Sensor → ESP8266	UART	Biometric verification
ESP8266 → Pico	GPIO	Virtual user-presence signal
Pico → PC	USB	FIDO2 authentication

D. Software Architecture

The software architecture of the proposed system follows a layered and modular design to ensure scalability, maintainability, and secure operation. Each layer performs a specific role in the authentication process.

1. **Input Layer:** This layer is responsible for fingerprint capture and sensor communication. It acquires biometric data from the R307 fingerprint sensor and forwards it for processing.
2. **Control Layer (ESP8266):** The control layer performs biometric decision-making by verifying the fingerprint data. It manages authentication sequencing, generates the user-presence signal, and handles errors during the process.
3. **Authenticator Layer (Pico-FIDO):** This layer operates on the RP2040 Pico and implements the USB stack (TinyUSB) along with CTAP2/U2F protocols. It performs secure challenge–response operations using stored cryptographic keys.
4. **Client Layer:** The client layer consists of the browser and operating system, which support WebAuthn APIs. It communicates with the hardware authenticator, sends authentication challenges, and verifies responses with the server.

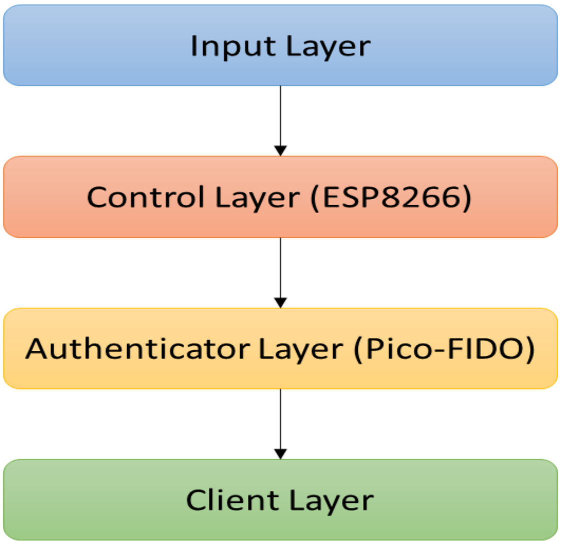

Fig. 3: Software Architecture of TouchAuth Biometric FIDO2 System

E. Security Design

The security design of the proposed system is based on a multi-factor hardware authentication model combined with secure key management principles to ensure strong, phishing-resistant authentication.

1) Authentication Model

The system enforces multi-factor authentication through the following factors:

a) Something You Have (Hardware Device): The RP2040 Pico functions as a physical security key required for authentication.

b) Something You Are (Fingerprint): Biometric verification is performed using the fingerprint sensor to ensure that only authorized users can initiate authentication.

c) Cryptographic Proof (FIDO2 Private Keys): Authentication is completed using a challenge–response mechanism based on securely stored private keys.

2) Key Management Design

The system implements secure key management in accordance with FIDO2 standards:

a) Key Pair Generation: Public-private key pairs are generated during the registration phase.

b) Private Keys: Private keys are securely stored within the authenticator memory and are never transmitted خارج the device, preventing unauthorized access or extraction.

c) Public Keys: Public keys are registered with the relying party (server/browser) during enrollment and are used to verify authentication responses.

IV. SYSTEM IMPLEMENTATION

The system implementation is divided into two main firmware components: the Pico-FIDO authenticator and the ESP8266 biometric controller. The overall operational flow is illustrated in Fig. 4, where the system initializes, waits for fingerprint input, verifies the user, and then performs FIDO2 authentication. The detailed operational logic of each module is illustrated in Fig. 5 and Fig. 6.

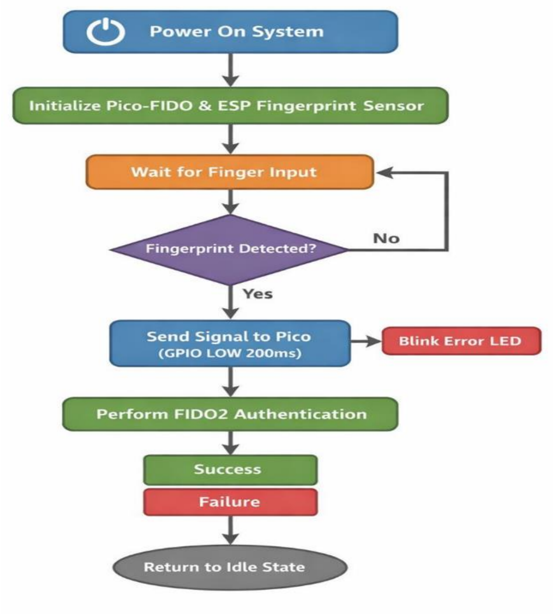

Fig. 4: System Implementation Flow of TouchAuth Biometric FIDO2 Key

1) ESP8266 Firmware Logic

The ESP8266 is responsible for biometric authentication and user-presence signaling, as shown in Fig. 5. It initializes the UART, GPIO, and fingerprint sensor, and enters an authentication-ready state. The system continuously monitors for fingerprint input. Upon detecting a fingerprint, the sensor performs template matching. If the fingerprint is valid, the ESP8266 generates a GPIO pulse (100–200 ms) to signal user presence to the Pico. It also provides user feedback through LEDs, indicating success or failure. After completion, the system returns to the idle state.

Key Principle: The ESP8266 performs only biometric authorization and does not participate in cryptographic operations, ensuring a clear separation of responsibilities.

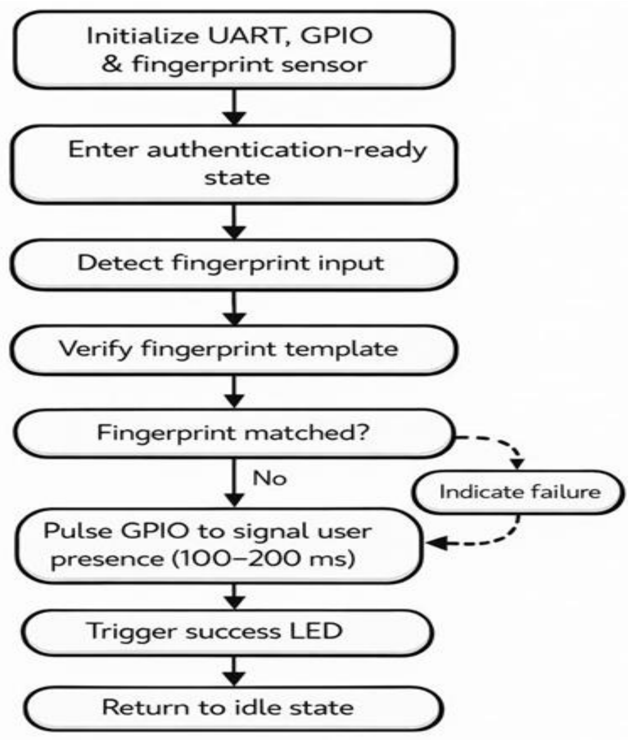

Fig. 5: ESP8266 Firmware Logic for Biometric Authentication and User-Presence Signaling

2) Pico-FIDO Firmware Logic

The RP2040 Pico operates as the FIDO2 authenticator, as illustrated in Fig. 6. It initializes the TinyUSB device stack and implements CTAP2/U2F protocols. The Pico continuously monitors the GPIO pin for the user-presence signal generated by the ESP8266. Upon receiving this signal, it processes authentication requests from the host.

The Pico receives an authentication challenge from the browser or relying party, signs it using a securely stored private key, and generates a cryptographic response. This signed response is then sent back to the host for verification.

Key Principle: The Pico never processes fingerprint data. Biometric operations are fully isolated from cryptographic functions, enhancing overall system security.

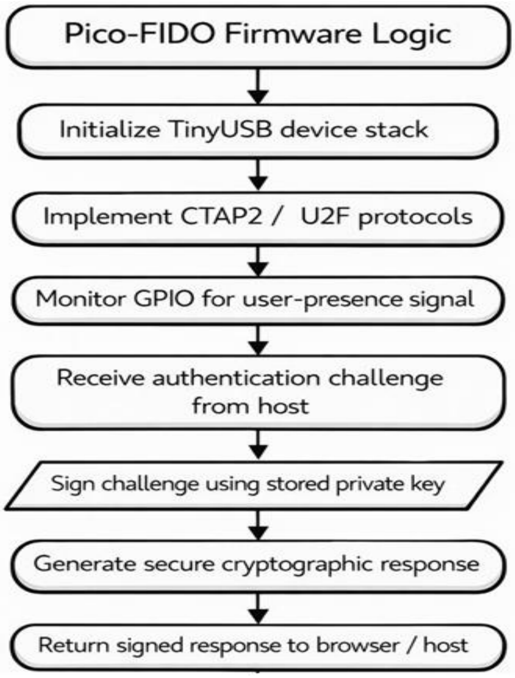
Pico-FIDO Firmware Logic
Initialize TinyUSB device stack
Implement CTAP2 / U2F protocols
Monitor GPIO for user-presence signal
Receive authentication challenge from host
Sign challenge using stored private key
Generate secure cryptographic response
Return signed response to browser / host

Fig. 6: Pico-FIDO Firmware Logic for FIDO2-Based Cryptographic Authentication

V.RESULTS AND ANALYSIS

F. Functional Results

The proposed TouchAuth system was successfully implemented and tested for biometric-gated FIDO2 authentication. The system correctly performs fingerprint-based user verification using the R307 sensor and triggers the RP2040 Pico to execute FIDO2 authentication. The device is recognized as a USB security key by WebAuthn-supported browsers, enabling seamless registration and login. The integration between ESP8266 and Pico ensures reliable user-presence signaling, resulting in successful authentication.

The developed hardware prototype of the system is shown in Fig. 7, demonstrating the integration of the fingerprint sensor, ESP8266, and Pico-FIDO module with a host device.

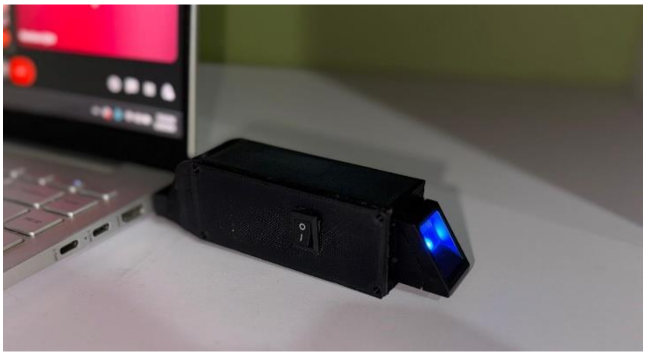

Fig. 7: Prototype Implementation of TouchAuth Biometric FIDO2 Key

B. Performance Analysis

The system demonstrates efficient performance with minimal delay. The average time required for fingerprint detection and verification is approximately 1–2 seconds. The FIDO2 challenge–response process is executed within milliseconds, resulting in low overall system latency and smooth authentication experience.

C. Accuracy Analysis

The fingerprint sensor provides reliable authentication under normal conditions. The system exhibits a low False Acceptance Rate (FAR), ensuring unauthorized users are denied access. A moderate False Rejection Rate (FRR) was observed, mainly due to improper finger placement or incomplete fingerprint capture.

D. Security Analysis

The system ensures strong security by combining biometric authentication with hardware-based cryptographic operations. Private keys are securely stored within the RP2040 Pico and are never exposed externally. The use of FIDO2 challenge–response mechanisms protects against phishing, replay, and credential theft attacks. Additionally, the separation of biometric processing and cryptographic functions enhances overall system security.

E. Observations

The system operates reliably with stable communication between components. USB HID implementation enables driverless compatibility across platforms. The authentication process is user-friendly and eliminates the need for passwords. Minor delays were observed during fingerprint registration due to sensor limitations.

F. Limitations

The system exhibits slight delays during fingerprint registration, primarily due to the limitations of the R307 fingerprint sensor. This can affect user experience during enrollment. The issue can be mitigated by using a higher-performance fingerprint module with faster processing capabilities. Additionally, the system lacks advanced liveness detection and has limited fingerprint storage capacity.

G. Summary

The proposed system successfully demonstrates a secure and efficient biometric FIDO2 authentication mechanism. It provides a practical solution for passwordless authentication while ensuring strong protection against common security threats.

H. Comparative Analysis

The comparative performance of different authentication methods is illustrated in Fig. 8. The proposed TouchAuth system demonstrates superior performance in terms of security, usability, and phishing resistance compared to traditional password and OTP-based systems.

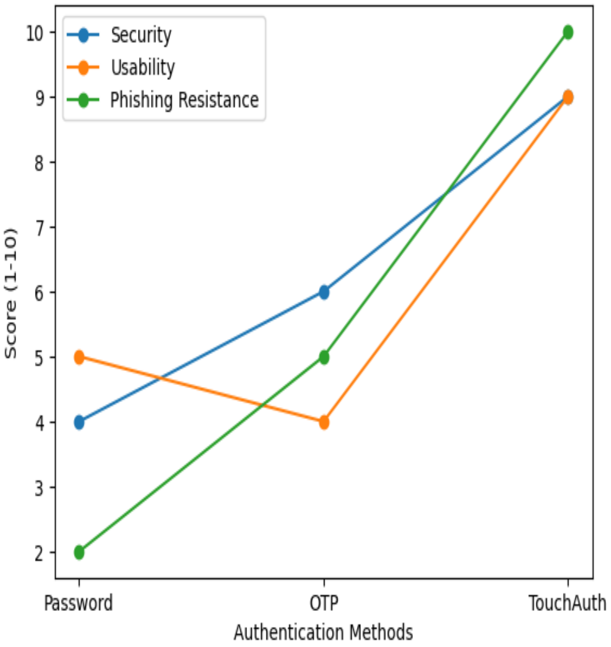

Fig. 8: Comparative Analysis of Authentication Methods

A comparison of the proposed TouchAuth system with traditional authentication methods is presented in Table II. The comparison is based on key parameters such as security strength, usability, and resistance to phishing attacks. The proposed system demonstrates significant improvements over conventional password- and OTP-based approaches by combining biometric verification with hardware-backed cryptographic authentication. This integration enhances protection against common attack vectors, including credential theft and replay attacks.

Table II: Comparison of Authentication Methods

Feature	Password	OTP	TouchAuth (Proposed)
Security Level	Low	Medium	High
Usability	Medium	Low	High
Phishing Resistance	Low	Medium	Very High
Hardware Dependency	No	No	Yes
Biometric Protection	No	No	Yes

VI. FUTURE ENHANCEMENTS

The proposed system can be further enhanced by incorporating additional security and usability features. One potential improvement is the integration of liveness detection mechanisms in the fingerprint sensor to prevent spoofing attacks using fake fingerprints. The use of a higher-performance biometric module can reduce delays during fingerprint registration and improve overall accuracy. The system can also be extended to support multiple user profiles, enabling shared device usage in organizational environments.

Furthermore, the addition of wireless connectivity, such as Bluetooth or Wi-Fi, can allow remote management and configuration of the device. Implementing a secure element for hardware-backed key storage can further strengthen protection against physical attacks. An onboard display or advanced LED indicators can be included to provide better user feedback during authentication. These enhancements would improve the system’s security, scalability, and user experience, making it more suitable for real-world deployment.

VII. CONCLUSION

The proposed system presents a biometric-gated hardware authentication solution that integrates fingerprint verification with a USB-based FIDO2 security key. By combining biometric authentication with hardware-backed cryptographic operations, the system ensures strong user identity assurance and enhances overall security. The separation of biometric processing and cryptographic functions improves system robustness and prevents exposure of sensitive data. The design follows a layered and modular architecture, enabling efficient operation and maintainability. Additionally, the system offers high usability and convenience by eliminating the need for traditional passwords. The proposed approach is well-suited for modern authentication requirements and provides a scalable foundation for future security enhancements.

REFERENCES

[1] J. Lang, A. Czeskis, D. Balfanz, M. Schilder, and S. Srinivas, “Security Keys: Practical Cryptographic Second Factors for the Modern Web,” in Proc. IEEE Symp. Security and Privacy, 2016.

[2] T. El Dandachi, A. Verma, and M. Abdullah, “U2F HID Implementation: Microprocessor to U2F Key.”

[3] Z. Zhang, J. Abbott, S. Das, and L. J. Camp, “Building an Authentication Infrastructure: Designing a Two Factor Authentication Hardware Token.”

[4] Security Keys: An Empirical Study of FIDO2 Security Keys in Practice,” University of Gothenburg, Sweden, 2019.

[5] W. M. AlOmari and H. Abusaimeh, “Modified USB Security Token for User Authentication,” 2015.