Design and Implementation of an FPGA-Based Smart Biometric Security System with Multi-Level Authentication and Real-Time Monitoring

Nathani Rajitha[1], Karanki Pallavi[2], Machavarapu Likitha[3], Mr. K. Ramesh Babu[4]
[1,2,3]Department of Electronics and Communication Engineering Vasireddy Venkatadri Institute of Technology (VVIT), Guntur, India
[4]Guide, Assistant Professor, Vasireddy Venkatadri Institute of Technology University

***Abstract*—The increasing demand for secure and intelligent home automation systems has led to the development of advanced authentication-based security solutions. This paper presents the design and implementation of an FPGA-based smart biometric security system integrated with multi-level authentication and real-time monitoring capabilities. The proposed system combines fingerprint recognition, keypad-based access, and one-time password (OTP) verification through email to enhance security reliability.**

The Field Programmable Gate Array (FPGA) acts as the central processing unit, enabling high-speed parallel processing of authentication inputs, thereby reducing system latency and improving response time compared to conventional microcontroller-based systems. A Raspberry Pi module is integrated with a cam- era unit to capture real-time images during access attempts, providing continuous surveillance and record maintenance.

The system is designed to allow access only to authorized users by verifying stored biometric data and dynamically generated OTP codes. Experimental results demonstrate improved authentication accuracy, faster response time, and enhanced security compared to traditional single-level authentication systems. The proposed solution is cost-effective, scalable, and suitable for modern smart home applications. Future enhancements include IoT-based remote monitoring, mobile application integration, and AI-driven facial recognition for intelligent threat detection. The developed system provides a robust foundation for next-generation smart security architectures.

***Index Terms*—FPGA, Biometric Security, Smart Home, Fingerprint Authentication, OTP Verification, Raspberry Pi, Real-Time Monitoring**

I. INTRODUCTION

The rapid growth of smart home technologies has significantly increased the demand for secure, reliable, and intelligent access control systems. Traditional security mechanisms such as mechanical locks, keys, and password-based systems are increasingly becoming inadequate due to their vulnerability to unauthorized access, key duplication, and pass- word leakage [1, 2]. These limitations emphasize the need for advanced security solutions that provide enhanced reliability, automation, and real-time monitoring capabilities.

Recent advancements in embedded systems and hardware acceleration have enabled the integration of biometric authentication and intelligent surveillance into modern security applications. Among these technologies, Field Programmable Gate Arrays (FPGAs) have gained significant attention due to their parallel processing capability, low latency, and high computational efficiency [3, 4]. Unlike conventional microcontroller-based systems, FPGAs can process multiple authentication inputs simultaneously, making them highly suitable for real-time and high-speed security systems.

Biometric authentication, particularly fingerprint recognition, has become a reliable method for identity verification due to its uniqueness and difficulty to replicate [2, 20]. However, single-level authentication systems are still vulnerable to spoofing and unauthorized access. To overcome these challenges, multi-factor authentication mechanisms have been introduced, combining biometric verification with additional security layers such as passwords or one-time passwords (OTP) [23].

In this paper, an FPGA-based smart biometric security system is proposed, integrating fingerprint authentication, keypad-based access control, and real-time monitoring using a Raspberry Pi camera module [7]. The system employs a multi-level authentication mechanism to enhance security, where access is granted only after successful verification of biometric credentials and dynamic OTP validation. This layered approach significantly reduces the risk of unauthorized access and improves overall system reliability.

Furthermore, the integration of Internet of Things (IoT) technologies enables remote monitoring and communication, allowing users to receive alerts and verify access requests in real time [8, 10]. The inclusion of a camera module enhances system transparency by capturing images during access attempts, providing visual evidence for security analysis. The proposed system aims to overcome the limitations of existing security solutions by offering faster response time, improved authentication accuracy, and reduced dependency on manual monitoring. By combining FPGA-based processing with embedded vision and multi-factor authentication, the system provides a scalable and efficient solution for modern smart home security applications.

This work contributes to the development of intelligent and robust security architectures and serves as a foundation for future enhancements such as IoT-based remote monitoring, mobile application integration, and AI-driven facial recognition systems.

II. LITERATURE REVIEW

The development of smart home security systems has gained significant attention in recent years due to increasing safety concerns and the demand for automated access control. Various approaches have been proposed in the literature, focusing on biometric authentication, embedded systems, and IoT-based monitoring.

Early security systems primarily relied on password-based and key-based mechanisms, which are vulnerable to security threats such as key duplication and password leakage [1]. To overcome these limitations, biometric authentication techniques such as fingerprint recognition were introduced, providing higher reliability and uniqueness in user identification [2]. However, these systems often rely on single-level authentication, making them susceptible to spoofing attacks.

Several researchers have proposed microcontroller-based smart security systems integrating fingerprint sensors and keypad interfaces [5, 11]. These systems are cost-effective and easy to implement but suffer from limitations such as sequential processing, increased latency, and inability to handle multiple inputs simultaneously. As a result, system performance and response time are significantly affected under real-time conditions.

To address these challenges, FPGA-based security systems have been explored due to their parallel processing capabilities and high-speed performance. FPGA-based implementations enable simultaneous processing of multiple authentication inputs, reducing latency and improving system efficiency [4, 21]. However, many existing FPGA-based systems focus only on basic authentication mechanisms and lack advanced features such as real-time monitoring and multi-factor authentication.

Recent advancements have introduced IoT-based smart home security systems that enable remote monitoring and control using internet connectivity [10, 17]. These systems allow users to monitor security status through mobile applications and receive alerts in real time. Despite their advantages, IoT-based systems often face challenges related to data security, network dependency, and latency issues.

Some studies have also integrated camera modules for surveillance purposes, enabling image capture and monitoring during access attempts [22]. While these systems enhance security through visual verification, they often lack efficient hardware acceleration and real-time decision-making capabilities.

Multi-factor authentication systems combining biometric verification with additional layers such as passwords or OTPs have been proposed to improve security robustness [23]. These systems provide enhanced protection against unauthorized access but may increase system complexity and processing time when implemented on traditional platforms.

2.1 Comparison of Existing Systems

2.2 Research Gap

From the literature, it is observed that existing systems either focus on biometric authentication, IoT-based monitoring, or hardware acceleration independently. Very few systems integrate all these features into a single unified platform. Moreover, limitations such as high latency, lack of real-time processing, single-level authentication, and insufficient security layers are still prevalent.

To address these challenges, the proposed system integrates FPGA-based parallel processing with biometric authentication, keypad input, OTP-based verification, and real-time monitoring using a camera module. This combination ensures enhanced security, reduced latency, and improved system reliability compared to existing solutions.

Table 1: Comparison of Existing Security Systems

System	Technology	Advantages	Limitations
Traditional Lock	Mechanical	Low cost, simple	Very low security
Microcontroller	Embedded Systems	Easy to implement	High latency
Biometric System	Fingerprint	High accuracy	Single-level security
IoT System	Cloud + Sensors	Remote monitoring	Network dependency
Camera System	Surveillance	Visual evidence	No real-time decision
FPGA System	Hardware Acceleration	High speed	Limited features
Proposed System	FPGA + Biometric	Multi-level security	Design complexity

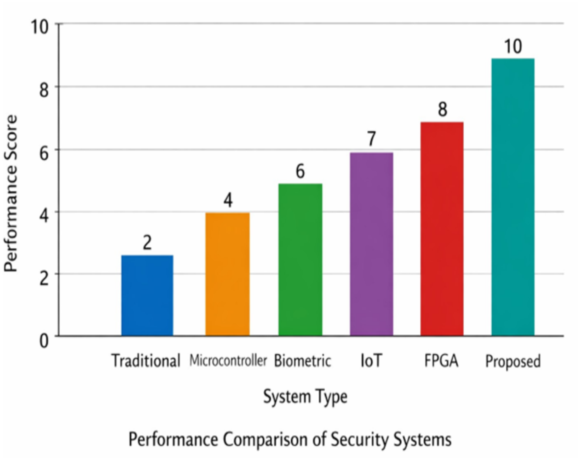


Figure 1: Performance Comparison of Security Systems

III. PROPOSED SYSTEM

The proposed system presents an FPGA-based smart biometric security solution designed to provide multi-level authentication and real-time monitoring for enhanced home security. The system integrates hardware acceleration, biometric verification, and embedded vision to ensure secure and efficient access control.

3.1 System Overview

The overall architecture of the system consists of input modules, processing unit, and output modules. The primary components include a fingerprint sensor, keypad interface, FPGA board, Raspberry Pi with camera module, and an LCD display.

The fingerprint sensor captures the biometric data of the user and compares it with the stored database for authentication. The keypad provides an additional layer of security by allowing users to enter a password or trigger OTP-based verification. The FPGA acts as the central controller, processing all authentication inputs in parallel and making real-time decisions. The Raspberry Pi is integrated with a camera module to capture images during access attempts. These images are stored for monitoring and security analysis. Additionally, an OTP (One-Time Password) is generated and sent to the registered email when required, enabling secure remote authentication.

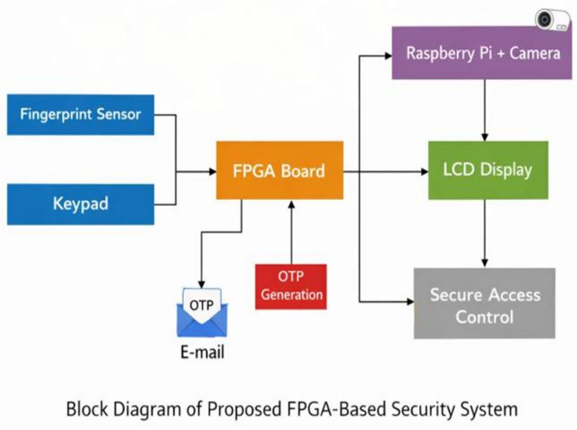


Figure 2: Block Diagram of Proposed FPGA-Based Security System

3.2 Working Principle

The system operates based on a multi-level authentication process:

1. The user initiates access by placing a finger on the fingerprint sensor.
2. The captured fingerprint is verified with stored data.
3. If authentication is successful, the system proceeds to the next level.
4. The user enters a password through the keypad or requests OTP verification.
5. The OTP is generated and sent to the registered email for validation.
6. Upon successful verification, access is granted.
7. Simultaneously, the camera captures an image for record maintenance.
8. If authentication fails at any stage, access is denied and an alert is generated.

3.3 Hardware Components

The proposed system consists of the following hardware modules:

- FPGA Board: Acts as the main processing unit, enabling parallel execution and fast response time.
- Fingerprint Sensor: Provides secure biometric authentication.
- Keypad: Enables password entry and OTP triggering.
- Raspberry Pi: Handles image capture and communication tasks.
- Camera Module: Captures real-time images during access attempts.
- LCD Display: Displays system status and authentication results.

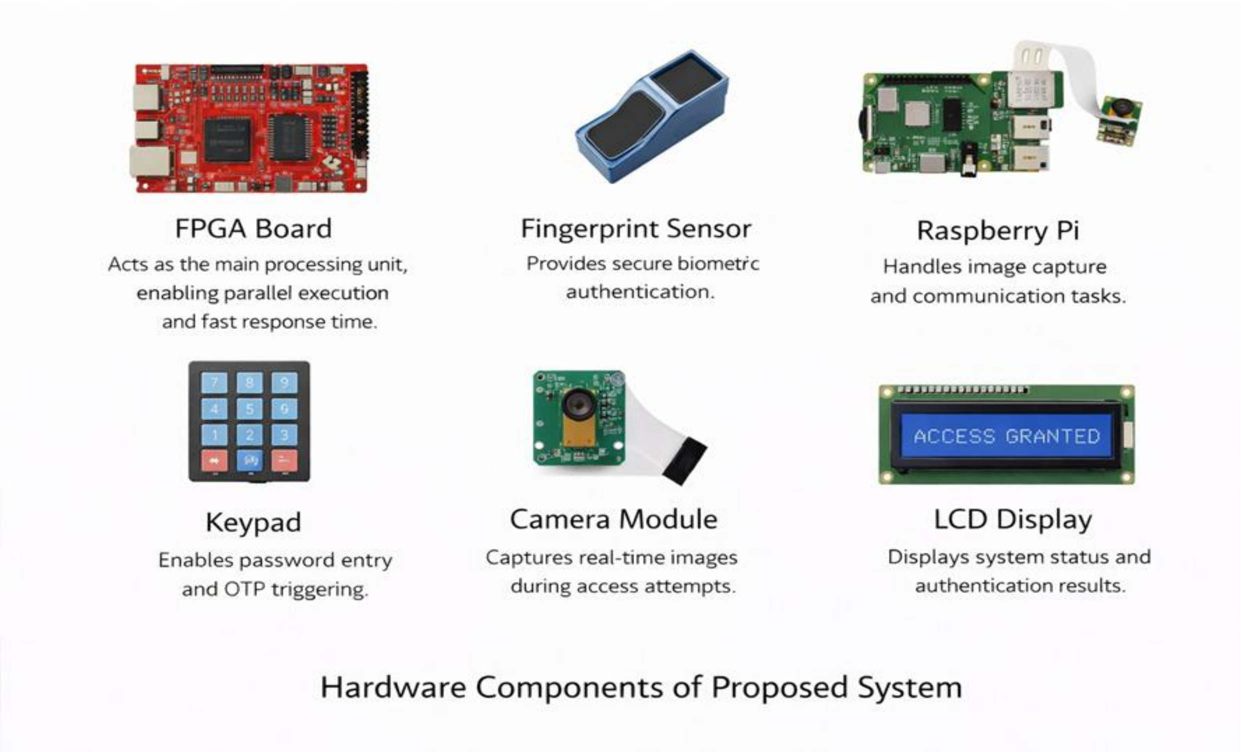

FPGA Board
Acts as the main processing unit, enabling parallel execution and fast response time.
Fingerprint Sensor
Provides secure biometric authentication.
Raspberry Pi
Handles image capture and communication tasks.
Keypad
Enables password entry and OTP triggering.
Camera Module
Captures real-time images during access attempts.
ACCESS GRANTED
LCD Display
Displays system status and authentication results.
Hardware Components of Proposed System

Figure 3: Hardware Components of the Proposed FPGA-Based Smart Biometric Security System

3.4 Advantages of Proposed System

The proposed system offers several advantages over existing solutions:

- Multi-level authentication enhances security.
- FPGA-based parallel processing reduces latency.
- Real-time monitoring using camera improves surveillance.
- OTP-based verification enables secure remote access.
- Scalable architecture supports future enhancements such as IoT integration.

IV. RESULTS AND ANALYSIS

The proposed FPGA-based smart biometric security system was successfully implemented and tested to evaluate its performance, accuracy, and reliability. The system integrates fingerprint authentication, keypad-based input, OTP verification, and real-time monitoring using a camera module. Experimental validation confirms that the system operates efficiently under different access conditions.

4.1 Prototype Implementation

The hardware prototype of the proposed system is shown in Fig. 4. The implementation includes FPGA board, fingerprint sensor, keypad, Raspberry Pi, and camera module integrated into a single system.

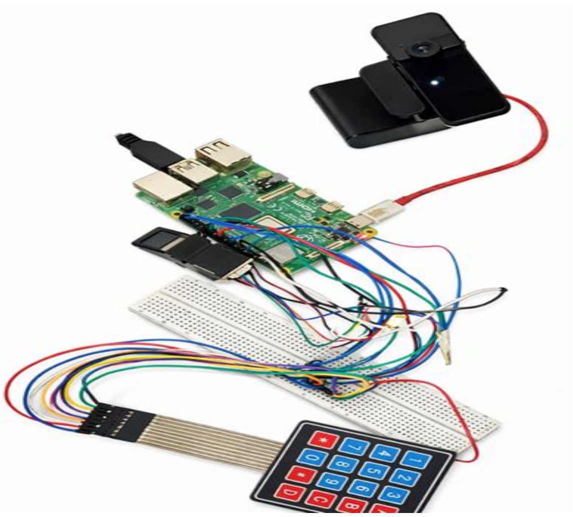
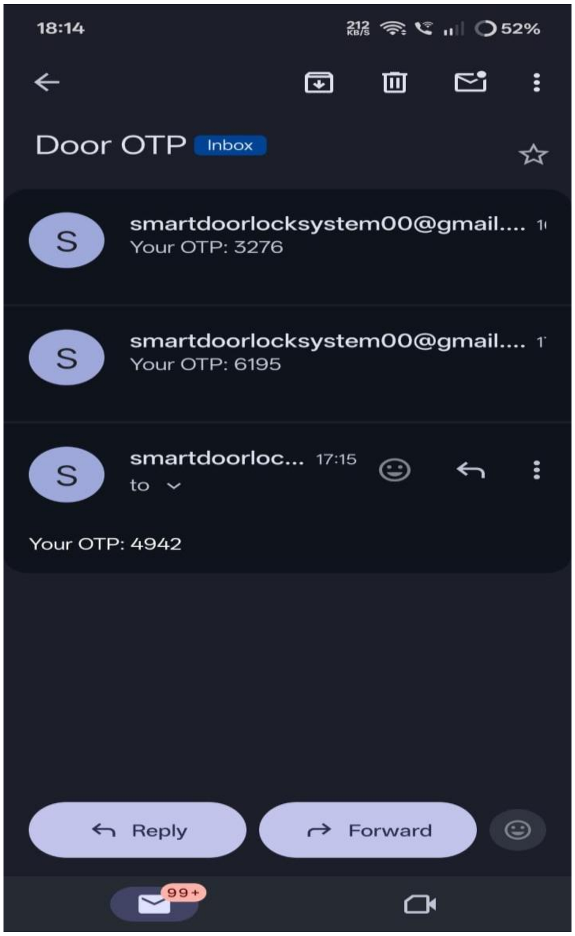


Figure 4: Hardware Prototype of FPGA-Based Smart Biometric Security System The prototype validates the real-time operation of the system and demonstrates successful integration of all hardware modules.

4.2 OTP Verification Result

The OTP-based authentication mechanism is illustrated in Fig. 5. A one-time password is generated and sent to the registered email during access attempts, providing an additional layer of security.

The OTP verification ensures secure remote authentication and prevents unauthorized access even if biometric data is compromised.



18:14 52%

Door OTP Inbox

smartdoorlocksystem00@gmail.... 1
Your OTP: 3276

smartdoorlocksystem00@gmail.... 1
Your OTP: 6195

smartdoorloc... 17:15
to

Your OTP: 4942

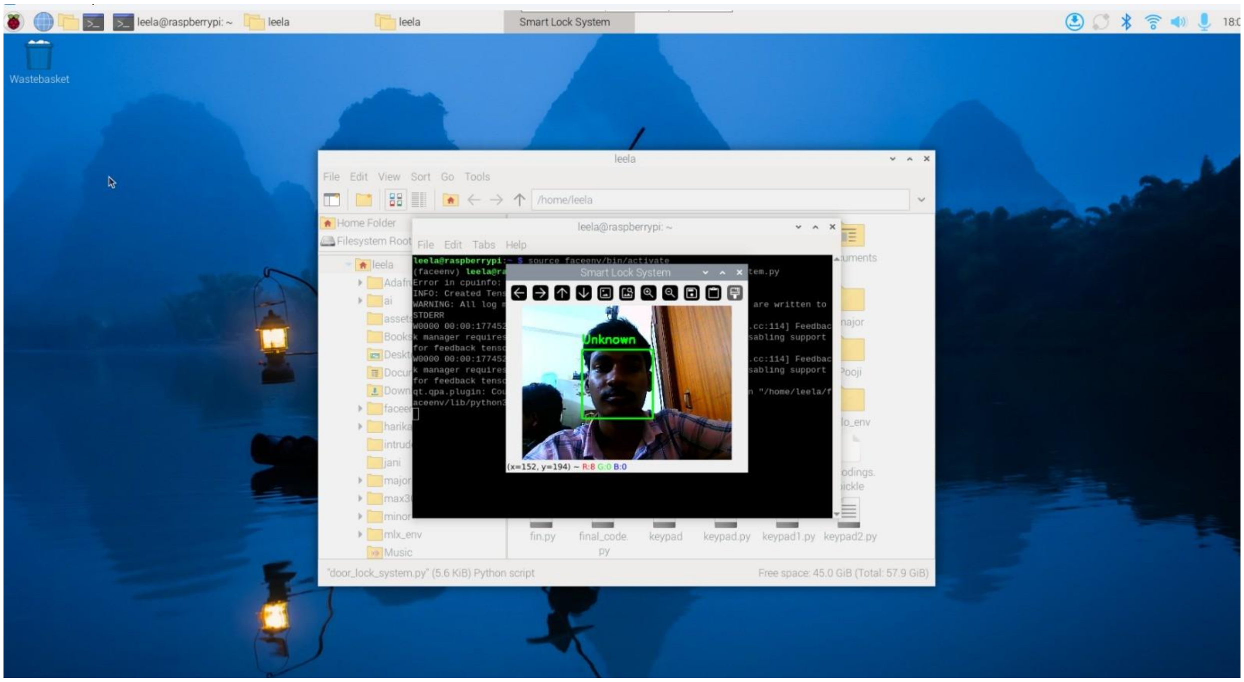
Figure 5: OTP Verification Result via Email

4.3 Camera Monitoring Result

The camera-based monitoring functionality of the system is illustrated in Fig. 6. The Raspberry Pi camera captures real-time images during each access attempt, enabling continuous surveillance and record maintenance.

The captured images provide visual evidence of user access and enhance system transparency. This feature is particularly useful for identifying unauthorized access attempts and maintaining security logs for further analysis.

Additionally, the integration of a camera module ensures real-time monitoring, visual verification, and record maintenance. The captured images provide an additional layer of security by enabling user identification and post-event analysis.



```
leela@raspberrypi:~ $ source faceenv/bin/activate
(faceenv) leela@ra                                    tem.py
Error in cpuinfo:
INFO: Created Tens
WARNING: All log                                      are written to
STDERR
W0000 00:00:177452                                    .cc:114] Feedbac
k manager requires                                    sabling support
for feedback tens
W0000 00:00:177452                                    .cc:114] Feedbac
k manager requires                                    sabling support
for feedback tens
qt.qpa.plugin: Cou                                    n "/home/leela/f
aceenv/lib/python3
```

"door_lock_system.py" (5.6 KiB) Python script

Free space: 45.0 GiB (Total: 57.9 GiB)

Figure 6: Real-Time Image Captured by Camera Module During Access Attempt

4.4 Discussion

The experimental results clearly demonstrate that the proposed system provides superior performance compared to traditional and existing security systems. The FPGA-based implementation enables parallel processing, which significantly reduces response time.

The combination of fingerprint authentication and OTP-based verification enhances security by introducing multi-level authentication. Additionally, the integration of a camera module ensures real-time monitoring and record maintenance.

Although the system introduces slight design complexity due to multiple integrated modules, it offers a highly secure, reliable, and scalable solution. The advantages in terms of performance, accuracy, and security outweigh the limitations.

Overall, the proposed system provides an efficient and intelligent approach for modern smart home security applications.

V. CONCLUSION

This paper presented the design and implementation of an FPGA-based smart biometric security system with multi-level authentication and real-time monitoring capabilities. The proposed system integrates fingerprint authentication, keypad-based access, OTP verification, and camera-based surveillance to provide a comprehensive and secure access control solution.

The use of FPGA as the core processing unit enables parallel processing of authentication inputs, resulting in significantly reduced response time and improved system efficiency compared to conventional microcontroller-based systems. The implementation of multi-level authentication enhances system security by combining biometric verification with OTP-based validation, thereby minimizing the risk of unauthorized access.

The experimental results demonstrate that the proposed system achieves high accuracy, low latency, and reliable performance. The integration of a camera module further strengthens the system by enabling real-time monitoring and maintaining security records.

Overall, the proposed system provides a scalable, efficient, and cost-effective solution for modern smart home security applications. It successfully addresses the limitations of traditional security systems and establishes a strong foundation for future intelligent security architectures.

VI. FUTURE SCOPE

The proposed FPGA-based smart biometric security system can be further enhanced by integrating advanced technologies to improve functionality, scalability, and user convenience.

- IoT Integration: The system can be connected to cloud platforms for real-time monitoring and remote access control using internet connectivity.
- Mobile Application Support: Development of Android/iOS applications can enable users to monitor and control the system remotely, along with receiving instant notifications and alerts.
- AI-Based Facial Recognition: Integration of machine learning algorithms for facial recognition can provide an additional layer of intelligent authentication.
- Wireless Communication: Technologies such as Wi-Fi, Bluetooth, or GSM mod- ules can be incorporated to enable wireless communication between system components.
- Data Analytics Dashboard: A web-based dashboard can be developed to analyze access logs and security patterns for better decision-making.
- Energy Optimization: Low-power FPGA designs and backup power solutions can be implemented to improve energy efficiency.
- Smart Home Integration: The system can be integrated with other smart home devices such as smart locks, lighting systems, and voice assistants to create a fully automated environment.

These enhancements can transform the system into a fully intelligent, connected, and autonomous security solution suitable for next-generation smart homes.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric recognition: Security and privacy concerns,” IEEE Security & Privacy, vol. 1, no. 2, pp. 33–42, 2003.

[2] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, 2004.

[3] Xilinx Inc., “7 Series FPGAs Data Sheet,” 2020.

[4] S. Trimberger, “Three ages of FPGAs: A retrospective on the first thirty years of FPGA technology,” Proc. IEEE, 2015.

[5] N. Z. Bawany et al., “Smart home automation and security system using FPGA,” IEEE Conf., 2017.

[6] M. A. Mazidi et al., “Embedded Systems: Introduction to ARM Cortex,” Pearson, 2015.

[7] Raspberry Pi Foundation, “Raspberry Pi 4 Model B Datasheet,” 2019.

[8] H. Sundmaeker et al., “Vision and challenges for realizing IoT,” European Commis- sion, 2010.

[9] A. Kamilaris and F. Prenafeta-Boldu´, “Deep learning in IoT applications,” Comput- ers and Electronics in Agriculture, 2018.

[10] S. Li, L. Da Xu, and S. Zhao, “The internet of things: A survey,” Information Systems Frontiers, 2015.

[11] J. Gutierrez et al., “Automated security system using wireless sensors,” IEEE Trans., 2014.

[12] P. Mell and T. Grance, “The NIST definition of cloud computing,” NIST, 2011.

[13] D. Vasisht et al., “IoT platform for real-time monitoring,” USENIX, 2017.

[14] L. Ruiz-Garcia et al., “A review of wireless sensor technologies,” Sensors, 2009.

[15] A. Alheraish, “Design of smart home system,” IEEE Trans. Consumer Electronics, 2004.

[16] M. Wolf et al., “Embedded security in smart systems,” IEEE, 2010.

[17] K. K. Patel et al., “IoT-based smart home system,” Int. Journal, 2016.

[18] S. Madakam et al., “Internet of Things: Vision and applications,” Procedia Com- puter Science, 2015.

[19] B. Schneier, “Applied Cryptography,” Wiley, 1996.

[20] A. Ross et al., “Handbook of Multibiometrics,” Springer, 2006.

[21] Y. Wang, “FPGA-based real-time system design,” IEEE Access, 2018.

[22] T. H. Kim et al., “Smart surveillance system using embedded systems,” IEEE, 2016.

[23] J. Smith, “Multi-factor authentication systems,” Journal of Cyber Security, 2019.