Fingerprint Authentication In Smart Home Environment Based On Embedded System

Apri Siswanto
Department of Informatics Engineering, Faculty of Engineering, Universitas Islam Riau,
Pekanbaru, Indonesia
aprisiswanto@eng.uir.ac.id

Akmar Efendi
Department of Informatics Engineering, Faculty of Engineering, Universitas Islam Riau,
Pekanbaru, Indonesia
akmarefendi@eng.uir.ac.id

Evizal Abdul Kadir
Department of Informatics Engineering, Faculty of Engineering, Universitas Islam Riau,
Pekanbaru, Indonesia
evizal@eng.uir.ac.id

2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) | 978-1-6654-7095-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICECCME55909.2022.9988711

***Abstract*— The idea of a "smart home" has recently grown in the security area. The use of biometric fingerprint technology for identification systems, such as those used for home access, is one concern area. This study designed a fingerprint authentication system based on fingerprints and PINs in a smart home environment. The hardware consists of an Arduino Mega 2560 as a microcontroller and an input/output supply. In addition, there is also a fingerprint sensor, and this component is used to capture the fingerprints of users. Based on the hardware design, the study determined implementation costs for authentication systems with fingerprints and PINs in an embedded system environment with lower implementation costs. It shows how to use a simple application to connect a door lock, fingerprint sensor, Arduino microcontroller, number keypad, and door lock.**

Keywords—fingerprint, authentication, security, embedded system, smart home

I. INTRODUCTION

In a smart home environment, user information needs protection to improve security identity management and authentication methods. However, conventional technologies, such as identification (ID) cards and personal identification numbers (PINs), are less reliable because they can be misplaced, forgotten, copied, forged, or misused. Therefore, it is inadequate to secure identity management and user authentication methods. Hence, the need for robust security practices is increasing. One of the practices is a fingerprint authentication system (FAS).

FAS is more secure than an ID card or PIN [1], where fingerprints have sixteen characteristics to distinguish each person, while a PIN only consists of a few numbers. In addition, FAS provides excellent accuracy and speed to become a more reliable and precise solution for user authentication and identity management [2]. A fingerprint system is a commonly used technology for user authentication and access control devices. It can manage access in various settings, including homes, workplaces, banks, factories, hospitals, universities, and e-commerce. This system can be implemented in an embedded system, combining hardware and software for specific functions in a particular device [3]. The system consists of a microcontroller, fingerprint sensor, secure access control, and human interface. In a FAS, users' fingerprint information, known as fingerprint template (FT), is stored in the embedded device.

FAS can be divided into two main processes: (1) enrolment and (2) authentication. During the enrolment process, users' FT is registered and stored in a database, while the enrolment phase compares and verifies users' FT with the one stored in the database. In the process of enrolment, the fingerprint will be used as an identifier. Afterward, a sensor acquires data, and an algorithm processes them to extract fingerprint characteristics (i.e., templates). Finally, the template is stored in local or remote storage for future comparisons. Once the enrolment has been completed, the users are authenticated through the following steps: 1) reading the fingerprint, 2) extracting characteristics, and 3) comparing one by one with the previously stored template [4].

Fingerprint information or FT must be protected to ensure that only authorized users can access offices, banks, factories, hospitals, universities, smart homes, e-commerce, cell phones, personal systems, and others. Therefore, identity theft could be avoided while preventing replay attacks, stolen-verifier attacks, and perfect forward secrecy [5]. The most significant attack in FAS is the replacement of FT by impostors to gain unauthorized access. Therefore, fingerprint template protection (FTP) is needed to access offices, banks, factories, hospitals, universities, smart homes, e-commerce, cell phones, and personal systems to improve security in both enrolment and authentication for personal fingerprint protection.

According to Jain, et al. [6], the FTP scheme protects the user's fingerprint template and identities various biometric system vulnerabilities from leakage of biometric template information, leading to severe security and privacy threats. Wong, et al. [7] also said that FTP is a way to avoid the FT from being compromised, to experience permanent privacy and security issues. Other than that, Stanko, et al. [8] argued that FTP scheme is a technique for privacy-preserving storage of fingerprint data. In line with this argument, Mwema, et al. [9] said that the FTP scheme is a technique to secure biometric systems against these attacks. In short, FTP scheme is a generalized and efficient method to preserve privacy and to enhance the security of fingerprint authentication by limiting the exposure of FT data, which cannot be revoked. Although there are many studies that showed improvements in FTP schemes, there are still many open issues that need to be resolved by researchers [10]. Most importantly, FTP schemes have different requirements depending on their applications' domain. Unlike other applications' domains, user authentication in the embedded system operates on resource-constraint devices.

In this study, FAS is proposed based on Fingerprint and PIN. In previous studies, an Internet of things (IoT)-based security system was designed using an Arduino microcontroller, and a fingerprint sensor was used to read the homeowner's fingerprint sensor. This system aims to design a tool for home security, especially the door of the house, which is very risky for theft, by using a fingerprint sensor as a verification for people who will enter the house, resulting in a system that can reduce the risk of theft at home [11, 12]. This research has the advantage of two alternatives that can be used to open door access in a smart home environment. The resident able use the PIN stored in the database to open the door if the sensor is unable to read the fingerprint data because of unclean or damaged hardware or fingers. The system is also equipped to handle a homeowner's request to delete a user.

II. BIOMETRICS IN EMBEDDED SYSTEM

Biometrics have been implemented in many embedded systems [13, 14]. Alilla, et al. [15], Danese, et al. [16], Nie, et al. [17], Shinde and Bendre [18] and Dahal [19] presented the implementation of biometrics in an embedded system based on microcontroller and field-programmable gate array (FPGA). However, biometric data encryption is not achieved in any FPGA implementation. Some research related to fingerprint authentication and embedded systems is presented in Table 1.

TABLE I. RESEARCH ON FINGERPRINT AUTHENTICATION SYSTEM

References	Embedded type	Highlights	Biometric
Nayak [20]	32-bit RISC microprocessor	The research suggested a fingerprint sensor that combines sensors and 32-bit RISC microprocessors on a single chip. Additionally, it has a sophisticated detecting system for processing signals from capacitive fingerprint sensors and a robust isolation system to counteract Electrostatic Discharge (ESD) effects.	Fingerprint
Militello, et al. [21]	FPGA	This study recommended embedded fingerprint authentication based on core and delta singularity points. The two components of the suggested method are extraction and matching algorithm point singularities.	Fingerprint
Nie, et al. [17]	FPGA	A multilayer fingerprinting technique for FPGA IP protection was proposed in this study.	Fingerprint
Murillo-Escobar, et al. [22]	Freescale	This research proposed an FTP based on the chaos-based encryption algorithm.	Fingerprint
Martin, et al. [23]		The research proposed a global schema for fingerprint authentication with Arduino and fingerprint reader, a database server, and monitoring mobile applications via smartphone. However, there is no encryption process in data transmission.	Fingerprint
García Vargas, et al. [24]	PIC18f252	A portable and effective fingerprint authentication system was suggested in this study. The device uses a fingerprint optical sensor with an integrated microcontroller for efficient image processing.	Fingerprint

The hardware and software that comprise the embedded system use input-output devices and CPUs with constrained memory and processing capabilities. Low cost, small physical size, low power consumption, good performance, and adaptability are all benefits of the system [20]. In other words, a template security interface on an embedded FAS can lower the risk of fraud and identity theft. An embedded expert system may execute fingerprint enrollment and verification with security assurances, cheap cost, high performance, guaranteed template protection, store data, and send it via unsecured connections[22]. This system can potentially be used as access control in an embedded system environment or smart offices. Embedded systems are designed for the specific purpose of performing one or many tasks in real-time computing. The characteristics of this system are [25] :

1. designed in one integrated device between one component and other components in a microcontroller.
2. designed to perform specific tasks and not for general tasks.
3. software for this system is generally in the form of firmware, which is the software to communicate and interact in real-time with hardware.

Fingerprint templates can be imitated or modified so that legal users cannot access the legal system environment and compromise the system's security. Then, the attackers illegally access and modify the system later. In addition, they can change the access rights of authorized users [26]. FT can be modified or replicated because FTP schemes are also vulnerable to systems that exploit insecure system infrastructures, such as replay attacks and denial of service attacks (see Figure 1). There are also loopholes or insider attacks [27].

Additional vulnerabilities from the FTP scheme are related to people's ability to identify fingerprint patterns based on fingerprints obtained from an object touched and limited liveness-detection capabilities of conventional FTP systems. FTP system is an architecture of fingerprint authentication, indicating its significant vulnerabilities and its four underlying causes, as shown in Figure 1. It is not difficult to make spoof fingerprints from fingerprints images or even a stored FT and get unauthorized access. This system is also vulnerable to intrinsic failure (also known as zero-effort attacks), which leads to incorrect authentication. Finally, it is due to limited individuality and intra-class fingerprint features that need to be secured by the FTP algorithm so that data integrity can be maintained properly.

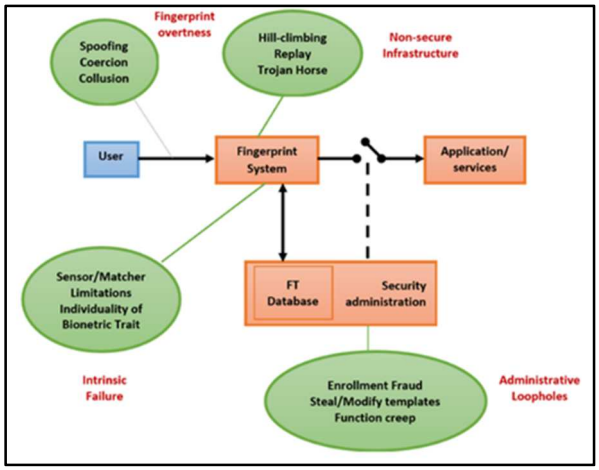

Fig. 1. The architecture of a biometric-based authentication system indicates its major vulnerabilities and their four underlying causes [27]

Fingerprint refers to the lines that appear on the skin of the fingertips. The fingerprint works to give a more significant frictional force for the finger to hold objects closer [28]. The reason for choosing fingerprint in this study is because it is highly distinctive and unique to every person, even identical twins [29]. Then, fingerprint authentication is the most extensive and reliable mechanism for individual identification [30]. It is also usually accessible, reliable, and highly accurate [31]. It has been widely used in various fields, including attendance systems, immigration, home building access, etc. A fingerprint is an ultimate choice for excellence as a biometric identifier. It has long been employed for recognition purposes. The reliability and superiority of fingerprints in authentication systems have gone beyond other types of biometrics such as faces or irises [32]. At the same time, due to the decreasing cost and size of fingerprint sensors, it is very prospective that fingerprint continues to be widely used in biometric recognition systems in the future. Indeed, the recent biometric market report, a summary in the Wall Street Journal, estimates that FAS will continue to dominate the biometric market in the future.

III. DESIGNING FAS IN A SMART HOME ENVIRONMENT

The FAS was implemented on a hardware module that included a 32-bit microcontroller, fingerprint sensor, networking tool, and human interface. In the enrolment process, the user can register the FT by using minutiae extraction to generate the user's FT. Then, the FT is sent to the microcontroller through the transmission line and stored in the microcontroller's flash memory. For the verification, users' FT will be compared to the FT stored in the database to authenticate the users. The hardware design is illustrated in Figure 2.

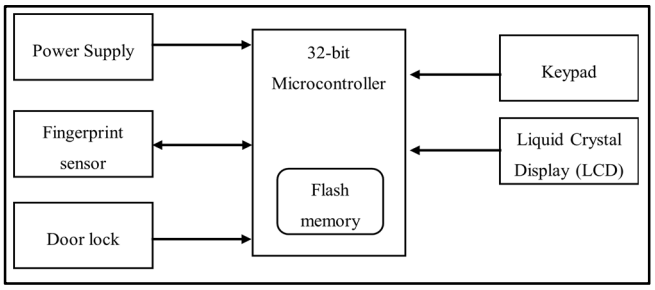

Fig. 2. The proposed hardware design of the FAS

The materials used in this study are divided into two categories software and hardware. Software resources are substances that cannot be seen or touched. They are virtual objects used in application development. Software applications include Arduino IDE, and C programming language. It provides access to the enormous Arduino library. Hardware component refers to concrete equipment used in the study, such as microcontroller, Personal Computer (PC), LCD, fingerprint optic sensor, door lock, and power supply.

IV. RESULT AND DISCUSSION

Fingerprint sensors control the smart home's main entrance and garage door. When this system is installed at home, authorized homeowners must use a simple application to register their fingerprint data, which is then kept in the microcontroller memory. Residents enter their PINs and use the fingerprint sensor to scan their fingerprints. In Arduino memory, the scan results are kept in digital format. Then, fingerprint records are analyzed to generate a list of distinct fingerprint features. A database stores the fingerprint pattern feature. Residents' fingerprint patterns will be changed to match those in the database when they scan their fingertips. If the two data sets are identical, the Arduino memory sends an agreement signal to the microcontroller, allowing the residents to unlock the electric latch/door lock. Figure 3 depicts the prototype that was produced.

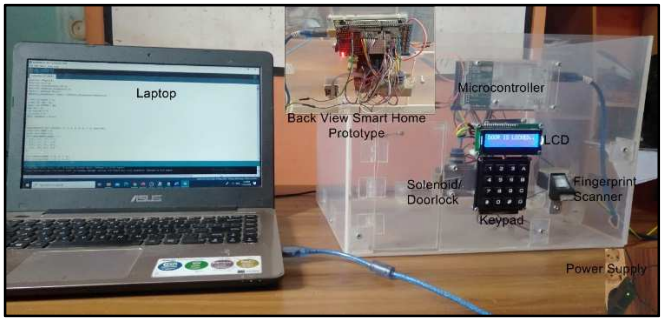

Fig. 3. Hardware prototype design

A resident necessity enrol his fingerprint in a smart home system for it to be recognized in the microcontroller database during the fingerprint user enrollment process. The following are the steps in the registration procedure. The user first enters their PIN and then scans their fingerprint. The user must then place their finger again to guarantee that the fingerprint model is formed. The resident will be able to access the smart home that has been constructed using the user's fingerprint or PIN

registered in the database after the fingerprint data has been effectively verified into the database. The fingerprint enrolment method for smart house door lock security is depicted in Figure 4.

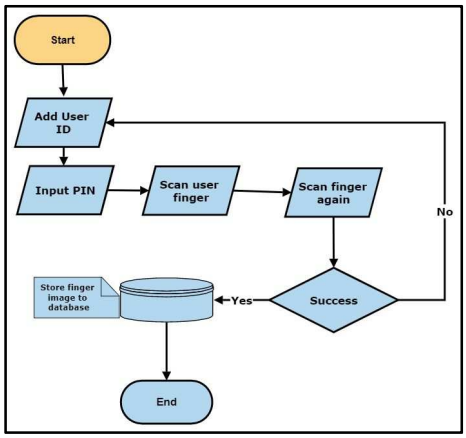

Fig. 4. Flow chart of enrolment process

There are three stages to handling the smart home prototype enrolment process. The first is the display process in the embedded smart-home system when deciding whether to add, delete, open, or exit. For example, to add a new user, press the "Add" button and then enter the new user's PIN. The fingerprint data will be recorded in the smart home system once you place your finger on the sensor twice. As illustrated in Figure 5, the prototype was created in an embedded smart home environment.

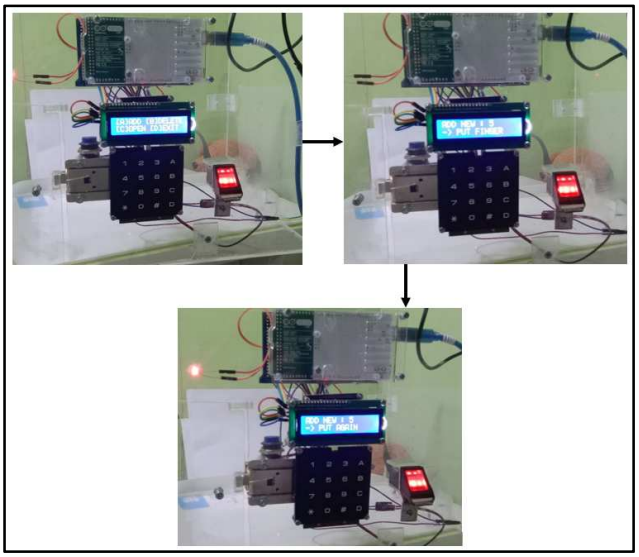

Fig. 5. Enrolment process in prototype smart home

The user fingerprint template that has registered with the system will be able to access the prototype of the smart home environment once it has been successfully entered into the database. The user scans their finger by placing it on a fingerprint sensor. The data model and database will be compared by the system. If it is appropriate, the door or solenoid will open; if it is not, it will be rejected. The user can open the door using the PIN that has been saved in the database if the sensor is unable to read the fingerprint data because to dirty or damaged hardware or fingers. A user's request to be deleted by the homeowner can also be handled by the system. The created prototype system's flowchart is shown in Figure 6.

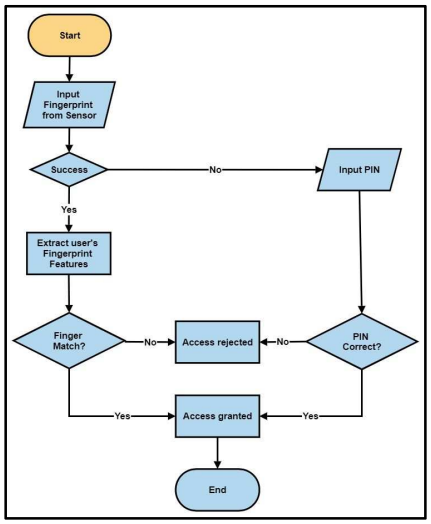

Fig. 6. Authentication process flow chart

At the moment, authentication methods rely on smart cards, which if lost will definitely lead to a number of security problems. Security difficulties brought on by lost or stolen smart cards could be resolved by using the proposed fingerprint system or PIN protocol for authentication. The authentication procedure in the smart house prototype is shown in Figure 7.

Fig. 7. The authentication process in the prototype

The solenoid will still lock even if the fingerprint pattern reading is off and the user is not listed in the system database. The LCD will display "access refused" in this case.

Based on testing with numerous user fingerprints, this prototype appears capable of performing well in the database's enrolment and authentication processes. The testing of user fingerprint prototypes in the smart home setting is shown in Table 2. The user creates a PIN and scans their fingerprints twice during enrolment. On the table, fingerprints are used instead of a PIN for authentication. The proposed FAS takes 3.5 seconds to enroll and 2 seconds to authenticate. However,

The user can enter a PIN to obtain access to the smart home system if the fingerprint sensors malfunction or the user's finger is injured (dirty) and can no longer be used to enter or unlock doors in the home.

V. CONCLUSION

This study designed a FAS based on fingerprints and PINs in a smart home environment. The proposed FAS is more efficient and secure for the authentication system in a smart home environment. It consists of user enrolment and authentication phases. A fingerprint smart home authentication model offers a rudimentary impression of integrating a door lock, fingerprint sensor, Arduino microcontroller, number keypad, and door lock with a modest application. The future research of this study is to design other biometric encryption and authentication schemes, such as face recognition, which may be very useful, especially during the Covid19 pandemic, where touching objects should be avoided where possible. This work is quite well developed, especially for the crossing system between countries.

REFERENCES

[1] F. R. Ishengoma, "Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies," *arXiv preprint arXiv:1410.0534,* pp. 162-167, 2014.

[2] D. Harikrishnan, N. Sunil Kumar, S. Joseph, and K. K. Nair, "Towards a fast and secure fingerprint authentication system based on a novel encoding scheme," *The International Journal of Electrical Engineering & Education,* pp. 1-13, 2019.

[3] P. Marwedel, *Embedded System Design: Embedded Systems, Foundations of Cyber-Physical Systems, and the Internet of Things*: Springer International Publishing: Imprint: Springer, 2018.

[4] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*: Springer Publishing Company, Incorporated, 2009.

[5] F. Demenschonok, J. Harrigan, and T. Bonaci, "An Overview of Fingerprint-Based Authentication: Liveness Detection and Beyond," *arXiv preprint arXiv:2001.09183,* pp. 1-13, 2020.

[6] A. K. Jain, K. Nandakumar, and A. Nagar, "Fingerprint template protection: From theory to practice," in *Security and privacy in Biometrics*, ed: Springer, 2013, pp. 187-214.

[7] K.-w. Wong, A. B. Teoh, M. D. Wong, and Y. H. Kho, "Enhanced multi-line code for minutiae-based fingerprint template protection," *Pattern Recognition Letters,* vol. 34, pp. 1221-1229, 2013.

[8] T. Stanko, B. Chen, and B. Škorić, "Fingerprint template protection using minutia-pair spectral representations," *EURASIP Journal on Information Security,* vol. 2019, pp. 1-15, 2019.

[9] J. Mwema, M. Kimwele, and S. Kimani, "A simple review of biometric template protection schemes used in preventing adversary attacks on biometric fingerprint templates," *International Journal of Computer Trends and Technology,* vol. 20, pp. 12-18, 2015.

[10] A. Sarkar and B. K. Singh, "A review on performance,security and various biometric template protection schemes for biometric authentication systems," *Multimedia Tools and Applications,* vol. 79, pp. 27721–27776 2020/07/29 2020.

[11] M. Faturrachman and I. Yustiana, "Sistem Keamanan Pintu Rumah dengan Sidik Jari Berbasis Internet of Things (IOT)," *Jurnal Teknik Informatika UNIKA Santo Thomas,* pp. 379-385, 2021.

[12] S. D. Putu Eka, "Sistem Keamanan Pintu Menggunakan Sensor Sidik Jari Berbasis Mikrokontroler Arduino Uno R3," *Sistem Keamanan Pintu Menggunakan Sensor Sidik Jari Berbasis Mikrokontroler Arduino Uno R3,* 2019.

[13] A. Fadell, A. Hodge, S. Schell, R. Caballero, J. L. Dorogusker, S. Zadesky*, et al.*, "Embedded authentication systems in an electronic device," ed: Google Patents, 2014.

[14] T. Phillips, X. Zou, F. Li, and N. Li, "Enhancing Biometric-Capsule-based Authentication and Facial Recognition via Deep Learning," in *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, Toronto ON, Canada, 2019, pp. 141–146.

[15] A. Alilla, M. Faccio, T. Vali, G. Marotta, and L. DeSantis, "A new low cost fingerprint recognition system on FPGA," in *2013 IEEE International Conference on Industrial Technology (ICIT)*, 2013, pp. 988-993.

[16] G. Danese, M. Giachero, F. Leporati, G. Matrone, and N. Nazzicari, "An FPGA-based embedded system for fingerprint matching using phase-only correlation algorithm," in *Conference on Digital System Design, Architectures, Methods and Tools*, 2009, pp. 672-679.

[17] T. Nie, Y. Li, L. Zhou, and M. Toyonaga, "A multilevel fingerprinting method for FPGA IP protection," in *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2013, pp. 1789-1792.

[18] A. S. Shinde and V. Bendre, "An Embedded Fingerprint Authentication System," in *International Conference on Computing Communication Control and Automation*, 2015, pp. 205-208.

[19] D. Dahal, "Electronic Fingerprint Voting System," Bachelor's Thesis, Helsinki Metropolia University of Applied Sciences, 2019.

[20] D. R. Nayak, "A novel architecture for embedded biometric authentication system," in *2008 Second UKSIM European Symposium on Computer Modeling and Simulation*, 2008, pp. 567-572.

[21] C. Militello, V. Conti, F. Sorbello, and S. Vitabile, "A novel embedded fingerprints authentication system based on singularity points," in *2008 International Conference on Complex, Intelligent and Software Intensive Systems*, 2008, pp. 72-78.

[22] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. M. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," *Expert Systems with Applications,* vol. 42, pp. 8198-8211, 2015.

[23] M. Martin, K. Štefan, and F. L'ubor, "Biometrics Authentication of Fingerprint with Using Fingerprint Reader and Microcontroller Arduino," *Telkomnika,* vol. 16, pp. 755-765, 2018.

[24] M. García Vargas, F. E. Hoyos, and J. E. Candelo, "Portable and efficient fingerprint authentication system based on a microcontroller," *International Journal of Electrical & Computer Engineering,* vol. 9, pp. 2346-2353, 2019.

[25] T. A. Henzinger and J. Sifakis, "The embedded systems design challenge," in *International Symposium on Formal Methods*, 2006, pp. 1-15.

[26] M. Joshi, B. Mazumdar, and S. Dey, "Security Vulnerabilities Against Fingerprint Biometric System," *arXiv preprint arXiv:1805.07116,* pp. 1-27, 2018.

[27] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing,* vol. 2008, pp. 1-17, 2008.

[28] J. D. Purbani, "Pembuatan mesin identifikasi sidik jari sebagai kunci pengaman pintu," Bachelor's Thesis, Universitas Sebelas Maret, 2010.

[29] A. Morales, R. Cappelli, M. A. Ferrer, and D. Maltoni, "Synthesis and evaluation of high resolution hand-prints," *IEEE Transactions on Information Forensics and Security,* vol. 9, pp. 1922-1932, 2014.

[30] K. Yoonjeong, J. Yoon, J.-H. Joo, and K. Yi, "Robust lightweight fingerprint encryption using random block feedback," *Electronics Letters,* vol. 50, pp. 267-268, 2014.

[31] H. van de Haar, D. van Greunen, and D. Pottas, "The characteristics of a biometric," in *2013 Information Security for South Africa*, 2013, pp. 1-8.

[32] R. Bhatia, "Biometrics and face recognition techniques," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, pp. 93-99, May 2013 2013.