International Journal of Scientific Engineering and Science
Volume 9, Issue 4, pp. 129-133, 2025. ISSN (Online): 2456-7361

A Conceptual Design of a Deep Learning-Based Smart Door Security System

Muhamad Yusuf[1], Mohammad Fathin Al Fikri[2], Rivo Juniandra Rumadi[3], Muhammad Ilham Abdul Mufid[4], Kharisma Rahmawati Lubis[5], Muhammad Givi Efgivia[6]
[123456]Faculty of Industrial Technology and Informatics, Muhammadiyah Prof. Dr. Hamka University, Indonesia
Email: [1]2203015092@uhamka.ac.id, [2]2203015010@uhamka.ac.id, [3]2203015126@uhamka.ac.id, [4]2203015148@uhamka.ac.id, [5]2203015072@uhamka.ac.id, [6]mgivi@uhamka.ac.id

Abstract— *The growing need for intelligent and secure access control solutions has accelerated the adoption of biometric authentication systems enhanced by machine learning (ML). This paper presents a conceptual design of a smart door security system that integrates advanced ML techniques particularly deep learning to achieve robust, real-time user authentication. Traditional methods such as keys, passwords, and access cards are increasingly inadequate due to their susceptibility to loss, theft, and duplication. In comparison, biometric systems employ distinctive physical and behavioral characteristics, such as facial features and fingerprints, which are naturally more secure and easier for users. At the core of the proposed system is the use of deep neural networks for feature extraction and classification. Convolutional Neural Networks (CNNs) are employed for processing visual biometric data, such as facial images, while Recurrent Neural Networks (RNNs) can be adapted for modalities involving sequential input like voice or behavioral patterns. These models enhance the accuracy and efficiency of the system, particularly in uncontrolled or variable environments. Moreover, the system incorporates ML-driven liveness detection and anti-spoofing mechanisms, which analyze subtle physiological cues to detect fake biometric samples such as photos or silicone fingerprints. The system architecture supports a multimodal biometric approach, combining multiple authentication factors to reduce false acceptance and rejection rates. This redundancy significantly increases resistance to spoofing attacks and ensures reliable operation across diverse environmental conditions. The design is scalable, enabling future expansion to include additional modalities like iris or voice recognition, and supports integration with IoT-based monitoring systems. This study demonstrates the practical application of machine learning in embedded biometric systems, contributing to the advancement of secure and adaptive access control technologies. The findings offer valuable insights for researchers and practitioners aiming to develop next-generation authentication systems that are resilient, accurate, and convenient in real-world scenarios.*

Keywords— *Deep Learning, Biometric Authentication, Smart Door Security, Multimodal Biometrics, Anti-Spoofing.*

I. INTRODUCTION

As digital transformation accelerates across various sectors, the demand for advanced and intelligent physical security systems has become increasingly pressing. Traditional access control methods—such as physical keys, PINs, and RFID cards—despite their widespread adoption, exhibit critical vulnerabilities. These conventional mechanisms are susceptible to loss, theft, duplication, and unauthorized use, rendering them inadequate for safeguarding sensitive environments, including smart homes, corporate offices, research laboratories, and critical infrastructure. Recent studies highlight that these traditional systems often fail to meet the security needs of modern applications, necessitating the integration of more sophisticated biometric solutions that leverage advanced technologies such as recurrent neural networks (RNNs) for enhanced authentication and anomaly detection (Alhamdani et al., 2022).

Biometric authentication emerges as a compelling solution, leveraging unique physical or behavioral characteristics of individuals, such as facial features and fingerprints. These traits are inherently difficult to forge or transfer, thereby enhancing the security and user-friendliness of biometric systems (Mane & Bhosale, 2023). However, systems relying on a single biometric modality often grapple with challenges related to environmental variability, sensor quality, and the persistent threat of spoofing attacks, which can significantly undermine their reliability and effectiveness (Liébana-Cabanillas et al., 2024).

The advent of artificial intelligence, particularly deep learning, has catalyzed new opportunities in the development of biometric access control systems. Deep learning facilitates the automatic extraction of meaningful features from complex biometric data, thereby improving accuracy and adaptability under diverse conditions. Its capacity for pattern recognition and generalization positions it as a suitable approach for enhancing authentication performance, even in real-world, dynamic scenarios (Sharma & Chaudhary, 2023).

This study proposes a biometric access system that integrates facial and fingerprint recognition within a deep learning-based framework. The combination of these two modalities offers a more robust and reliable authentication process compared to systems that rely solely on a single biometric input. Furthermore, the system incorporates anti-spoofing mechanisms designed to detect and thwart presentation attacks, such as the use of counterfeit fingerprints or facial images.

The architecture of the proposed system is designed to support scalability and future enhancements, including the potential integration of additional biometric modalities and connectivity features for centralized monitoring and control. By leveraging deep learning within a multimodal biometric framework, this research aims to provide a more secure,

adaptable, and practical access control solution for modern smart environments.

II. METHOD

This study employs a literature review methodology to develop a conceptual framework for a secure biometric authentication system. The literature review approach enables a systematic exploration and synthesis of existing research on biometric systems, deep learning techniques, and multimodal authentication solutions. The objective is to identify relevant theories, methodologies, and technologies that contribute to the design and implementation of advanced biometric security systems (Kish, 2018).

The literature review serves as a foundation for understanding the underlying principles and emerging technologies pertinent to biometric authentication. It involves identifying, evaluating, and synthesizing existing research on topics such as authentication mechanisms, system vulnerabilities, user identity verification, and integration with smart environments. This process aids in formulating a comprehensive view of the field and informs the conceptual development of the proposed system.

To ensure the quality and relevance of the reviewed materials, the study focuses on peer-reviewed sources published in recent years. These sources span various domains, including computer science, information security, and artificial intelligence. The review does not concentrate on a specific algorithm or technology but aims to understand broader trends and methods that contribute to building secure, efficient, and adaptive biometric systems.

The findings from the literature form the basis for designing a conceptual model that emphasizes system robustness, user convenience, and adaptability to real-world conditions. This general framework can later be refined and tested in future research or practical implementations using appropriate methodologies and technologies.

III. RESULT & DISCUSSION

A. Emerging Trends in Biometric Systems

The evolution of biometric systems has reached a pivotal stage, characterized by rapid technological advancements that are fundamentally transforming authentication paradigms. As organizations and individuals increasingly seek secure and efficient methods of identity verification, contemporary biometric solutions are emerging as a cornerstone of modern security frameworks. These systems use special physical and behavior-based features like fingerprints, face, eyes, and voice to give more accurate and reliable security than traditional methods.

Recent innovations in biometric technology have led to unprecedented accuracy rates, often exceeding 99% in ideal conditions. This remarkable precision is largely attributable to advancements in machine learning and deep learning algorithms, which enable the automatic extraction and analysis of complex biometric features from raw data. For instance, convolutional neural networks (CNNs) have been particularly effective in enhancing facial recognition capabilities by allowing systems to learn intricate patterns and variations in facial features, even under diverse lighting conditions and angles (Alhamdani et al., 2022). Similarly, recurrent neural networks (RNNs) have shown promise in processing sequential data, making them suitable for applications such as voice recognition and behavioral biometrics, where temporal patterns are crucial for accurate identification.

Moreover, the integration of multimodal biometric systems where multiple biometric traits are combined has emerged as a significant trend in the field. By leveraging the strengths of various modalities, such as combining facial recognition with fingerprint scanning, these systems enhance security and reduce the likelihood of false positives and negatives. This approach not only improves the overall accuracy of authentication but also provides a robust defense against spoofing attacks, where malicious actors attempt to deceive the system using fake biometric samples (Septyanlie et al., 2024). The synergistic effect of multimodal systems creates a more resilient authentication framework, ensuring that weaknesses in one modality can be compensated for by the strengths of another.

TABLE 1: Overview of Biometric Modalities

Modality	Accuracy	Advantages
Fingerprint	90-99%	High Accuracy
Facial Recognition	95-99%	Contactless, fast
Iris Recognition	99%	Very Accurate
Voice Recognition	90-95%	Hands-free
Vein Pattern	98%	High security
Multimodal	99%	Enhanced security

The following table summarizes various biometric modalities, highlighting their accuracy rates, advantages, challenges, and applications.

The experience of the user has also been a primary area of advancement in biometric systems. As these technologies evolve, they are increasingly crafted to be user-friendly and discreet. For example, advancements in touchless biometric systems, such as facial recognition and iris scanning, allow for seamless interactions that do not require physical contact, thereby enhancing convenience and hygiene an aspect that has gained particular importance after the COVID-19 outbreak pandemic. This shift towards more intuitive and accessible biometric solutions reflects a growing recognition of the need to balance security imperatives with operational practicality in smart environments (Murjitama et al., 2024).

Furthermore, the proliferation of Internet of Things (IoT) devices has catalyzed the integration of biometric systems into everyday applications, from smart home security to mobile payments. As these devices become interconnected, the demand for secure and efficient authentication methods has surged, prompting the development of biometric solutions that can operate in real-time and across various platforms. This trend not only enhances security but also facilitates a more cohesive user experience, as individuals can utilize their biometric data across multiple devices and services without the need for multiple passwords or PINs.

In conclusion, the emerging trends in biometric systems signify a transformative shift in how identity verification is approached. With advancements in technology driving unprecedented accuracy, the integration of multimodal systems

enhancing security, and a focus on user experience making these solutions more accessible, biometric authentication is poised to become a fundamental component of modern security infrastructures. As these systems continue to evolve, they will play an increasingly key part in protecting important areas and keeping digital activities safe and trustworthy

B. *Biometric Systems: Balancing Security and Practical Considerations*

Biometric systems provide significant advantages in accuracy and user convenience, yet they also present critical challenges that require careful attention. A primary concern is the tension between robust security and user privacy. Biometric data, such as fingerprints and facial images, are unique and permanent. If compromised, they can lead to severe privacy violations, making their protection essential. This necessitates stringent data protection measures and compliance with privacy regulations (Ananta et al., 2024).

The centralized storage of sensitive biometric data brings additional risks, as these databases are appealing targets for cyberattacks. If breached, they could reveal large volumes of personal data, potentially resulting in identity theft. Organizations must implement strong encryption and access control measures to safeguard this data effectively (Ananta et al., 2024).

Spoofing attempts are another significant threat, particularly for unimodal biometric systems that rely on a single authentication factor. These systems are vulnerable to attacks using replicas or images, which can undermine their effectiveness. Research indicates that unimodal systems struggle to adapt to variable environmental conditions, such as lighting changes, further compromising their reliability (Ananta et al., 2024).

To mitigate these challenges, multimodal biometric systems are gaining traction. By combining multiple biometric traits, such as fingerprints and facial recognition, these systems enhance security and reduce the likelihood of successful spoofing attempts. However, implementing multimodal systems can be complex and costly, requiring careful planning and investment (Ananta et al., 2024).

Balancing security and user accessibility is crucial. While enhancing security measures is vital, it should not hinder user convenience. Biometric systems must be designed for seamless user experiences, ensuring quick and efficient authentication. User acceptance is closely linked to perceived ease of use and effectiveness, particularly in consumer-facing applications (Ananta et al., 2024).

In summary, while biometric systems offer promising solutions for secure authentication, they also present challenges that must be addressed. The interplay between security, privacy, and user experience requires a thoughtful approach to the design and implementation of biometric technologies. Ongoing research and development will be essential to create systems that effectively balance these critical considerations (Ananta et al., 2024).

C. *The Multimodal Advantage*

Multimodal biometric systems present a robust solution to the challenges faced by unimodal systems, offering enhanced security through the integration of multiple authentication mechanisms. Research indicates that combining various biometric factors consistently yields superior performance compared to single factor approaches (Septyanlie et al., 2024). This synergistic effect creates a more resilient authentication framework, where the weaknesses of one modality can be compensated for by the strengths of another.

TABLE 2: Comparison between Unimodal vs Multimodal Systems

Feature	Unimodal Systems	Multimodal Systems
Accuracy	Moderate	High
Security Level	Vulnerable	Robust
User Satisfaction	Variable	High
Adaptability	Limited	Flexible
Spoofing Resistance	Low	High

The following table provides a comparative overview of the key features, advantages, and disadvantages of unimodal and multimodal biometric systems, highlighting the significant benefits of adopting a multimodal approach.

For example, facial recognition may struggle in low-light conditions, but this limitation can be effectively addressed by incorporating fingerprint verification. Such a combination ensures reliable performance across diverse scenarios, enhancing the overall accuracy of the system. Additionally, the inherent redundancy of multimodal systems significantly complicates spoofing attempts. Attackers would need to simultaneously bypass multiple independent authentication layers, making successful breaches considerably more difficult (Jannah et al., 2024).

TABLE 3: Performance Metrics of Biometric Modalities

Biometric Modality	Accuracy (%)	FAR (%)	FRR (%)	EER (%)
Facial Recognition	85-95	0.1-5	5-15	1-10
Fingerprint Recognition	90-99	0.01-1	1-5	0.5-2
Iris Recognition	95-99	0.01-0.5	1-3	0.1-1
Voice Recognition	80-95	1-10	5-20	2-15
Palm Vein Recognition	95-99	0.01-0.5	1-3	0.1-1
Retina Recognition	90-98	0.1-1	1-5	0.5-2

The table above presents a comparative analysis of various biometric modalities based on four critical performance metrics: Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). Each biometric modality demonstrates varying levels of effectiveness, with fingerprint and iris recognition generally exhibiting the highest accuracy and lowest FAR and FRR, indicating their reliability in authentication scenarios. In contrast, voice recognition shows a wider range of FAR and FRR, suggesting potential challenges in its implementation. Overall, this data underscores the importance of selecting the appropriate biometric modality based on specific security requirements and user contexts, as each modality has its

strengths and weaknesses that can impact overall system performance.

Furthermore, multimodal systems can adapt to varying user conditions and environments, improving user experience and satisfaction. By leveraging different biometric traits, these systems can provide more flexible and inclusive authentication options, accommodating users with different needs or preferences. This adaptability not only enhances security but also fosters greater user acceptance, as individuals are more likely to trust systems that offer reliable and convenient access (Septyanlie et al., 2024).

In summary, the multimodal approach addresses the limitations of unimodal systems by providing a more secure, reliable, and user-friendly authentication solution. The combination of multiple biometric factors not only enhances performance but also significantly increases resistance to spoofing, making it a compelling choice for modern security applications (Jannah et al., 2024).

D. AI-Driven Enhancements in Biometric Security

The incorporation of artificial intelligence (AI) has greatly enhanced biometric systems by introducing adaptive learning and advanced threat detection capabilities. Machine learning algorithms are particularly effective at interpreting complex data patterns found in multimodal biometrics, enabling systems to continuously learn and gradually increase their accuracy. This capability is particularly valuable as it enables biometric systems to adapt to variations in user behavior and environmental conditions, enhancing overall reliability (Alhamdani et al., 2022).

Advanced liveness detection, powered by deep learning, plays a crucial role in distinguishing genuine biometric traits from artificial replicas. By analyzing subtle physiological cues, such as skin texture and micro-movements, these intelligent systems can effectively identify spoofing attempts, thereby bolstering security. This degree of sophistication not only improves the integrity of biometric authentication but also fosters greater user trust in the reliability of the system (Septyanlie et al., 2024).

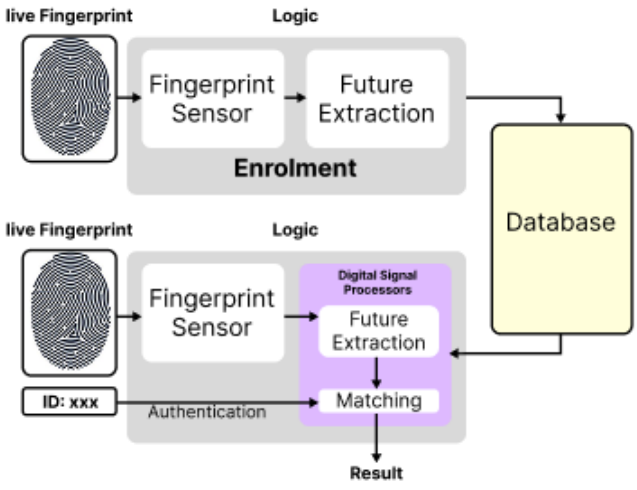

Figure 1: Integration of AI in Biometric Systems

Figure 1 illustrates the integration of artificial intelligence (AI) within biometric systems, highlighting the key components and their interactions that enhance security and user experience. The flowchart is structured to depict the following critical stages:

1. Data Collection: The process begins with the acquisition of biometric data from various sources, such as fingerprints, facial images, iris scans, and voice samples. This data serves as the foundation for the biometric system.
2. Data Preprocessing: Collected biometric data undergoes preprocessing to enhance quality and remove any noise or distortions. This step is essential for ensuring that the data is accurate and reliable for further analysis.
3. Feature Extraction: In this stage, the system extracts distinctive features from the preprocessed data. Machine learning algorithms identify unique patterns that characterize each biometric trait, which are crucial for accurate identification and verification.
4. AI Analysis: The integration primarily relies on advanced AI methods such as machine learning and deep learning. These algorithms process the extracted features, enabling the system to learn from past data and enhance its accuracy over time. This adaptive learning capability allows the system to respond effectively to changes in user behavior and environmental conditions.
5. Liveness Detection: A critical security feature, liveness detection utilizes AI to differentiate between genuine biometric traits and artificial replicas. By analyzing subtle physiological cues, the system can effectively identify spoofing attempts, thereby enhancing the integrity of biometric authentication.
6. Contextual Adaptation: AI-driven biometric systems exhibit contextual awareness by dynamically adjusting authentication parameters based on environmental factors and perceived threat levels. This adaptability ensures that security measures are appropriate for the context, providing a seamless user experience.
7. User Interaction: The final stage emphasizes the importance of user experience. The integration of AI aims to create intuitive and efficient authentication processes that minimize friction for users while maintaining robust security.

Overall, Figure 1 encapsulates the multifaceted approach to integrating AI in biometric systems, illustrating how each component contributes to enhanced security, improved accuracy, and a user-friendly experience. This integration represents a significant advancement in biometric technology, positioning it as a critical tool for secure authentication in various applications.

Moreover, AI-driven biometric systems exhibit remarkable contextual awareness, dynamically adjusting authentication parameters based on environmental factors and perceived threat levels. For instance, a system may increase its scrutiny during high-risk situations, such as accessing sensitive data in a public space, while maintaining a more relaxed approach in secure environments. This adaptability ensures a seamless user experience without compromising security, as users are less

likely to encounter unnecessary friction during authentication (Murjitama et al., 2024).

The convergence of multimodal biometrics with AI technologies represents a significant leap forward in secure authentication. By combining the strengths of various biometric modalities with the analytical power of AI, these systems offer robust protection against emerging threats while providing a user-friendly experience. As AI continues to evolve, its integration into biometric security will likely play an increasingly critical role in safeguarding sensitive information and ensuring the integrity of digital interactions (Alhamdani et al., 2022).

IV. CONCLUSION

In the rapidly evolving landscape of security technology, the imperative for robust and reliable access control systems has never been more pronounced. This study underscores the profound advantages of employing a multimodal biometric authentication system, which integrates two distinct biometric modalities specifically facial recognition and fingerprint authentication over traditional unimodal systems that rely on a single biometric input.

The inherent limitations of single-modality systems, such as susceptibility to spoofing attacks and environmental variability, can significantly undermine their effectiveness. In contrast, a dual biometric approach not only enhances the accuracy and reliability of user identification but also fortifies the system against potential vulnerabilities. By leveraging the complementary strengths of both modalities, we create a more resilient authentication framework that is capable of adapting to diverse conditions and user behaviors.

Combining multiple biometric traits improves usability by simplifying access while enhancing security. This two-factor method reduces unauthorized entry risks and boosts user trust, as their identity is protected by a smart, advanced system.

As we advance into an era where security threats are increasingly sophisticated, the adoption of multimodal biometric systems will be pivotal in redefining access control paradigms. This research advocates for a paradigm shift towards embracing the synergy of dual biometric modalities, which not only enhances the security of automatic doors but also aligns with the broader goals of creating adaptive, intelligent, and user-friendly security solutions. Ultimately, the future of access control lies in the integration of advanced technologies that prioritize both security and user experience, ensuring that our environments remain safe and accessible in an ever-changing world.

REFERENCES

[1] Mortezapour Shiri, F., Perumal, T., Mustapha, N., & Mohamed, R. (2024). A comprehensive overview and comparative analysis on deep learning models. *Journal of Artificial Intelligence*, *6*(5), 869–898. https://doi.org/10.32604/jai.2024.054314

[2] Mane, J. S., & Bhosale, S. (2023). Advancements in biometric authentication systems: A comprehensive survey on internal traits, multimodal systems, and vein pattern biometrics. *Revue d'Intelligence Artificielle*, *37*(3), 353–362. https://doi.org/10.18280/ria.370319

[3] Hassanien, A. E., Bhatnagar, R., & Darwish, A. (Eds.). (2020). *Advanced machine learning technologies and applications: Proceedings of AMLTA 2020* (Vol. 1141). Springer. https://doi.org/10.1007/978-981-15-3383-9

[4] Moi, S. H., Yong, P. Y., Hassan, R., Asmuni, H., Mohamad, R., Weng, F. C., & Kasim, S. (2022). An improved approach to iris biometric authentication performance and security with cryptography and error correction codes. *International Journal on Informatics Visualization*, *6*(4), 555–561. https://doi.org/10.30630/joiv.6.4.1046

[5] Boulkenafet, Z., Akhtar, Z., Feng, X., & Hadid, A. (2017). Face anti-spoofing in biometric systems. In R. Jiang, S. A. C. Schuckers, & A. Ross (Eds.), *Biometric Security and Privacy: Signal Processing for Security Technologies* (pp. 337–368). Springer. https://doi.org/10.1007/978-3-319-47301-7_13

[6] Alhamdani, A. A. (2023). Application of deep learning using convolutional neural network (CNN) algorithm for gesture recognition. *Journal of Electrical and Computer Engineering Education*, Universitas Pendidikan Indonesia.

[7] Ackerson, J. M., Dave, R., & Seliya, N. (2021). Applications of recurrent neural network for biometric authentication & anomaly detection. *Information*, *12*(7), 272. https://doi.org/10.3390/info12070272

[8] Liébana-Cabanillas, F., Kalinic, Z., Muñoz-Leiva, F., & Higueras-Castillo, E. (2023). Biometric m-payment systems: A multi-analytical approach to determining use intention. *Information & Management*, *61*(2), 103907. https://doi.org/10.1016/j.im.2023.103907

[9] Wadly, F. (2023). Design smart door locks with Internet of Things based on PIN security features. *International Journal of Computer Sciences and Mathematics Engineering*, *2*(2), https://ijecom.org/index.php/IJECOM/article/view/40/40 . https://www.ijecom.org. ISSN 2962-4274.

[10] Septyanlie, V., Ikawati, V., Subiyanta, E., & Lestari, N. (2024). Face recognition-based door lock security system using TensorFlow Lite. *Journal of Electrical Engineering and Computer (JEECOM)*, *6*(2). https://doi.org/10.33650/jeecom.v4i2. p-ISSN: 2715-0410; e-ISSN: 2715-6427.

[11] Permana, K. A. K., Piarsa, I. N., & Wiranatha, A. A. K. A. C. (2024). IoT-based smart door lock system with fingerprint and keypad access. *Journal of Information Systems and Informatics*, *6*(3), 2086. https://doi.org/10.51519/journalisi.v6i3.844. p-ISSN: 2656-5935; e-ISSN: 2656-4882.

[12] Jannah, N. F., Pratama, H. P., & Fuada, S. (2024). IoT-based smart door selector for double security: Integration of RFID and Blynk app for economical solution. *Eduvest – Journal of Universal Studies*, *4*(10), 8097-8102. p-ISSN: 2775-3735; e-ISSN: 2775-3727. Retrieved from https://greenpublisher.id/.

[13] Sharifani, K., & Amini, M. (2023). Machine learning and deep learning: A review of methods and applications. *World Information Technology and Engineering Journal*, *10*(07). Retrieved from https://ssrn.com/abstract=4458723.

[14] Janiesch, C., Zschech, P., & Heinrich, K. (2021). Machine learning and deep learning. *Electronic Markets*, *31*(685–695). https://doi.org/10.1007/s12525-021-00475-2

[15] Murjitama, F.L., Raihan, H.N., Adiwijaya, R.P., Ramadan, D.F., Pasaribu, B.I., Silalahi, B.A., Tasman, N.N., Dwijayanti, S.A., Panjaitan, U.P.S., & Purwanto, Y.S. (2024). Smart Door Lock Using Face Recognition Access Based on Internet of Things (IoT). *TEKNIKA*, *13*(2), 199-203. https://doi.org/10.34148/teknika.v13i2.816