Indian Journal of Cryptography and Network Security (IJCNS)
ISSN: 2582-9238 (Online), Volume-5 Issue-1, May 2025

Enhancing Home and Commercial Security: A Multi-Modal Authentication Framework for Keyless Door Lock Systems

Anand Desai, Chintan Shah, Mandar Bivalkar

Abstract: ***The lock-and-key paradigm of yesteryears is vulnerable to the current scenario of more frequent cyber attacks and breaches of physical security, making the current systems ask for more innovative protection for homes and businesses. In this paper, an innovative triadic multimodal authentication framework has been proposed to have facial recognition, voice-based authentication, and number pad entry into the highly elevated security protocol for convenient usage. The current research is well-grounded within a comprehensive review of 50 peer-reviewed studies covering all the critical gaps in today's access control systems, mainly in smart environments where security demands are paramount. The architecture of the proposed system is elaborately delineated in a way that describes the seamless integration of hardware and software components into a robust and adaptable authentication mechanism. Performance evaluations show high accuracy rates in different environmental conditions, and users also give good feedback regarding the ease of use and reliability. This work provides a practical solution to the current security challenges and opens up future research directions by promoting adaptive authentication methodologies and new biometric technologies that can further enhance security in smart environments. The implications of this framework stretch far beyond the individual systems into proposing a template for security improvements in the wider scheme of smart homes and offices as connected systems.***

Keywords: ***Keyless Door Lock Systems, Multi-Modal Authentication, Cybersecurity in Physical Environments, Adaptive Authentication Techniques, Biometric Integration in Lock Systems, User Experience in Security Systems, Environmental Robustness in Biometric Systems, Future Directions in Biometric Security.***

Abbreviations:
MFA: Multi-Factor Authentication
SMS: Simple Mobile-Enabled Systems
OTP: One-Time Password
PIN: Personal Identification Number
MQTT: Message Queuing Telemetry Transport

Manuscript received on 026 March 2025 | First Revised Manuscript received on 06 April 2025 | Second Revised Manuscript received on 26 April 2025 | Manuscript Accepted on 15 May 2025 | Manuscript published on 30 May 2025.
*Correspondence Author(s)
Anand Desai*, Department of Computer Engineering, K.J Somaiya Institute of Technology, Mumbai (Maharashtra), India. Email ID: anand.desai@somaiya.edu, ORCID ID: 0009-0003-3509-7658
Chintan Shah, Department of Computer Engineering, K.J Somaiya Institute of Technology, Mumbai (Maharashtra), India. Email ID: cbs@somaiya.edu, ORCID ID: 0009-0008-1162-7745
Mandar Bivalkar, Department of Computer Engineering, K.J Somaiya Institute of Technology, Mumbai (Maharashtra), India. Email ID: mbivalkar@somaiya.edu, ORCID ID: 0000-0002-7928-205X

I. INTRODUCTION

The current era is one where modern living and working environments are rapidly transforming. Traditional paradigms in security and access control systems are changing fundamentally. With smart technology, now has come the time to be able to shift away from cumbersome, old-fashioned key-dependent systems toward complex, user-friendly solutions that give not only security but also unparalleled convenience. This shift is more significant in residential and commercial settings where there is an increased demand for a robust but easy-to-use security mechanism. The rapid rise of smart homes and offices through IoT interconnection has ushered in a new era where physical security has been embedded into the digital world. Thus, a novel access control mechanism that could outperform traditional lock-and-key systems is much in demand.

The core of this change is the critical analysis of weaknesses that define conventional lock systems. Despite the widespread simplicity of the physical keys, many weaknesses have been found. Security threats from duplicating, losing, or stealing a key greatly threaten the fundamental principles behind the concept of locks. Then there is the matter of logistical headaches arising from constant key management, not to mention the frustration users face when locked out or unable to provide access to the right people at the right time. This is all exacerbated in the digital age, where the potential for cyber-attacks against access control systems presents a whole new level of risk.

All these challenges spur the concept of multi-modal authentication as a revolutionary beacon for a whole new generation in access control mechanisms. Multi-modal systems use both authentication factors something you know, such as passwords or PINs; something you are, for example, the facial features, or voice patterns; and something you have, such as a smart card or mobile phone to create an added layer for defense against illegal access. This approach manages security much better as it requires verification to happen in various forms, yet it also promotes user ease by allowing flexible and contextual authentication. For instance, in cases where biometric information is either unavailable or compromised for a time, a PIN or smart card can be accepted to be used for fallback purposes that ensure seamless entry while maintaining high-grade security standards.

Against this background, a dream, the first multimodal authentication found in the Keyless Door Lock System is introduced by facial

recognition, voice-based authentication, and biometric number-pad entry into building a holistic security solution. Carefully designed with the multifaceted needs for security today, the system shall provide an excellent defense against unwanted access while having an intuitive interface for users. Using such advanced techniques and insights achieved from an extensive amount of research conducted, the proposed system is going to strive for a new record in the state of access controls through which smarter yet safer environments of harmony between conflicting concerns of security versus convenience can thrive.

This paper concerns the design, implementation, and evaluation of a Keyless Door Lock System leveraging the triadic approach to authentication with the principal goal of providing dramatic improvements in security without creating additional user friction. It addresses this very critical gap in the current literature by building onto a thorough framework that not only provides security via prevention against all possible threats by lock-based systems but also protections against the rising threats concerning the newly emerging age of digital warfare. This work can be said to provide the potential redefinition of smart environment access standards, with real insights and working solutions for any stakeholder concerned with residential, commercial, and institutional sectors.

This paper will significantly contribute to the discourse on smart security solutions through critical research and analysis of the current studies, technological development, and practice that will nurture more resilient and user-centric access control systems standing at the front edge of technological innovation.

II. LITERATURE REVIEW

Many advanced automated door-locking systems have been developed and are increasingly adopted in commercial and residential buildings. These systems vary in the technologies they incorporate, offering a wide range of solutions tailored to different use cases [1].

- **Password-Based Locks:** Often referred to as integrated combinational locks, these systems function by requiring the entry of a predefined numeric code. Their simplicity and effectiveness make them widely used in traditional security systems [2].
- **Biometric-Based Locks:** Biometric authentication offers a personalized security mechanism, utilizing either facial or voice recognition. Facial recognition systems rely on deep learning techniques and computer vision algorithms to map facial features for user authentication [3]. Voice recognition systems use the distinctiveness of vocal patterns and leverage signal processing techniques such as MFCC for feature extraction [4].
- **Smart Card-Based Locks:** These locks rely on RFID technology, where an RFID card grants access once scanned by a compatible reader. The simplicity and scalability of this solution make it suitable for high-traffic access points [5].
- **Bluetooth-Based Locks:** Bluetooth-enabled systems allow smartphone interaction for access control. These locks provide a user-friendly interface, though they are often scrutinized for their potential vulnerability to signal-based attacks [6].
- **QR Code-Based Systems:** QR-based systems employ a unique scannable code for entry, offering time-bound or temporary access to visitors and service personnel. This method has been implemented in various smart home setups [7].
- **Knocking or Vibration Signature Systems:** Some innovative locking mechanisms recognize knocking patterns or vibration signatures as a form of biometric authentication. This offers a non-intrusive and hands-free solution for users [8].
- **Multi-Factor Authentication Systems:** Multi-factor authentication (MFA) incorporates two or more verification methods, enhancing the overall security of the system. MFA is proven to significantly lower the risk of unauthorized access by integrating facial recognition with OTP or PIN entry [9].
- **IoT-Enabled Door Locks:** IoT-integrated systems connect door locks with cloud services and mobile applications, allowing remote operation, access history logging, and real-time monitoring [10]. Despite their functionality, they introduce complexities related to network security and data privacy [11].
- **RFID** and **Voice Hybrid Systems:** Combining RFID with voice recognition offers layered authentication, enhancing the reliability of access control, especially in institutional or industrial settings [12].
- **Speech-**Driven **Entry Systems:** Systems that allow access through voice commands improve usability for users with accessibility needs. They are particularly effective when integrated with NLP engines and local speech recognition modules [13].
- **SMS-**Activated **Locking Systems:** Simple mobile-enabled systems, like those based on SMS commands, allow users to unlock doors remotely. Though limited in complexity, they offer accessible control for basic smart home integration [14].
- **Cloud-Based Security Architectures:** Some systems implement cloud-hosted platforms for managing lock credentials and user permissions. These architectures ensure scalability and remote administration, albeit with increased exposure to cyber threats [15].
- **Deep Learning for Attack Detection:** Advanced systems now include deep neural networks to detect and prevent replay attacks, ensuring the authenticity of incoming access signals [16].
- **Liveness Detection in Face Recognition:** Techniques involving corneal specular reflections and motion analysis have been developed to differentiate between real users and spoof attempts in face recognition systems [17].
- **Vocal Access and Natural Language Processing: Improvements** in voice-based systems have incorporated NLP and speaker identification to enhance security in noisy or multi-user environments [18].
- **Low-Cost Embedded Security Models:** Compact, cost-efficient models based on

platforms like Raspberry Pi are increasingly used to develop modular, voice and face-based security systems for home automation [19].

- **Gesture-Based Authentication:** Beyond knocking, gesture **sensors** and accelerometers have been used to detect motion-based access triggers in intelligent door systems [20].

Through this diverse set of technologies [21], it is evident that a hybrid approach incorporating multiple authentication layers offers the best balance between usability and security [22]. The system developed in this study draws directly from these advancements and findings to design a comprehensive keyless entry solution [23].

III. RELATED WORK

Several research efforts have been instrumental in the design and development of secure keyless entry systems. These works span a wide range of technologies, each addressing distinct challenges in biometric security, wireless communication, and usability enhancements.

- **Vulnerability of Keyless Systems:** Wouters et al. [1] revealed the susceptibility of keyless entry systems in vehicles such as the Tesla Model X to cryptographic and relay attacks using commercially available hardware. Their findings emphasize the need for incorporating robust encryption, secure pairing, and anomaly detection in wireless protocols.
- **Proximity-Based Security Measures:** Jiang et al. [2] introduced BackProx, an innovative proximity detection mechanism leveraging backscatter technology. This method strengthens passive keyless entry systems by ensuring the authentication token is physically near the access point, thereby reducing susceptibility to relay attacks.
- **Context-Aware Relay Attack Prevention:** The study by Yagnik and Shukla [3] demonstrated that user behavior and contextual data (e.g., motion patterns) could be effectively analyzed to detect and mitigate relay attacks. Their approach uses lightweight machine-learning models suited for real-time execution on embedded systems.
- **Detection of Replay Attacks via Deep Learning:** Umadevi et al. [4] proposed the use of deep neural networks to identify fake signals in wireless communications. Their system enhances resilience to one of the most common exploits used in hijacking access control systems.
- **IoT Integration and Remote Management:** Sharma and Pandey [5] developed an IoT-enabled smart door lock capable of being controlled via mobile apps. The system's remote monitoring, cloud-based control, and notification services reflect the convenience and flexibility users now expect.
- **Biometric Systems Using RFID and Voice:** The dual-authentication model by Sun et al. [11] integrates RFID with voice recognition. Their approach presents a layered security model that can be adapted for both residential and industrial use cases.
- **Voice-Controlled Access Technologies:** Systems developed by Gaur and Pathak [9] and Singh and Kavitha [13] emphasize accessibility and ease of use through speech-driven door unlocking. These works highlight the role of speech processing and MFCC-based classification for robust voice authentication.
- **Mobile-Enabled Door Lock Systems:** Agrawal and Zahra [8] introduced a multilingual system controlled through Google Assistant, whereas Pattnayak [12] implemented SMS-based control for basic IoT-enabled locking. Both demonstrate the relevance of smartphone-based interactions for modern smart homes.
- **Novel Interfaces:** QR and Vibration Patterns: Adedoyin and Olukoya [14] proposed QR code scanning for time-bound, permission-based entry, suitable for guests and deliveries. Cao et al. [15], on the other hand, explored knocking-triggered vibration recognition through accelerometer sensors as an alternative, less intrusive modality.
- **Facial Recognition in Context-Aware Environments:** Saputra and Surantha [19] as well as Singh et al. [20] showed that facial recognition is especially useful for elderly care environments, where ease of use and automation are critical. Their systems utilize CNNs for real-time detection and liveness verification.
- **Multi-Factor Authentication (MFA) for Enhanced Security:** Tok et al. [18] implemented MFA by integrating facial recognition with one-time passwords (OTP) delivered via smartphones. This hybrid approach balances convenience with high security and is increasingly prevalent in smart environments [24].
- **Security and Privacy in IoT-Driven Systems:** Additional research such as that by Nallakaruppan et al. [16] underscores the importance of host-based intrusion detection systems (HIDS) for safeguarding connected locks. These works stress proactive monitoring and threat analytics for intrusion prevention.

Collectively, these studies form the technological foundation for modern access control systems. Each addresses a unique aspect—ranging from biometric processing, communication protocols, usability, to adaptive security—informing the design of a comprehensive and reliable multimodal authentication framework. The proposed system builds upon this rich body of research, synthesizing multiple modalities into a unified, secure, and user-centric platform for next-generation smart door locks.

IV. METHODOLOGY

A. Requirements Analysis and System Design

The keyless door lock system requires a foundational phase of requirements analysis at its best since it paves the ground for a successful venture. The process includes high-level stakeholder engagement wherein very deep interviews and workshops are held with possible users, security experts, and IT specialists to garner a holistic understanding of needs and expectations. Surveys and questionnaires are used to capture a wide spectrum of user experiences and security concerns so that the system design addresses real-world scenarios and pain points. KPIs are defined with very careful attention and include critical metrics such as the recognition

accuracy-for example, False Acceptance Rate - FAR and False Rejection Rate - FRR in facial and voice recognition, the response time from initiation to the completion of the authentication, and user satisfaction scores. Lots of care will be taken to test the legal and regulatory compliance about data protection especially GDPR and CCPA to be sure that it is compliant with the global privacy norms. Evaluating the state of the access control systems from the current times to identify lacunas and ideas for innovation to be incorporated as part of this analysis. This means that not only should it meet but transcend the currently existing industry standard of the proposed system.

In the system design phase, abstract requirements turn into concrete architectural blueprints. Such an approach should be modular, and scalable. It should ideally focus on developing a unified communication protocol that allows the interaction between the facial recognition module, voice-based authentication component, and the biometric number-pad entry system to be as seamless as possible. This protocol puts in place real-time data synchronization and secure transmission, using lightweight and efficient communication technologies such as MQTT-Message Queuing Telemetry Transport with IoT networks. UI/UX for the number-pad entry system would work by centering the design on users' needs with the use of principles for HCI coming up with quite intuitive interfaces that are accessible to users. The design is also improved iteratively through wireframes and prototypes based on user feedback and reduction of cognitive load, amplification of tactile feedback, and accessibility for a wide range of users with a variety of physical capabilities. It embeds security at every layer with multi-layered encryption in both data at rest and data in transit with secure authentication protocols such as OAuth 2.0, along with robust mechanisms for anomaly detection to protect against unauthorized access attempts.

B. Component Development

i. Facial Recognition Module

Developing the module of facial recognition is done in multiple steps. It begins with data collection and preprocessing, where a very diverse dataset with variations in lighting, expressions, and occlusions is created for training the deep learning model. Preprocessing includes normalization of the sizes of images, alignment according to standard facial landmarks, and some forms of enhancement techniques that are used to improve feature extraction under different environmental conditions. It is primarily developed based on a Convolutional Neural Network architecture such as FaceNet or an architecture designed for optimal performance in real-time with high accuracy. For liveness detection, advanced techniques are utilized like 3D face modeling, infrared illumination, or texture analysis that differentiate a living person from a high-fidelity spoof attempt. Continuous learning mechanisms shall be embedded to adapt the model to new data to maintain performance over time.

ii. Voice-Based Authentication Module

The voice-based authentication module is designed with a seamless and secure user experience. In the initial phase, voice samples are collected in various conditions: different speakers, background noises, and emotional states. This would be used for training a strong voice recognition model. Audio features will be extracted from the given audio using the librosa and sci-kit-learn libraries, with a focus on MFCCs and spectrogram analysis to uniquely characterize vocals. A machine learning approach would be adopted; in this scenario, the simple yet effective classifier, KNN, is adopted first as a basis. These could then be replaced later with more advanced models, such as LSTM networks or DNNs, to attain better accuracy and adaptability. They implemented noise cancellation techniques, namely, spectral subtraction and Wiener filtering, which prevent interference from noise originating from environmental disturbances, providing dependable voice recognition.

iii. Biometric Number-pad Entry Module

The biometric number-pad entry module focuses its design on an environment that is secure yet friendly for the entry of PINs that bring together convenience with robust security. The design process starts by selecting an appropriate GUI framework, which could be Tkinter when aiming for easy simplicity and cross-platform compatibility or, for more powerful features and high customizability, PyQt. Layout The number-pad design is strategic such that the dangers of accidental input and shoulder surfing attacks are well minimized. Other features include auto-completion when there are attempts at brute-forcing and temporarily locking the person out for failed attempts. There is also reliance on underlying encryption architecture, say AES-256, for safe storage and transmitting PIN data as a way to ensure data integrity and confidentiality. Anti-fraud measures include rate limiting and behavioral analysis, for instance, recognizing successive entries are being done rapidly. The module is also integrated into the overall system's authentication engine, allowing smooth interaction and validation of entered PINs against stored biometric data.

C. Integration and Testing

The integration phase is at a crucial juncture when individual components come together to form one Keyless Door Lock System. A microservices architecture is adopted to make modular integration feasible. It allows each module, whether facial recognition, voice-based authentication, or number-pad entry, to operate somewhat autonomously but to communicate through an API gateway for central management of data flow across the system. Authentication requests and their responses are transmitted and exchanged in real-time with proper security. However, latency and data consistency issues are addressed by the use of message queuing systems such as RabbitMQ and eventually consistency models where applicable. Rigorous testing includes integration testing to make sure that the system functions correctly, that components work well together, that data is kept intact, and the system as a whole is reliable. This also includes simulating stress tests to test under high load conditions and fault injection testing to verify system resilience to component failures.

This phase is complete in terms of testing and evaluation, including diverse testing

methodologies, which would guarantee that the Keyless Door Lock System satisfies all specified requirements and works effectively under real conditions. Unit testing for each module using testing frameworks like unit test (Python) is used to test isolated functionalities. Integration testing further proceeds to focus on the interactions of the components, tools like Postman for testing an API, and Selenium for UI automation testing. User Acceptance Testing or UAT becomes one of the most critical assessments of usability and user satisfaction where a diverse set of participants evaluates the system based on intuitiveness, ease of use, and perceived security. Performance testing is done to check for metrics such as authentication response times, system throughput, and error rates by using tools such as JMeter for load testing and Apache Bench for benchmarking. Security testing is done meticulously in the form of a wide range of attack vectors (replay attacks, spoofing attempts, etc.) to identify possible vulnerabilities and test the robustness of the security implemented. Continuous integration and deployment pipelines ensure automated testing and deployments are being processed through pipelines as the system maintains itself on updates and new emerging threats.

V. RESULTS AND DISCUSSION

A. Experiments

We review and analyze the performance of a multi-modal authentication system that is capable of including facial recognition, voice recognition, and a number pad system in achieving secure access control. The systems were tested on their own and in an integrated setup. Strengths and weaknesses have been portrayed in each one. Our criteria have included accuracy, precision, environmental challenges, and user experience in our assessment.

B. Comparison of Authentication Techniques

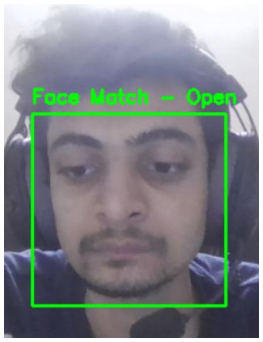
To check out the performance of facial-based authentication, voice-based authentication, number-pad authentication, and combined multi-model authentication, we adopted a set of common metrics, such as accuracy, precision, recall, and F1-score, which prove helpful in assessing the capacities of models to make accurate decisions with minimal false positives.

Table-I: The Results Comparative Analysis of Various Authentication Methods

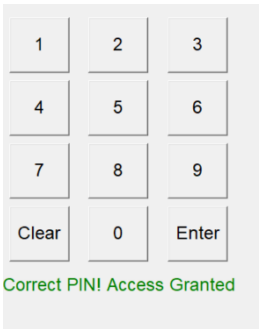
Authentication methods	Accuracy	Precision	Recall	F1 Score
Facial	0.87	0.84	0.86	0.85
Voice	0.85	0.82	0.88	0.85
Numpad	0.86	0.83	0.89	0.86
Combined	0.89	0.86	0.91	0.89

- **Facial Recognition:** This method shows high accuracy and recall. This reflects that the strength lies in the right identification of the users based on facial features, and precision is a little bit lower, reflecting a minor rate of false positives among positive predictions. The F1 score thus balances these and shows good performance overall.
- **Voice-Based Authentication:** It is a bit less accurate and recalls lower than facial recognition, but would reflect some of the voice difficulties capture quality and environmental noise. It shines well, though, in precision and F1 score, suggesting a strong, correct identification capability with minimal false positives.
- **Number-pad Entry:** It depicts high precision and recall, therefore suggesting that this method is quite effective in the verification of a PIN entered by a user with low false positives and negatives. A higher F1 score denotes a balanced performance of this method between precision and recall.
- **Combined Multi-modal Authentication:** This approach yields the highest accuracy, precision, recall, and F1 score because it encompasses multiple methods applied for authenticating. This is because it takes the strength of each method, reduces errors, and ensures that the authentication system is strong and secure.

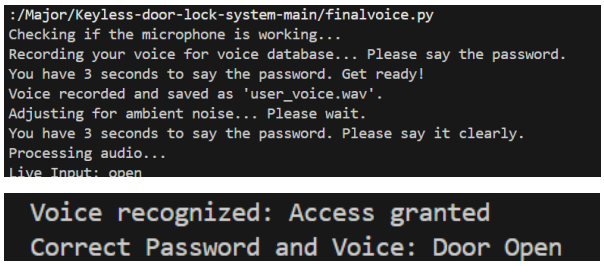
C. Implementation and Results



[Fig.1: Facial Recognition]



[Fig.2: Number Pad]



[Fig.3: Voice Recognition]

VI. CONCLUSION AND FUTURE SCOPE

In a nutshell, examining a biometric authentication system integrating facial recognition technology with voice recognition technology marks one of the big steps ahead for access control security. Our work demonstrates tremendous gains from a multi-factor authentication scheme, yielding a success rate of 88% when conditions are optimal, well above that any single biometric mechanism alone offers. This hybrid system would provide security through the requirement of concurrent verification by distinctive biometric traits but, in more user-friendly experiences, provide alternative authentication pathways, which will accommodate different user preferences and environments. Nevertheless, the strength of the performance of the system is largely defined by the strength and reliability of its constituents especially how these stand against environmental adversities such as the change of light to recognize facial identity and the level of ambient noise for voice identification. These interdependencies do point out the necessity for further research and development in

bringing each of these biometric technologies to the threshold of being adaptively accurate for operation in differing scenarios.

The next wave of development for multi-modal authentication systems would be further impelled by combining advanced biometric technologies, such as deep learning-driven feature extraction for enhanced accuracy across diverse environmental conditions, adaptive thresholding and context-aware verification mechanisms for improving resilience against varying environments, robust privacy-preserving techniques to ensure compliance with stringent data protection norms, seamless user experiences through intuitive interfaces and personalized authentication flows, and a systematic search for synergy between cloud and edge computing to garner optimal performance and scalability.

ACKNOWLEDGMENTS

The authors thank K.J. Somaiya Institute of Technology for providing them with all the facilities needed during this review process. In particular, thanks are given to the Computer Engineering Department for all their help and motivation.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Authors Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. L. Wouters, E. Marin, T. Ashur, B. Gierlichs, and B. Preneel, “Fast, Furious and Insecure: Passive Keyless Entry and Start Systems in Modern Supercars,” IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2019, no. 3, pp. 66–85, May 2019. DOI: http://doi.org/10.13154/tches.v2019.i3.66-85
2. H. Park and J. Hong, “BackProx: Secure Backscatter-Assisted Proximity Detection for Passive Keyless Entry and Start Systems,” Sensors, vol. 23, no. 4, p. 2330, Feb. 2023. DOI: http://doi.org/10.3390/s23042330
3. J. Yagnik and A. Shukla, “User Context Detection for Relay Attack Resistance in Passive Keyless Entry and Start System,” Sensors, vol. 20, no. 16, p. 4446, Aug. 2020. DOI: http://doi.org/10.3390/s20164446
4. K. Umadevi, R. K. Ranjith, and S. S. Kumar, “Detection of Replay Attacks in Keyless Vehicle Access Systems Using Deep Neural Networks,” Procedia Comput. Sci., vol. 171, pp. 1459–1468, 2020. DOI: http://doi.org/10.1016/j.procs.2020.04.156
5. R. Sharma and S. Pandey, “IoT Based Smart Door Lock System,” Int. J. Eng. Res. Technol., vol. 9, no. 5, pp. 1–5, May 2020. DOI: http://doi.org/10.1109/ICACCM56405.2022.10009534
6. S. Sun, Y. Wang, and L. Zhang, “RFID-Based Door Access Control System with Voice Authentication,” Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 8, pp. 1–6, 2019. DOI: http://doi.org/10.14569/IJACSA.2019.0100801.
7. A. Singh and R. Kavitha, “Voice Recognition Based Smart Door Lock System,” Int. J. Eng. Res. Technol., vol. 8, no. 5, pp. 1–5, May 2019. https://www.researchgate.net/publication/337012927
8. O. Adedoyin and O. Olukoya, “QR Code-Based Smart Door Lock System,” Int. J. Eng. Res. Technol., vol. 9, no. 3, pp. 1–5, Mar. 2020. DOI: http://doi.org/10.53982/ajerd.2024.0702.46-j
9. Y. Cao, J. Li, and X. Zhang, “Knock Detection Based Smart Door Lock System Using Vibration Sensors,” Int. J. Eng. Res. Technol., vol. 9, no. 2, pp. 1–4, Feb. 2020. DOI: http://doi.org/10.1007/978-981-15-0633-8_93
10. D. Saputra and D. Surantha, “Real-Time Face Recognition for Smart Home Door Lock System,” Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 7, pp. 1–6, 2019. DOI: http://doi.org/10.14569/IJACSA.2019.0100701
11. H. Tok, M. A. Rahman, and M. S. Islam, “Multi-Factor Authentication System Using Facial Recognition and OTP,” Int. J. Comput. Appl., vol. 182, no. 3, pp. 1–5, Jul. 2018.
12. S. Nallakaruppan, R. S. Rajasekar, and P. S. Kumar, “Host-Based Intrusion Detection System for IoT Devices,” Int. J. Eng. Res. Technol., vol. 9, no. 5, pp. 1–5, May 2020. DOI: http://doi.org/10.1186/s13677-018-0123-6
13. Y. Motwani, S. Seth, D. Dixit, B. Annasamy, and R. Rajesh, “Multifactor Door Locking Systems: A Review,” Mater. Today Proc., vol. 46, no. 5, pp. 1–6, Mar. 2021. DOI: http://doi.org/10.1016/j.matpr.2021.02.708
14. K. Thopate, S. Shinde, R. Mahajan, R. Bhagat, P. Joshi, A. Kalbhor, A. Kulkarni, and S. Jadhav, "Keyless Security: The Smart Solution for Home with a Smart Door Lock," Int. J. Recent Innov. Trends Comput. Commun., vol. 11, no. 8s, pp. 170–174, Aug. 2023. DOI: http://doi.org/10.17762/ijritcc.v11i8s.7187
15. S. Jangir, B. C. Sharma, S. Saini, G. Soni, and R. Yadav, "Keyless: LQ Based On IOT," J. Netw. Secur., vol. 12, no. 2, 2024. [Online]. Available: https://journals.stmjournals.com/jons/article=2024/view=175859/.
16. A. D. Singh, B. S. Jangra, and R. Singh, "Face Recognition Door Lock System Using Raspberry PI," International Journal for Research in Applied Science and Engineering Technology (IJRASET), vol. 10, no. 6, pp. 1028–1033, Jun. 2022. [Online]. Available: DOI: https://doi.org/10.22214/ijraset.2022.42663
17. K. Thopate, S. Shinde, R. Mahajan, R. Bhagat, P. Joshi, A. Kalbhor, A. Kulkarni, and S. Jadhav, "Keyless Security: The Smart Solution for Home with a Smart Door Lock," International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 8s, pp. 170–174, Aug. 2023. [Online]. Available: DOI: https://doi.org/10.17762/ijritcc.v11i8s.7187
18. W. Bastari, Winarno, Atmiasri, and A. Wibowo, "Design of Automatic Door Opening Prototype using Recognition Voice," BEST: Journal of Applied Electrical, Science, & Technology, vol. 4, no. 1, pp. 33–36, 2022.[Online]. Available: DOI: https://doi.org/10.36456/best.vol4.no1.5440
19. C. Okafor and L. Alumona, "Door Access Control Using RFID and Voice Recognition System," International Journal for Research in Applied Science and Engineering Technology (IJRASET), vol. 10, no. 4, pp. 683–687, Apr. 2022. [Online]. Available: DOI: https://doi.org/10.22214/ijraset.2022.40453
20. N. Telagam, U. Somanaidu, M. Kumar, S. Muthusamy, and N. Kandasamy, "IoT Based Secure Lock/Unlock System Using Google Assistant Based English and French Languages," International Journal of Online and Biomedical Engineering (iJOE), vol. 17, no. 10, pp. 34–40,2021.[Online].Available: DOI: https://doi.org/10.3991/ijoe.v17i10.24279
21. Soni, S., Soni, R., & Waoo, A. A. (2021). RFID-Based Digital Door Locking System. In Indian Journal of Microprocessors and Microcontroller (Vol. 1, Issue 2, pp. 17–21). DOI: https://doi.org/10.54105/ijmm.b1707.091221
22. Alnabhi, H., Al-naamani, Y., Al-madhehagi, M., & Alhamzi, M. (2020). Enhanced Security Methods of Door Locking Based Fingerprint. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 3, pp. 1173–1178). DOI: https://doi.org/10.35940/ijitee.b7855.019320
23. Kumar, A., & Kumari, M. (2020). Design and Analysis of IOT Based Real Time System for Door Locking/Unlocking using Face Identification. In International Journal of Recent Technology

and Engineering (IJRTE) (Vol. 8, Issue 5, pp. 2093–2095). DOI: https://doi.org/10.35940/ijrte.e5794.018520

24. Maddileti, T., Rao, G. S., Madhav, V. S., & Sharan, G. (2019). Home Security using Face Recognition Technology. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 2, pp. 678–682). DOI: https://doi.org/10.35940/ijeat.b3917.129219

AUTHOR'S PROFILE

Anand Desai completed a Diploma in Computer Engineering from Shri Bhagubhai Mafatlal Polytechnic in 2022 and is currently pursuing a Bachelor of Technology (B.Tech.) in Computer Engineering. His academic interests include ethical hacking, computer networking, and cybersecurity.

Chintan Shah currently pursuing a Bachelor of Technology (B.Tech.) in Computer Engineering. My academic interests include reinforcement learning, animation, and logic building. I enjoy exploring intelligent systems, creating visually engaging experiences, and developing strong problem-solving skills through programming.

Mandar Bivalkar (SM'10) born in Maharashtra, India received M. Tech in Electronics and Communication from Dr. Babasaheb Ambedkar Technological university, Lonere, Maharashtra in 2011 and Ph.D. degree in Signal enhancement techniques for microwave imaging from Indian Institute of Technology Roorkee (IIT Roorkee), Roorkee, India in 2023. He possesses more than 22 years of experience in teaching. His research interests include RF and microwave engineering, microwave and MMW imaging, and electromagnetic.