IAES Journal of Electrical and Electronics Engineering
Vol. 8, No. 1, June 2021, pp. 1~5
ISSN: 2338-7432, DOI: 10.11591/jeee.v8i1.pp1-5

Electronic door lock systems: technologies, architectures, authentication methods, and security challenges-a review

Tole Sutikno[1], Sarif Syahrudin[1], Watra Arsadiando[2]
[1]Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Embedded Systems and Power Electronics Research Group, Yogyakarta, Indonesia

Article Info

Article history:

Received May 20, 2019
Revised Jan 30, 2020
Accepted May 7, 2020

Keywords:

Access control
Biometric authentication
Electronic door lock
Internet of things
RFID
Smart lock

ABSTRACT

Electronic door locks have become an important alternative to conventional mechanical locking systems because they provide flexible access management, improved monitoring, and integration with modern security technologies. However, their effectiveness depends not only on the locking mechanism but also on authentication reliability, electronic control, communication security, and power availability. This review examines the development and technical characteristics of electronic door lock systems, emphasizing their applications in residential, commercial, and institutional environments. The discussion covers the principal system architecture, including electronic controllers, sensors, actuators, and credential management components. Major authentication technologies, such as personal identification numbers, radio-frequency identification (RFID), Bluetooth, fingerprint recognition, and mobile-based access, are compared in terms of usability, implementation complexity, and security limitations. Particular attention is given to credential cloning, replay attacks, biometric spoofing, unauthorized wireless access, and system failures. The review also considers the integration of electronic locks into Internet of Things environments and the resulting cybersecurity requirements. The findings indicate that reliable electronic door locks require layered authentication, secure communication, robust mechanical design, and appropriate emergency provisions. These considerations provide a foundation for developing more dependable, accessible, and secure electronic access control systems.

This is an open access article under the CC BY-SA license.

1. INTRODUCTION

Door locking systems are fundamental components of building security because they regulate access to private, commercial, and institutional spaces. Conventional mechanical locks provide a relatively simple means of protection, but their dependence on physical keys creates several operational limitations. Keys can be lost, duplicated, stolen, or transferred without authorization, while conventional systems generally provide limited information about access activities. These limitations have encouraged the development of electronic door locks that use digital credentials and electrically controlled locking mechanisms [1], [2].

Electronic door locks replace or supplement conventional keys with electronic identification and authorization methods. Their operation commonly involves a credential reader, a control unit, an authentication mechanism, and an electromechanical actuator. Depending on the design, users may enter a personal identification number, present a radio frequency identification (RFID) card, use a fingerprint, or communicate through a mobile device. Previous studies have demonstrated the feasibility of combining these technologies with microcontrollers and mobile applications for automated access management [3]–[6].

Despite these developments, electronic locking systems introduce technical problems that cannot be solved simply by replacing mechanical keys with digital credentials. Unauthorized access may occur through weak passwords, cloned RFID credentials, insecure wireless communication, or manipulated biometric inputs. Network-connected locks also depend on software, communication infrastructure, and power sources

that may introduce additional failure points [7], [8]. Therefore, this review examines electronic door lock technologies, their system architectures, authentication methods, security challenges, and development requirements.

2. RESEARCH PROBLEMS AND REVIEW SCOPE

The central research problem concerns how electronic door locks can provide convenient access while maintaining reliable physical and digital security. A system that offers multiple unlocking methods may improve usability, but additional interfaces can also increase the number of potential attack points. Similarly, remote access and monitoring can improve management but create dependence on communication networks and software services. Consequently, electronic door lock performance must be evaluated through security, reliability, usability, and operational continuity rather than authentication convenience alone [9], [10].

This review focuses on electronic door locks implemented using embedded controllers, electronic identification technologies, biometric sensors, and wireless communication. The discussion draws on research concerning RFID authentication, fingerprint security, smart-home access control, and Internet of Things security published no later than 2019. These related research areas are included because electronic door locks share their principal technical components and security requirements. The review is intended to connect existing technological approaches with the engineering challenges that must be addressed in practical access control applications.

3. ARCHITECTURE AND OPERATING PRINCIPLES

An electronic door lock generally consists of an input interface, a processing unit, an actuator, and a power supply. The input interface receives identification information from a keypad, RFID reader, fingerprint sensor, or wireless device. A microcontroller or embedded processor evaluates the received information against stored credentials or an authorized database. If authentication succeeds, the controller activates an actuator to release the locking mechanism for a predefined period [3], [4].

The actuator determines how electronic authorization is translated into physical door movement. Common mechanisms include solenoid locks, electromagnetic locks, motor-driven deadbolts, and electric strikes. Solenoid-based systems provide direct electromechanical movement, whereas motorized mechanisms can support more complex locking operations. The selection of an actuator must consider door construction, required holding force, operating speed, energy consumption, installation requirements, and the consequences of power interruption.

Power management is another important component of electronic door lock architecture. Battery-powered systems can operate independently of building electrical infrastructure, but they require monitoring of battery condition and replacement schedules. Wired systems may provide continuous power but need protection against supply interruption and electrical faults. Emergency mechanical access, backup batteries, and clearly defined fail-safe or fail-secure behavior are therefore important design considerations, particularly in buildings where access and evacuation requirements must be maintained.

4. ELECTRONIC AUTHENTICATION TECHNOLOGIES

4.1. Password and keypad authentication

Keypad authentication allows authorized users to unlock a door by entering a predefined numerical code. This approach is relatively inexpensive and straightforward to implement using a microcontroller, keypad module, and electronic actuator. It also avoids the need for physical cards or specialized biometric sensors. However, weak codes, repeated password use, observation during entry, and inadequate protection against repeated attempts can reduce its security [10].

A more reliable keypad implementation should include password length requirements, temporary lockout after repeated failures, and secure storage of authentication data. Password changes and user-specific access codes can improve administrative flexibility. Nevertheless, PIN-based authentication remains dependent on the confidentiality of the code and the user's ability to protect it. Combining a keypad with another independent authentication factor can reduce the consequences of a compromised password.

4.2. Radio-frequency identification

RFID is widely used in electronic access control because it enables contactless identification through a reader and an electronic tag or card. An RFID system typically consists of a tag, reader, controller, and credential database. When a user presents an authorized tag, the reader obtains its identification data and

forwards it to the controller for verification. Its convenience and relatively simple integration have made RFID suitable for laboratories, offices, educational institutions, and residential buildings [3], [11].

However, RFID security depends strongly on the authentication protocol and the type of tag employed. Basic systems that rely only on a static identifier may be vulnerable to credential copying, cloning, eavesdropping, and replay attacks. Research on RFID security has therefore emphasized mutual authentication, confidentiality, privacy protection, and resistance to cloning [1], [12], [13]. For electronic door locks, cryptographic authentication and secure credential management are preferable to systems that accept a fixed identification number without further verification.

4.3. Bluetooth and mobile-based authentication

Bluetooth-enabled electronic locks allow users to interact with the locking system through smartphones or other wireless devices. A mobile application can transmit authentication information, manage access permissions, and provide information about locking events. Bluetooth communication is particularly attractive for short-range applications because it can provide convenient connectivity without requiring a permanent Internet connection. Keyless smart-home prototypes have demonstrated the feasibility of combining Bluetooth communication with security codes and predefined user credentials [5].

Nevertheless, wireless communication introduces additional security requirements. Pairing procedures, device authentication, encryption, and protection against unauthorized connection attempts must be carefully implemented. Research on Bluetooth secure pairing has examined authenticated link-key establishment and its implications for home automation applications [14]. A mobile-based lock should also address lost or stolen smartphones, revoked credentials, software updates, and the possibility of unauthorized access through compromised applications.

4.4. Biometric authentication

Biometric authentication identifies users through physiological or behavioral characteristics, including fingerprints, facial features, and voice patterns. Fingerprint recognition is particularly relevant to electronic door locks because compact fingerprint sensors can be integrated into embedded control systems. The system captures a fingerprint sample and compares its extracted features with previously registered templates. This approach reduces dependence on physical cards and memorized passwords, although recognition accuracy and sensor quality influence practical performance [15], [16].

Biometric systems are not automatically secure merely because they use unique human characteristics. Artificial fingerprints, presentation attacks, poor sensor conditions, and compromised biometric templates can undermine authentication reliability. Studies on fingerprint anti-spoofing have examined methods for detecting artificial samples and improving liveness assessment [17]. Biometric templates should therefore be protected through secure storage, access restrictions, and appropriate anti-spoofing techniques, while alternative authentication methods should remain available for users whose biometric samples cannot be reliably recognized.

5. INTEGRATION WITH SMART HOMES AND IOT

The integration of electronic door locks with smart-home platforms extends their functionality beyond local access authorization. Network connectivity enables remote locking, access notifications, event logging, and centralized user management. RFID readers, mobile applications, sensors, and embedded controllers can operate as components of a wider home automation environment. Such integration can improve convenience and monitoring, but it also makes the lock dependent on the security of interconnected devices and communication services [6], [7].

IoT-based access control requires attention to device identity, authorization policies, communication confidentiality, and software integrity. A compromised mobile application or network service may affect the operation of a connected lock even when its physical actuator remains functional. Research on IoT security has identified authentication, privacy, availability, and secure communication as important challenges across interconnected devices [8], [18]. Accordingly, electronic door locks should retain essential local access functions when Internet connectivity is unavailable and should not rely exclusively on cloud-based authorization.

6. SECURITY CHALLENGES AND RELIABILITY ISSUES

Electronic door locks face threats at several levels, including physical components, authentication interfaces, communication channels, and software applications. Physical attacks may involve damage to the reader, actuator, wiring, or power supply. Digital attacks may include credential cloning, replay, impersonation, unauthorized application access, and manipulation of stored authorization data. RFID and IoT

security research demonstrate that weak authentication and inadequate communication protection can compromise the overall system [1], [8], [12].

Reliability is equally important because an electronic lock must operate consistently under different environmental and electrical conditions. Sensor errors, electromagnetic interference, mechanical misalignment, battery depletion, and software faults may prevent legitimate users from entering or cause unintended unlocking. A robust design should therefore include diagnostic functions, event logging, actuator status monitoring, and suitable backup power arrangements. System testing should evaluate both successful access and failure conditions, including repeated authentication attempts, communication loss, and power interruption.

Privacy also requires attention when electronic locks record user identities and access histories. Biometric templates, mobile identifiers, and entry logs may reveal sensitive information about individuals and their activities. Research on biometric authentication and IoT security highlights the importance of privacy protection and secure handling of personal information [18], [19]. Access records should therefore be retained only, when necessary, protected against unauthorized disclosure, and managed according to clearly defined data access policies.

7. FUTURE RESEARCH DIRECTIONS

Future electronic door lock development should prioritize integrated security rather than relying on a single authentication technology. Multi-factor authentication can combine independent credentials, such as an RFID card and PIN or a mobile device and biometric verification. However, combining several methods should not create unnecessary complexity or make emergency access difficult. Research on authentication protocols for RFID and smart-home wireless sensor networks provides useful foundations for developing more secure and resource-efficient access systems [12], [13], [20].

Further research should also address interoperability, low-power operation, and systematic security testing. Electronic locks from different manufacturers may use incompatible communication protocols and access management platforms, limiting integration within larger building automation systems. Standardized interfaces and secure update mechanisms could improve maintainability and reduce the risks associated with outdated software. Experimental evaluations should measure authentication accuracy, response time, power consumption, mechanical endurance, communication reliability, and resistance to representative attacks.

8. CONCLUSION

Electronic door locks represent an important development in access control because they combine electronic authentication, embedded processing, and electromechanical locking mechanisms. Keypads, RFID, Bluetooth, mobile applications, and biometric sensors provide different approaches to user identification, each with specific advantages and limitations. Their practical effectiveness depends on the quality of the authentication method, the reliability of the actuator, and the protection of electronic and communication components. The review also shows that IoT connectivity can improve remote management while introducing additional cybersecurity and privacy concerns. Reliable electronic door lock design therefore requires a balanced approach to security, usability, reliability, and emergency operation. Multi-factor authentication, cryptographic credential protection, secure wireless communication, backup power, and local operating capability should be considered essential design priorities. Future systems should be evaluated through comprehensive testing that includes physical, electrical, software, and communication failure scenarios. By addressing these requirements together, electronic door locks can provide more dependable access control for residential, commercial, and institutional environments.

REFERENCES

[1] A. Juels, "RFID security and privacy: a research survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, 2006, doi: 10.1109/JSAC.2005.861395.

[2] H. M. Sun and W. C. Ting, "A Gen2-based RFID authentication protocol for security and privacy," *IEEE Transactions on Mobile Computing*, vol. 8, no. 8, pp. 1052–1062, 2009, doi: 10.1109/TMC.2008.175.

[3] S. S. Chandra, R. Lim, and H. Khoswanto, "Door access control system using RFID and an Android application in a control systems laboratory," *Jurnal Teknik Elektro*, vol. 11, no. 1, pp. 17–22, 2018.

[4] A. A. G. Ekayana, "Implementation of a multi-access door locking system using 13.56 MHz Mifare RFID," *Jurnal Pendidikan Teknologi dan Kejuruan*, vol. 15, no. 2, 2018, doi: 10.23887/jptk-undiksha.v15i2.14361.

[5] A. Dewani, P. Memon, V. Kumari, A. Arain, A. Jiskani, and S. Bhatti, "Keyless smart home: an application of home security and automation," *Oriental journal of computer science and technology*, vol. 11, no. 2, pp. 107–114, 2018, doi: 10.13005/ojcst11.02.06.

[6] S. Shin and T. Kwon, "A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart homes," *Sensors (Basel, Switzerland)*, vol. 19, no. 9, 2019, doi: 10.3390/s19092012.

[7] D. Mendez Mena, I. Papapanagiotou, and B. Yang, "Internet of things: survey on security," *Information Security Journal*, vol. 27, no. 3, pp. 162–182, 2018, doi: 10.1080/19393555.2018.1458258.
[8] M. binti Mohamad Noor and W. H. Hassan, "Current research on internet of things (IoT) security: a survey," *Computer Networks*, vol. 148, pp. 283–294, 2019, doi: 10.1016/j.comnet.2018.11.025.
[9] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, "Access control in internet-of-things: a survey," *Journal of Network and Computer Applications*, vol. 144, pp. 79–101, 2019, doi: 10.1016/j.jnca.2019.06.017.
[10] Z. Rui and Z. Yan, "A survey on biometric authentication: toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019, doi: 10.1109/ACCESS.2018.2889996.
[11] R. Baashirah and A. Abuzneid, "Survey on prominent RFID authentication protocols for passive tags," *Sensors (Switzerland)*, vol. 18, no. 10, 2018, doi: 10.3390/s18103584.
[12] D. Z. Sun and L. Sun, "On secure simple pairing in bluetooth standard v5.0-Part I: Authenticated link key security and its home automation and entertainment applications," *Sensors (Switzerland)*, vol. 19, no. 5, 2019, doi: 10.3390/s19051158.
[13] X. Zhang and Y. Hu, "RFID mutual-authentication protocol with synchronous updated-keys based on Hash function," *Journal of China Universities of Posts and Telecommunications*, vol. 22, no. 6, pp. 27–35, 2015, doi: 10.1016/S1005-8885(15)60690-2.
[14] Y. Qiu, J. Zhou, J. Baek, and J. Lopez, "Authentication and key establishment in dynamic wireless sensor networks," *Sensors*, vol. 10, no. 4, pp. 3718–3731, 2010, doi: 10.3390/s100403718.
[15] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: a review," *Symmetry*, vol. 11, no. 2, 2019, doi: 10.3390/sym11020141.
[16] J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: a survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014, doi: 10.1109/ACCESS.2014.2381273.
[17] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys*, vol. 47, no. 2, 2015, doi: 10.1145/2617756.
[18] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017, doi: 10.1109/JIOT.2017.2694844.
[19] S. Olarewaju, A. S. Sadiq, O. Kaiwartya, and A. Konios, "Privacy-preserving biometric authentication in resource-constrained environments: a Prisma systematic review of multimodal and fuzzy-vault methods," *Journal of Cybersecurity and Privacy*, vol. 6, no. 3, 2026, doi: 10.3390/jcp6030103.
[20] A. Barua, M. A. Al Alamin, M. S. Hossain, and E. Hossain, "Security and privacy threats for Bluetooth low energy in IoT and wearable devices: a comprehensive survey," *IEEE Open Journal of the Communications Society*, vol. 3, no. 5, pp. 251–281, 2022, doi: 10.1109/OJCOMS.2022.3149732.