IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 16 October 2023, accepted 10 November 2023, date of publication 20 November 2023,
date of current version 29 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3335115

SURVEY

Design Recommendations for Gate Security Systems and Health Status: A Systematic Review

ABDULLAH M. ALMUHAIDEB[1], MARIAM ELHUSSEIN[2], REEM OSMAN[3], FATEMA ALHOLYAL[2], LEENA ALGHAMDI[2], MAJD AL-ISMAIL[2], MARAM ALAWAMI[2], ZAINAB KADOUR[2], AND RACHID ZAGROUBA[2]

[1]Saudi Aramco Cybersecurity Chair, Department of Networks and Communications College of Computer Science and Information Technology, Imam Abdulrahman bin Faisal University, Dammam 31441, Saudi Arabia
[2]Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman bin Faisal University, Dammam 31441, Saudi Arabia
[3]Department of Computer Science, Applied College, Imam Abdulrahman bin Faisal University, Dammam 31441, Saudi Arabia

Corresponding author: Mariam Elhussein (maelhussein@iau.edu.sa)

This work was supported by the Saudi Aramco Cybersecurity Chair, Imam Abdulrahman bin Faisal University, Saudi Arabia.

ABSTRACT Gate security systems use authentication methods to operate hardware components that grant or deny access to restricted areas. Each context has specific requirements to determine user admissibility. There are currently no design recommendations available for these systems despite their significance. Most research proposes designs based on their recommended authentication scheme without providing general guidance on constructing these systems. This study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to conduct a systematic literature review, focusing on recent smart gate research. Studies published between 2016 and 2023 are analyzed and evaluated to identify their main components and authentication schemes. A total of 52 studies published in various journals and conferences are collected. After conducting the review, three main design themes are identified: smartphones, tags, and biometrics. These themes are the focal point of the study. Of all the designs, 66% consider using only one-factor authentication. These designs primarily rely on biometric-based methods. During the COVID-19 crisis, some designs used biometric authorization instead of identity authentication to incorporate health status, with a focus on detecting whether the person wore a face mask and had a normal body temperature. Furthermore, the review reveals that most studies disregard the system's hardware components and focus on authorization. Additionally, only 25% of the studies conduct an implementation for their design and produce results evaluating their performance. The study concludes that a successful smart gate design must consider and balance cost, usability, and security. Furthermore, health status needs to be verified as an additional layer of protection after determining the existing authentication requirements.

INDEX TERMS Biometrics (access control), COVID-19, face recognition, health and safety, iris, Internet of Things, smart healthcare.

I. INTRODUCTION

The main task of a gate is to protect and prevent unauthorized entry. A smart gate performs its task while heavily relying on an intelligent ecosystem that incorporates other factors to either allow or deny access. Consequently, a gate security system can be defined as an integrated gate equipped with electronic components, such as proximity sensors and actuators, with the aim of reducing the effort needed to open and close gates [1]. A smart door has a smart digital lock system that allows a person to open a door or grant access to a location via user authentication. Essentially, the technology used for smart-door implementation is controlled by a microcontroller, combined with identification in the form of a password [2].

With increasing industrial and residential sectors, automated gates have become a significant concern for end users. Automated access control systems for security and privacy threat prevention are vital in various contexts, such as airports, educational facilities, and residential compounds.

The associate editor coordinating the review of this manuscript and approving it for publication was Zahid Akhtar.

Standard requirements are shared among all contexts, such as verifying the user attempting to enter and the hardware that opens and closes the gate once the user is approved. However, the security level is different based on the criticality of the place. For instance, in airports, designs are focused on allowing only one person through the gate. Such a requirement is relaxed at a residential gate, thus allowing multiple people to enter together.

Various researchers have developed designs for gate security systems. While only some of these designs identify the hardware components of the gate, all of the designs focus on the authentication scheme used to either allow or deny access. To our knowledge, a systematic review has yet to be conducted on gate security systems. Such a review is essential for identifying the trending technologies and the emerging issues associated with these systems. Furthermore, such a systematic review will serve as a reference for design recommendations based on previous studies and highlight areas for possible improvement. Moreover, such a review can help identify possible threats and attacks that can affect these systems and possible solutions.

Authentication schemes are expected to preserve the integrity, certification, and availability of the systems they protect [3]. They generally fall into three categories: what you know, what you have, or what you are [4]. Some researchers have proposed other categories, such as where the user is (based on location) and what the user does [5]. Systems are secured with one or more factors from the following categories. Each factor is associated with threats or weaknesses that compromise access. To identify system vulnerabilities, one can map the authentication schemes being used. This approach will help to detect any potential weaknesses in the system.

A. HEALTH STATUS AS SECURITY REQUIREMENT

In response to the COVID-19 pandemic, countries ramped up efforts to trace and contain the virus's rapid spread. Countries imposed restrictions to limit the advancement of COVID-19, such as wearing masks, maintaining the temperature within the normal range, minimizing gatherings, enforcing social distancing, the continuous sterilization of surfaces and hands, and not sharing artifacts. These measures were necessary to tackle the virus and slow its spread until a cure or vaccination was found. Accordingly, a new form of admissibility was introduced in many countries worldwide.

In early December 2020, drug authorities in several countries conditionally approved newly developed vaccines. The Kingdom of Saudi Arabia linked all its residents to an application called ''Tawakkalnaâ'' to manage and display their health status to those concerned. Those who were not fully vaccinated were not allowed access to facilities. Security personnel oversaw the verification of the health status of those who wished to enter various facilities despite them having obtained prior permission. This became problematic as the queue of people or cars wanting to enter increased at certain times, placing additional pressure on the security guards. Thus, the access of gate security systems needs to be automated based on the existing designs of automatic gate systems while also considering the health status as a security requirement.

This study aims to identify the general design requirements for gate security systems by referring to existing designs. Furthermore, it reviews the possible threats to such systems and identifies ways to overcome them. The design recommendations are based on the emerging technologies reported in the literature while also incorporating health status regarding COVID-19 as a security requirement. Identifying health-aware gate security systems contributes to the consideration of health requirements, as in the case of the COVID-19 pandemic and other future situations. This study also aims to identify the performance evaluation metrics for gate security systems.

B. VULNERABILITIES OF GATE SECURITY SYSTEMS

Gate security systems are becoming increasingly crucial for preventing access to those who are unauthorized. Such systems can be set up for protection in various locations, such as banks, healthcare centers, educational facilities, and gated houses. For example, a previous study [6] designed a gate system to protect automatic teller machines (ATMs) from unauthorized access. Other systems have been designed to automatically allow access to educational facilities based on an official ID. During the COVID-19 pandemic, screening shifted to checking the health status of those entering based on certain guidelines. Users were not allowed entry if they were not vaccinated, not wearing a mask, or presented with a high temperature. Smart gate systems have authentication vulnerabilities such as man-in-the-middle attacks, stolen verifiers, guessing, forgery, or eavesdropping [7]. The choice of the authentication approach is based on its performance, usability, and security [4]. Therefore, the design considerations of a smart gate are primarily guided by the understanding of possible threats and drawbacks.

This study mainly aims to thoroughly review gate security system designs. Specifically, it aims to collate the literature and critically evaluate how the designs of gate security systems are proposed, implemented, and considered. The remainder of this paper is as follows. Section II describes the research methodology and research questions. Section III provides a background that explains the design of gate security systems. Section IV proposes various classifications for gate security systems based on the reviewed literature. Section V includes a discussion and a review of the limitations. Section VI explains the solution requirements for gate security systems, specifically those that incorporate health status. Section 7 presents a brief conclusion and future directions of study.

C. RESEARCH CONTEXT

The current research was inspired by the challenges encountered during the COVID-19 pandemic. The main

challenge at this time was introducing health status as an extra layer of security along with authentication schemes. Another challenge was to utilize technology to achieve health guidelines that required social distancing and contactless interaction. Furthermore, the designs were expected to incorporate data from external systems, including vaccination status and negative test results. These dimensions suggested exploring the existing efforts and determining how new designs can be extended to support the new requirements. It also presented the need to identify design evaluation methods and quality targets.

This work is expected to contribute the following to the body of knowledge:

- Explore and categorize the existing smart gate designs;
- Identify design guidelines that can be followed to produce new smart gate designs;
- Determine the quality dimensions of smart gates that can guide performance evaluation; and
- Identify the gap in the published works that propose smart gate designs.

II. RESEARCH METHODOLOGY

Systematic literature reviews collate literature and combine findings to examine a hypothesis [4]. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines describe the steps that should be taken to ensure a study's rigor. The current such review will guide similar future reviews and justify the list of the included literature. The current systematic literature review process involved three main stages: planning, conducting, and reporting.

A. RESEARCH QUESTIONS

This study performed a systematic literature review of papers about gate security systems that have been published since 2016. Although articles on gate security systems were published before 2016, only the most recent ones are focused on uncovering the latest trends. Moreover, more recent papers are expected to highlight the current designs that propose incorporating health status as part of the COVID-19 calamity. Numerous databases were consulted, including SpringerLink, ScienceDirect, Elsevier, and Institute for Electrical and Electronics Engineers (IEEE) Xplore. Access was obtained through Web of Science and Scopus to obtain trusted and relevant papers. To identify the relevant articles, the following search terms were used: ''Secure Access,'' ''Automatic Gate,'' ''Smart Door,'' ''Access Control System,'' and ''Gate Security.'' Research questions were formulated to guide the search process as follows: Q1: What are the components of gate security systems? Q2: How does authentication occur in such systems? Q3: What are the possible threats and drawbacks of gate security systems? Q4: What are the design considerations of gate security systems when supporting health security?

B. SCOPE OF REVIEW

Papers were reviewed in terms of relevance using their titles, abstracts, and keywords. Many were excluded because they were based on similar topics, such as cloud storage and network access. In the screening process, titles available for full access were also reviewed. Studies proposing the design of gate security systems were the focus. Some such studies addressed hardware- and software-related aspects, whereas others only focused on authentication and authorization processes. All these studies were included in this review.

C. RESULTS

Initially, 486 papers were retrieved, of which 45 were found to be duplicates. After identifying the target period as 2016-2023, the number of papers decreased to 255. Moreover, papers that were not fully accessible were excluded. Some of the papers were thoroughly read to identify their contributions and contents. The final number of papers reviewed was 52. Fig. 2 shows the PRISMA diagram created by [8].

III. BACKGROUND AND RELATED WORK

Gate security systems include smart locks, smart doors, automatic gates, gate controllers, access control systems, entrance guards, electronic gates, security controls, and other systems. Some of these terms are used in this review to refer to gate security systems, as defined in the introduction. Gate security systems comprise authentication/authorization schemes that aim to determine whether a user can enter. Authentication involves the identification of the user's identity, whereas authorization determines whether the user has access. This scheme commands a hardware component that moves the door and allows access. Some smart doors described in the literature comprise a sensor that automatically activates the authorization process. Numerous studies have focused on authentication/authorization schemes, only some of which provide descriptions of the hardware components used. Some of the described hardware components need to be more suitable for real-life doors. These designs have been used as prototypes to test the door's ability to authorize access. This section closely examines hardware components and authentication schemes used in smart doors. The first subsection summarizes the hardware components used to design gate security systems. The second subsection groups the authentication schemes used, including smartphone-, biometric-, and tag-centered systems.

A. HARDWARE IN GATE SECURITY SYSTEMS

The hardware components described in the literature include a microcontroller, a distance sensor, and an actuator. The microcontroller is a programmable circuit board that connects and controls other hardware. A distance sensor measures the distance between the user and the gate. The actuator moves the gate to open and close. Some studies employed Raspberry

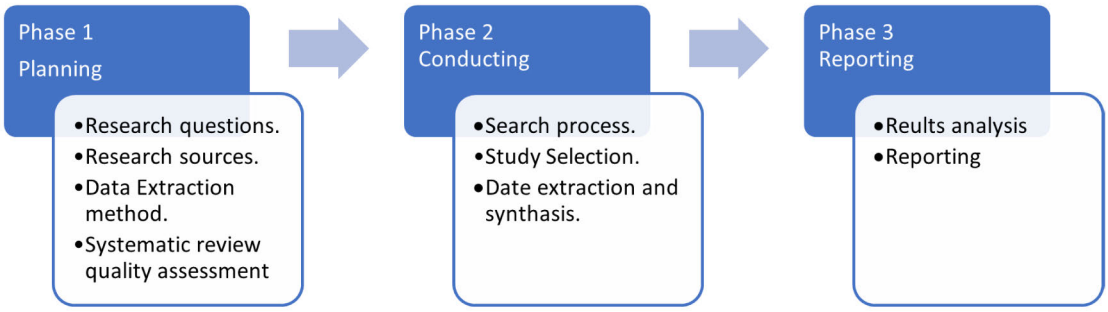

FIGURE 1. Systematic literature review phases.

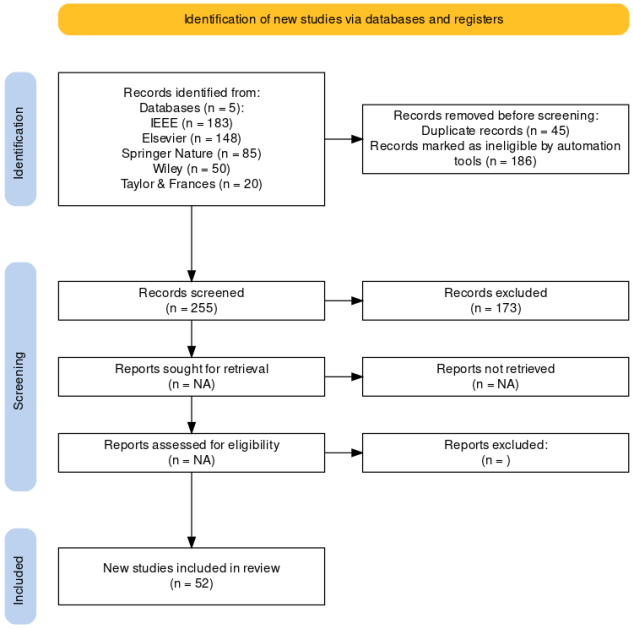

FIGURE 2. Selection process results.

Pi and Arduino as microcontrollers, whereas others do not discuss what hardware they used. The type of motion sensor used is also specified in some studies. Regarding actuators, some studies used direct current (DC) motors with electromagnetic locks, whereas others used solenoid door locks. The employment of other hardware components was found to depend on the authentication scheme, such as radio frequency identification (RFID) tag readers, quick response (QR) code readers, cameras, thermal cameras, fingerprint readers, and vein pattern readers. Overall, while the software components of gate security systems have received a fair amount of attention, the selection and setup of hardware components need to be more focused on.

B. AUTHENTICATION IN GATE SECURITY SYSTEMS

The software component of a gate security system is responsible for verifying whether a user meets the requirements to be allowed access. The literature review revealed a trend regarding the approaches used to design smart doors. Three types of systems were identified: smartphone-, tag-, and biometric-centered systems. These categories emerged based on the main authentication factor used when designing each gate. Some gates may use multiple factors; however, entrance requires a smartphone, a tag, or a biometric feature to function. These systems are summarized in the following subsections.

1) SMARTPHONE-CENTERED SYSTEMS

Smart gates are designed to utilize smartphones to exploit their various options. Smartphones provide a means for verifying a user's identity. Reference [9] used smartphones to verify user login information. They designed a smart gate that uses broadcast messages from a mobile app that connects to the gate to either allow or deny access. Their zero-effort authentication is activated based on proximity to the smart gate and whether the user has logged into the mobile application. Similarly, [10] suggested sending a QR code to a smartphone app to allow users access to secured areas. Their design is low-cost and flexible.

Furthermore, some designs center around smartphones that employ technologies that are available in these devices, such as Bluetooth, Wi-Fi, and General Packet Radio Service (GPRS). A study published in 2016 suggested the use of Bluetooth [6]. The authors proposed a solution for its application as a locking system in ATMs. Using an exclusive mobile app, the smartphone functions as a repeater and sends a secret code from the server. This code is communicated to the gate using Bluetooth technology. The design allows other options for connecting with the gate, including university serial bus (USB) channel connections. A similar study was conducted in [11]. Reference [12] tested a system based on smartphone Bluetooth authentication and found that it is a good alternative to RFID technology regarding accuracy and speed. Additionally, they highlighted its convenience, as users are more likely to remember their smartphones. They found that the gate responded to the system when the phone was at a maximum distance of 5 m. Reference [13] improved

this distance to 8 m. Their application was set up to allow the opening of garage doors from a distance. References [14], [15], and [16] used a similar approach.

Reference [17] introduced an automatic lock for short-stay vacation homes using smartphones and Bluetooth connections. This system unlocks the door using Wi-Fi, allowing homeowners to unlock their homes for visitors. Consequently, homeowners can leave the house and still allow visitors entry; moreover, the designed mobile app with Bluetooth-enabled messages allows one to authenticate visitors. Therefore, homeowners have high flexibility and can unlock their homes from almost anywhere. Reference [18] proposed a similar approach.

Furthermore, [19] presented an alternate method for authorizing smartphone access. Their cloud-based approach encourages logins from the WeChat applet. This front-end solution allows users to register a smart door to be unlocked through the app in the future. Authentication occurs in a cloud database that passes a Hypertext Transfer Protocol (HTTP) request to Raspberry Pi for hardware response. Although the system outperforms existing designs, some safety- and integrity-related deficiencies require improvement.

Smartphone imaging capabilities have been used to provide live feed for property owners based on the design proposed by [20]. When a user arrives at a locked door, they must have an Android app installed that connects to the Bluetooth scanning application in the gate. The owner can view the user through the mobile app and grant access if the user is authenticated. The owner's app is connected through Wi-Fi to the smart gate. Similarly, [21] used an Android app for similar authentication, which worked at a maximum distance of 19.2 cm.

2) TAG-CENTERED SYSTEMS

This subsection describes the designs that contain tags or cards that use RFID or QR codes. References [22] and [23] proposed using a QR code. Their systems have an acceptable response time and are inexpensive to install. Reference [24] created an authentication protocol by defining public and private keys. The keys are augmented in a smart card that the user can use. Tag-centered authentication in smart doors based on RFID has also been reported. Reference [25] combined RFID authentication with the image scanning of the user's picture from their card. However, this method still leaves the final decision up to the security guard. Another study combined RFID and messages sent via the Global System for Mobile Communication (GSM) to the user's phone [26].

3) BIOMETRIC-CENTERED SYSTEMS

The third design theme is based on biometrics. Biometrics are unique anatomical or behavioral features either found in or performed by individuals, respectively [27]. Anatomical features include the iris, retina, face, and veins, whereas behavioral features include one's voice, signature, and keystroke rhythms. In the context of smart doors, iris, vein patterns, fingerprints, and face recognition have been employed for authentication. Many studies have yet to consider factors other than single-factor authentication. A previous study proposed using irises to authenticate a smart door [28]. This method uses images scanned from patterns in the user's eye for recognition. It is regarded as one of the fastest and most reliable biometric authentication approaches; however, it is not as common owing to its high cost. Another study proposed using one's vein pattern [29]. They concluded that a high level of classification accuracy can be achieved using neural networks as classification and categorization models. Reference [30] proposed a fingerprint-based smart-door design. Their system uses a ZigBee wireless network to transfer a fingerprint image to the server for comparison. However, they did not publish any results. Another study proposed using fingerprinting as an authentication method [31]. Specifically, they proposed an algorithm to improve fingerprint reading using short-time Fourier transform (STFT). Reference [32] combined fingerprint authentication with RFID to enhance security. Their system was found to be sensitive to sunlight. In a recent study, [3] proposed fingerprinting as an authentication method. They used an artificial neural network (ANN) for feature extraction from fingerprint images. However, their main contribution is enhancing gate security using blockchain technology. This is crucial for the door design of sensitive areas where network attacks threaten gate security.

Earlier models focused on the facial features to be extracted. Using a webcam and principal component analysis (PCA), reference [33] attained an accuracy of 95% from a distance of 60-120 cm. They also reported a response time of 1.21 s for the matching process, without accounting for the hardware response time. A similar study [34] reported a response time of 4.6 s, including hardware movement. However, their model was 80% accurate. Reference [2] proposed a similar design; they applied a PCA method called EigenFace, and their model achieved an accuracy of 94% from a distance of 25-75 cm. Similar designs have been proposed by [35] and [36]. In [37], face recognition was used to identify gender, but no results were reported. Another study by [38] performed facial detection using neural networks. These authors built a backpropagation neural network model to improve face recognition accuracy and achieved 97.8% accuracy and an 0.8% false detection rate. Recently, [39] used a low-cost camera to collect images of users and place them in the cloud. Their system automatically compares the saved images with users attempting to access them. If a match exists, the door unlocks; otherwise, an alarm goes off, and pictures of the user are sent to the place owner. Reference [40] proposed a similar design.

Reference [41] designed a multifactor authentication approach that mainly relies on face recognition. They used PCA and linear discriminant analysis to improve the model

TABLE 1. Table summarizing the designs in the literature along with their advantages, disadvantages, and challenges.

Study	Type of system	Advantages	Disadvantages	Challenges
[9]	Mobile-centered	Convenience	Small proximity, needs a Wi-Fi connection	Distance, connectivity, identity checking, need for specific software or apps
[10]		Low cost		
[6], [11]		There is an option to access using a USB link	Needs a connection through Bluetooth and Wi-Fi	
[12]		Accurate, speed, convenience, response distance up to 5 m		
[13], [14], [15], [16]		Improved response distance up to 8 m		
[17], [18]		Good response distance, authorize user phone	No identity authentication	
[19]		Faster, improved response distance	Some security deficiencies	
[20]		Identity check using a camera	The need for connection through Wi-Fi, decision made by humans	
[21]		Identity check using a camera, improved response distance 19.2 cm		
[22],[23]	Tag-centered	Low cost	Low response time	Tag can be lost
[24]		Double authorization through public and private keys		
[25]		Authentication through picture scanning	Final human decision	
[26]		Confirm through GSM	Connectivity	
[28]	Biometric-centered	Fast, reliable	High cost	Distance, cost, response time
[29]		Accuracy		
[30]		Compare images to a database	Connectivity, no published results	
[31]		Improved reading time		
[32]		Combined with RFID to enhance security	Sensitive to sunlight	
[3]		Enhanced security using blockchain		
[33]		Accuracy 95%	Short distance 60-120 cm, response time 1.21 s + hardware response	
[34]			Response 4.6 s, low accuracy at 80%	
[2]		94% accuracy, distance better at 25-75 cm		
[38]		Accuracy of 97.8%		
[39], [40]		Low-cost camera	Needs Wi-Fi	
[41], [42], [43]		Recognition under different lighting conditions, alternative options (card and password), 98.9% accurate	Speed	
[44], [45]		Investigated order to authentication to improve accuracy (RFID, fingerprint, face detection)		
[46]		Improve response distance	Low accuracy at 74.6%	
[47]		92% accuracy	Slow at 14 s	
[48]	Health centered		No identity verification	Reporting cases of not wearing mask, final decision by human
[49]			Human decision	
[50]		Checking temperature	Human decision	
[51]		Collect vaccination and temp using audio	Problem with dim lighting and voice detection	
[52]		Authenticate, although with a mask	77% accuracy	
[53]		Checking the temperature and verifying masks	High-cost sensors	

accuracy. They resolved the issue of facial recognition under various lighting conditions. Furthermore, for increased user friendliness, users are needed to swipe RFID cards. The door accepts password authentication when the user forgets their card. The system has 98.9% accuracy. Similar designs have been proposed by [42] and [43], with 100% and 97.2% accuracies, respectively.

Reference [44] adopted a multifactor approach focusing on face recognition. They used face recognition, RFID, and fingerprints to investigate different scenarios to reduce the

false acceptance and false rejection rates. They experimented with the order of authentication and found that RFID followed by fingerprint and face recognition yields the best results. Reference [45] proposed a similar design. Reference [46] proposed a multifactor authentication design. They used license plates, car makeup, and face detection to allow access. Their model aims to protect gate communities and allow access from a distance. The model has 74.63% accuracy. A two-factor approach based on face detection and a smartphone application was presented in [47], in which the authors achieved 92% accuracy, a 4% false detection rate, and low error rates. The response times were 13 s for iOS smartphones and 11 s for Android.

a: HEALTH STATUS-CENTERED SYSTEMS

In health status-centered systems, the user's health status needs to be verified before allowing access. Three such designs have been proposed following COVID-19 restrictions. The first design proposed using face recognition to identify whether a user is wearing a face mask [48]. Using deep learning, particularly Mnet and Res-Net, [49] proposed a system to recognize and report those who are not wearing masks. Reference [50] extended this design to incorporate the temperature of the user, in which the user's temperature is acquired using a thermal camera attached to the gate. The third design includes COVID symptoms, risk factors, and vaccination information [51]. It also collects audio data to reduce the chances of contact with users. However, the system suffers from problems, such as dim lighting and voice detection.

The design proposed by [52] uses an OpenCV image-processing library from Python to detect people wearing face masks. It incorporates color recognition from a smartphone, which displays green if someone does not have COVID-19. The main contribution of this design is highlighted by the model's ability to identify human faces despite the use of a mask. For users wearing masks, the model detection accuracy rate was 77%. Reference [53] presented a model that checks the use of masks and evaluates body temperature. They used OpenCV and TensorFlow libraries for image processing and noncontact infrared temperature sensors.

It is noticeable that these designs were not proposed as an additional layer to the existing authentication process of a specific place, i.e., an educational facility. Instead, the authors suggested that these gates be used for the sole purpose of determining the admissibility of users based on their health status. Therefore, none of the abovementioned designs explored the effect of having the gate authenticate or authorize the user. However, the work of [52] was directed toward uncovering the person's identity behind their mask. While representing a step toward incorporating health status with the traditional authentication/authorization process, the authors' effort needs to be explored or detailed more than it is in their design. Table 1 summarizes and compares the results based on advantages, disadvantages, and challenges.

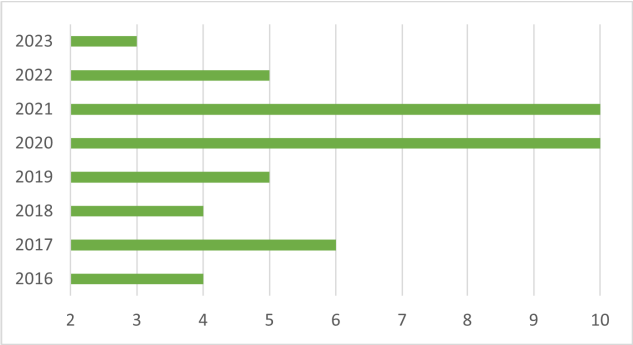

FIGURE 3. Distribution of publications over time.

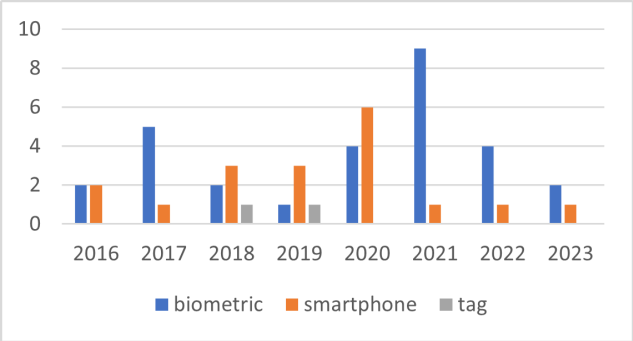

FIGURE 4. Distribution of themes over the years.

IV. CLASSIFICATION OF SECURE GATE SECURITY SYSTEMS

A. DISTRIBUTION BY YEAR OF PUBLICATION

The literature review shows that gate security systems are gaining an increasing amount of attention. Figure 3 shows that the level of interest in research on gate security solutions focusing on health-aware designs increased between 2021 and 2022. Specifically, biometric-centered gate systems have gained the most interest, followed by smartphone-centered systems (Figure 4).

B. DISTRIBUTION BY TYPE OF PUBLICATION

Fig. 5 displays the distribution of publications based on four categories: journal papers, proceedings, IEEE conferences, and conferences. It can be seen that journal papers and conferences are the most common type of publications.

C. DISTRIBUTION BY AUTHENTICATION ELEMENTS

This review reveals an increasing interest in applying face-detection authentication, with almost half of the designs including face detection as either the only authenticating factor or an accompaniment to other factors. The trend is moving toward applying face detection and improving system accuracy by implementing machine-learning and image-processing techniques. Most of the proposed designs suggest features that can improve the accuracy of the detection algorithm. Advancements in image-processing techniques have suggested further progress in this domain. Furthermore,

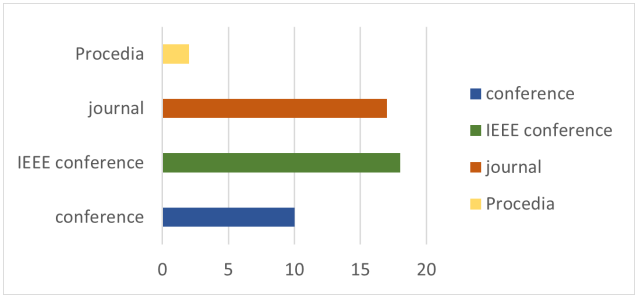

FIGURE 5. Distribution based on the type of publication.

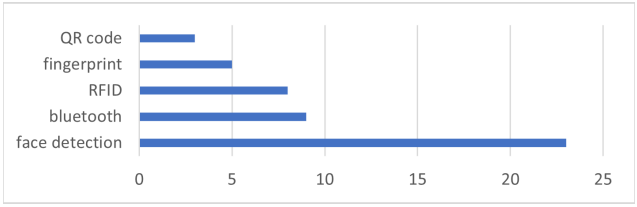

FIGURE 6. Distribution based on main authentication elements.

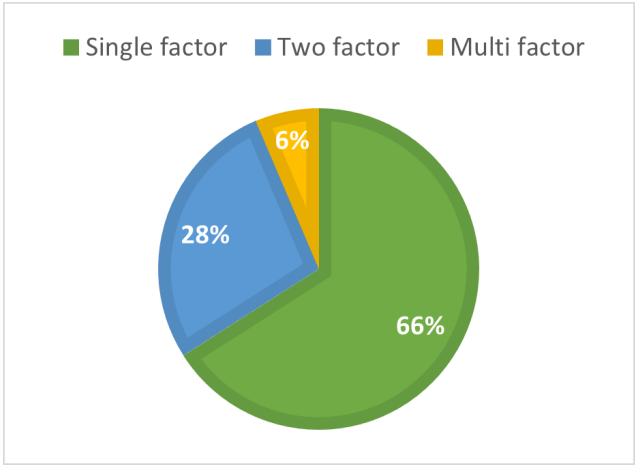

FIGURE 7. Distribution based on the authentication model.

the fact that most smartphones use face detection for authentication has encouraged the use of these devices as a second layer to verify user identity. Fig. 6 shows the distribution of the principal elements in the designs. Single-factor authentication has been dominantly used in the literature, with almost half the designs employing biometric factors and the other half employing smartphones. Fig. 7 displays the number of designs that suggest single, double, and multiple factors for authentication. Based on [54], an authentication scheme is considered multifactor if it employs two or more authentication technologies from the following categories: something you know, something you have, and something you are. Although many designs have employed single-factor authentication, others have employed double- or multifactor authentication. Fig. 8 shows the distribution of the most-combined themes, which are the biometric and tag themes.

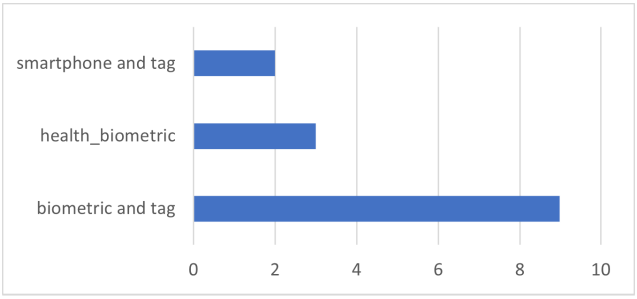

FIGURE 8. Distribution based on the most-combined themes.

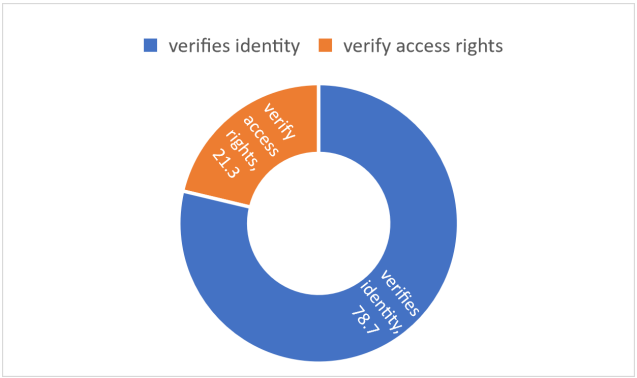

FIGURE 9. Distribution based on authentication or authorization.

Another evaluation criterion for gate security systems is whether they verify access rights (authorization) or identity (authentication). Almost 80% of the designs verify the user's identity, whereas the remaining designs confirm only the user's accss rights. Figure 9 shows the distribution. Only two designs verify the user's identity out of the six health status-centered designs presented.

V. DISCUSSION AND LIMITATIONS

This literature review reveals that the hardware components associated with gate security systems have yet to be discussed for all designs. However, these components are an integral part of the system and can affect its performance. Raspberry Pi and Aurdino have been used as controllers, with the latter being more affordable. Therefore, most of the designs have employed Aurdino. Sensors are not frequently used because of the design specifications; for example, the card reader is activated when a card is swiped in designs with RFID cards. Other aspects related to the response time of the gate can be attributed to hardware components; however, this has yet to be discussed in the literature.

Additionally, the authentication themes proposed and the factors frequently used in the literature were revealed through the current review. Security, usability, and performance are the aspects that need to be considered when discussing solution requirements. Smart gates aim to provide protection and prevent unauthorized individuals from passing through the gate. This is achieved by satisfying the basic requirements of the security process via authentication. Most designs

TABLE 2. Comparing themes based on possible attacks and those that can be overcome or reduced.

Theme	Factors	Possible attacks	Overcomes/reduces
Smartphone-centered	Bluetooth	man-in-the-middle attacks, stolen verifiers, guessing, forgery, or eavesdropping	Guessing, shoulder surfing
	Mobile app		
Tag-centered	QR code	Forgery, man-in-the-middle attacks, stealing token	Guessing, shoulder surfing, one-time observation
	Smartcard		
Biometric-centered	Face detection	Replay attack, impostor attack, forgery, man-in-the-middle attacks	Guessing, shoulder surfing, forgery, brute force, stolen verifier, one-time observation
	Fingerprint		
	Iris		
	Vein		
	Health status		

employ single-factor authentication that relies on biometric factors. For instance, face-detection methods verify the identity of a user along with their right to access. Table 1 compares single factors, possible attacks, and attacks that the factors can overcome.

Security can be enhanced by combining multiple factors. Although combining tag authentication with biometrics increases security, the cost increases, and performance may be compromised.

Usability is defined as the degree to which legitimate users can enter the main gate with an acceptable level of efficiency and satisfaction without compromising the proposed security mechanisms and ease of use and without having recurring problems [9]. User satisfaction addresses several aspects, including approval and acceptance of the system's functionality and efficiency. This is typically guided by the gate's performance under the applied security scheme. Usability can be determined by interviewing or surveying users or observing their interactions with a gate [55]. Among the reviewed literature, although some studies have investigated the system's performance, none of them have explored usability. Generally, a usable system balances performance and security requirements to manage user errors efficiently. Reference [4] listed some items relevant to usability applicable to gate security systems, such as convenience (less to carry), learnability, accessibility (from a wide range of users), and prioritizing users.

Convenience involves what the user must have to be admitted through the gate. Biometric authenticators are highly convenient, mobile authenticators are moderately convenient, and tags are the least convenient. The chance of one forgetting his or her mobile phone is lower than forgetting a tag. Regarding learnability, smartphone- and tag-centered systems are generally easy to learn, and most users are familiar with them. Biometric-centered devices are relatively less available because of their high cost; therefore, users may need more time to learn to use them. However, smartphones have given people access to fingerprinting and face recognition technologies, making learning easier. According to [56], biometric usability is a challenge for users with disabilities, which affects the accessibility level of this user group. Gate systems that employ mobile phones or tags prioritize users, whereas those that use biometrics prioritize system security. Some solutions have been introduced, such as the introduction of hand gesture recognition found in [57]. However, this solution does not verify user identity. Table 2 compares the usability of the three methods.

TABLE 3. Comparing authentication factors based on usability items: High (h), Medium (m), and Low (l).

	Smartphone systems	Tag systems	Biometric systems
Convenience	m/h	l	l
Learnability	h	h	l/m
Accessibility	h	h	l
Prioritize users	h	h	m

TABLE 4. Summary of performance criteria of gate security systems.

Tag-centered systems	Response time	None reported
Smartphone-centered systems	Distance	19.2 cm up to 8 m
Biometric-centered systems	Distance	25-120 cm
	Accuracy	74.63%-100%
	Response time	1.21 s
	False detection rate	0.8%-4%

The performance of the smart gates was evaluated in terms of the error rate, accuracy, reliability, and responsiveness. The error rate denotes the frequency with which the system gives falsely authorized/unauthorized access [9]. A false match rate occurs when two samples of user data from different individuals are labeled to belong to the same individual. This type of error is known as false acceptance [58]. Accuracy is the degree of precision with which a system distinguishes authorized individuals from unauthorized individuals. Reliability indicates the capacity of a system to deliver the necessary functions and features when needed and its ability to be error-free. Moreover, responsiveness evaluates the speed at which the system yields results. It is determined by calculating how long the system takes to match an individual's identity with the user requesting access, as well as the level of accuracy it delivers in the matching phase. When evaluating performance, various trade-offs exist; for example, increased accuracy can lead to decreased responsiveness. Therefore, the solution must satisfy the performance parameters.

The performance of smartphone-centered gate systems is focused on measuring the appropriate distance. Systems using Bluetooth have reported distances that do not exceed

TABLE 5. Comparison of gate security systems based on security, usability, and performance. ✓, requirement fulfilled; ∼, requirement fulfilled and exists; x, requirement not fulfilled; NF, requirement is not found.

System	Factor	Security	Usability					Performance			
		Authentication	Convenience	Learnability	Accessibility	Prioritizing users	Low cost	Distance	Accuracy	Response time	False detection rate
Tag-centered	QR	✓	∼	✓	✓	✓	✓	x	✓	NF	✓
	RFID	✓	∼	✓	✓	✓	✓	x	✓	NF	✓
	Smart card	✓	∼	✓	✓	✓	✓	x	✓	NF	✓
Smartphone-centered	Bluetooth	✓	✓	✓	✓	✓	∼	✓	✓	∼	✓
	Mobile app	✓	✓	✓	✓	✓	∼	✓	✓	∼	✓
	Wi-Fi	✓	✓	✓	✓	✓	∼	✓	✓	∼	✓
	Cloud-based	✓	✓	✓	NF	✓	∼	✓	✓	∼	✓
Biometric-centered	Face detection	✓	✓	✓	x	x	x	∼	∼	✓	∼
	Fingerprint	✓	✓	✓	x	x	x	∼	∼	✓	∼
	Iris	✓	✓	∼	x	x	x	∼	∼	✓	∼
	Vein	✓	✓	∼	x	x	x	∼	∼	✓	∼

19.2 cm. Tag-centered systems measure performance based on responsiveness; however, results have yet to be reported. Biometric-centered systems measure performance based on accuracy, in which the lowest reported accuracy for face detection is 74.63%, and the highest is 100%. Another measure is the distance, with the closest being 25 cm and the furthest being 120 cm. Responsiveness is another reported performance measure, and it ranges from 1.21 to 11 s. However, the higher end of the response time measures the time the hardware takes to physically open the gate and the time the detection algorithm takes. Some studies have also measured the false detection rate as 0.8%-4%. Table 3 summarizes the performance criteria and reported values. Although sufficient data do not exist for comparing the three approaches, it can be concluded that smartphone-centered systems allow for detection from a further distance compared with biometric-centered systems. This means that they can be used in gated houses or garages. On the other hand, the accuracy of biometric-centered systems is an important performance measure because it affects the security level.

Health-aware Gate Security Systems Gate security systems designed to address admissibility based on COVID-19 requirements are user-centric, as seen in most similar gate systems [59]. The designs are mainly biometric-centered. Earlier designs focused on authorization, whereas more recent designs incorporate authentication. Some designs detect whether a user is wearing a face mask. The use of a face mask complicates the authentication task. The only study in which the design performed authentication with face masks achieved 77% accuracy [52]. Other designs check the user's temperature; such designs employ thermal cameras to detect temperatures. Some performance features of thermal cameras include their temperature range, accuracy, and distance range [51]. Some cameras can detect temperatures from up to 1.5 m, with an accuracy of ±0.5°C. One study proposed a design that checks the user's vaccination status. This information is obtained from mobile phone applications provided by another independent system. In such solutions, priority is given to health status: facemasks, temperature, and vaccination status. Facemasks affect the authentication process; therefore, most designs do not check user identity. Using multiple factors to verify authentication increases the cost of these gates.

The usability of these gates is related to the factors that are used. Thermal cameras are easy to use and accessible to all user communities. Facial detection is used to detect masks, and it displays previously discussed issues. Gate security systems that check for COVID-19 requirements have more response times than other solutions. Table 4 compares the three types of systems regarding some of the factors discussed. The table shows where the requirements are fulfilled, partially fulfilled, not fulfilled, or not discussed.

VI. CONCLUSION AND FUTURE WORK

This study has reviewed the existing research on gate security systems. While various designs have been published in the literature, very few have highlighted the system's hardware components. The literature review has shown that smart gate designs could be smartphone-, tag-, or biometric-centered. Furthermore, the following research questions have been answered:

Q1: What are the components of gate security systems? Gate security systems comprise a hardware component that is controlled by a microcontroller. Designs propose the use of Raspberry PI and Arduino. They also include an authentication scheme that collects the data needed to authenticate users.

Q2: How does authentication occur in such systems? Authentication is achieved by obtaining data from a user's smartphone, tag, or biometrics and comparing this data with the user information stored in the gate system. The different approaches have both advantages and disadvantages related to security and usability. Some designs do not verify user identity. The designs based on COVID-19 are mainly focused on confirming facemasks and symptoms.

Q3: What are the possible threats and drawbacks of gate security systems? The threats identified in the literature are directly linked to the authentication schemes used. Issues such as man-in-the-middle attacks, forgery, and stolen tokens can occur. Solutions to these vulnerabilities have been summarized in Section V based on the classification of the designs presented. However, this discussion was drawn from studies focused primarily on authentication schemes rather than smart gate designs. None of the literature that has proposed designs for smart gates has critically evaluated these designs. There has been no discussion of attacks that can be associated with the gate's hardware, for instance, which can compromise the security of the gate system. Most designs

have focused on verifying smart gate performance regarding authentication/authorization.

Q4: What are the design considerations of gate security systems when supporting health security? The three considerations explained earlier apply when designing health status-aware smart gates. Most of the proposed designs rely on biometric authentication techniques such as face detection to detect masks and temperature sensors to check for those who present with a fever. However, the COVID-19 requirement of wearing a facemask hinders efforts toward automatic face detection. Therefore, it is necessary to use other forms of identity checking. On the other hand, using fingerprints may increase the hazard of spreading the virus since this process requires touching the surface of the fingerprint reader. Balancing these choices with the limitations of cost and usability make it challenging to propose a design that checks both the user's health status and identity to determine their admissibility. These dimensions have yet to be explored collectively and need to be presented to justify the trade-offs affected by the design decision. It is worth noting, however, that despite the urgent need presented by the COVID-19 pandemic, only six designs supported health status checking. However, these designs do not consider the need to check for the user's identity before entering a restricted area; rather, they consider the health status as the primary and only condition. The latest design was published in 2022. This may suggest that the interest level in the pandemic will not be long-lasting.

This review was conducted with the aim of synthesizing the existing efforts to clarify the approaches and highlight the gaps. The PRISMA guidelines were followed to ensure the highest rigor level in such research. However, some limitations may have affected the findings. Examples of such constraints include that not all the retrieved papers were accessible to the researchers. Other issues are related to the quality of the papers retrieved. While most of them propose designs for smart gates, very few are keen on exploring the full depth of the design. This allowed the inclusion of many designs that still need to be implemented or evaluated. Nonetheless, the review is considered a step forward that can attract attention to this critical aspect and inspire other designs and discussions to improve the quality of the produced research. It combines the technologies in both software and hardware domains, along with threats and solutions to some designs. It can serve as a good reference for future design within any context, as it helps determine the applicable requirements.

This review highlights the need to analyze the software and hardware components implemented in terms of security, usability, and performance. A holistic approach considering the three dimensions is needed to produce better designs. Furthermore, the focus needs to incorporate the hardware used. Hardware usage will affect a gate's cost, usability, and security. Future research directions can propose designs that are context aware based on the requirements of admissibility. This indicates the need for suitable hardware, software, and performance requirements based on where they will be used.

In conclusion, this review makes theoretical and practical contributions. The review categorizes smart gate systems based on authentication schemes based on the main technology used. This approach differs from other classification attempts based on the number of authenticating factors. Such categorization is useful because it indicates some characteristics associated with each type. Furthermore, the review identifies the gap in the published works describing smart gates. It highlights the issue of overlooking the importance of hardware specifications and how these specifications affect the quality of the design. The paper presents a practical contribution by presenting design guidelines for future efforts, including considering a smart gate's cost, performance, and security dimensions. It also argues for the importance of considering health status as an extra layer of security instead of proposed designs that focus on the health dimension while ignoring verifying user identity.

REFERENCES

[1] O. Bhat, P. Gokhale, and S. Bhat, "Introduction to IoT," *Int. Adv. Res. J. Sci., Eng. Technol. ISO*, vol. 5, no. 1, pp. 1–4, Jan. 2018.

[2] F. Azmi, I. Fawwaz, and R. Anugrahwaty, "Smart door system using face recognition based on Raspberry Pi," *JURNAL INFOKUM*, vol. 10, no. 1, pp. 360–369, 2021.

[3] K. Sujatha, N. P. G. Bhavani, U. Jayalatsumi, T. Kavitha, B. Latha, A. Ganesan, and A. Kalaivani, "Smart door locking system using IoT—A security for railway engine pilots," in *Sentiment Analysis and Deep Learning*. 2023, pp. 263–271.

[4] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, "Authentication systems: A literature review and classification," *Telematics Informat.*, vol. 35, no. 5, pp. 1491–1511, Aug. 2018.

[5] K. Abhishek, S. Roshan, P. Kumar, and R. Ranjan, "A comprehensive study on multifactor authentication schemes," in *Advances in Computing and Information Technology*. 2013, pp. 561–568.

[6] J.-I. Jeong, "A study on smart door lock control system," *Cluster Comput.*, vol. 19, no. 3, pp. 1607–1617, Sep. 2016.

[7] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in telecare medicine information systems," *J. Netw. Comput. Appl.*, vol. 87, pp. 1–19, Jun. 2017.

[8] N. R. Haddaway, M. J. Page, C. C. Pritchard, and L. A. McGuinness, "*PRISMA2020*: An R package and shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and open synthesis," *Campbell Syst. Rev.*, vol. 18, no. 2, Jun. 2022, Art. no. e1230.

[9] A. A. S. AlQahtani, H. Alamleh, and J. Gourd, "0EISUA: Zero effort indoor secure user authentication," *IEEE Access*, vol. 8, pp. 79069–79078, 2020.

[10] Y. Hong, "Design of intelligent access control system based on DES encrypted QR code," in *Proc. IEEE Int. Conf. Adv. Electr. Eng. Comput. Appl. (AEECA)*, Aug. 2020, pp. 1005–1008.

[11] M. Y. B. Ishak, S. B. Ahmad, and Z. Zulkifli, "IoT based Bluetooth smart radar door system via mobile apps," in *Proc. 1st Int. Conf. Artif. Intell. Data Sci. (AiDAS)*, Sep. 2019, pp. 142–145.

[12] K. Khreasarn and K. Hantrakul, "Automatic gate using Bluetooth technology (open the gate with the strength of the Bluetooth signal on the smartphone)," in *Proc. Int. Conf. Digit. Arts, Media Technol. (ICDAMT)*, Feb. 2018, pp. 54–58.

[13] A. S. Prabowo, M. A. Siregar, and J. Margolang, "Enhance a control method in the smart gate door based on sensor metal detector," *J. Phys., Conf. Ser.*, vol. 1361, Nov. 2019, Art. no. 012047.

[14] M. Shanthini, G. Vidya, and R. Arun, "IoT enhanced smart door locking system," in *Proc. 3rd Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Aug. 2020, pp. 92–96.

[15] Z. Mu, W. Li, C. Lou, and M. Liu, "Investigation and application of smart door locks based on Bluetooth control technology," in *Proc. Asia–Pacific Conf. Image Process., Electron. Comput. (IPEC)*, Apr. 2020, pp. 68–72.

[16] C. S. Okafor, C. U. Nnebe, T. L. Alumona, V. C. Onuzuluike, and U. C. Jideofor, "Door access control using RFID and voice recognition system," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 3, pp. 157–163, Mar. 2022.

[17] A. Zhang and R. V. P. Kandubai, "Access control schema for smart locks using a WiFi bridge: An exploration of a smart lock access control system based around the SimSim retrofitting smart lock," in *Proc. 6th Int. Conf. Robot. Artif. Intell.* New York, NY, USA: Association for Computing Machinery, Nov. 2020, pp. 174–178.

[18] C. K. Pappa, N. Ashokkumar, P. Nagarajan, and K. Thandapani, "Bluetooth based garage door opening system," in *Proc. 5th Int. Conf. Smart Syst. Inventive Technol. (ICSSIT)*, Jan. 2023, pp. 131–134.

[19] Y. J. Xin, W. Zhong, and L. Hong, "Smart gate system design and implementation based on cloud platform," *Proc. Comput. Sci.*, vol. 154, pp. 40–46, Jan. 2019.

[20] S. Kavde, R. Kavde, S. Bodare, and G. Bhagat, "Smart digital door lock system using Bluetooth technology," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2017, pp. 1–4.

[21] N. M. B. M. Noor and M. A. A. B. M. Zafie, "Smart gate using Android applications," *J. Phys., Conf. Ser.*, vol. 1755, no. 1, Feb. 2021, Art. no. 012003.

[22] S. Mukherjee and S. Mondal, "A scheme for QR code based smart door locks security system using an ARM computer," in *Proceedings of the First International Conference on Intelligent Computing and Communication*. 2017, pp. 613–621.

[23] M. N. H. A. Hassan, M. H. Jumali, and D. P. Dahnil, "Enhancement of access features for a gated system in a guarded community," in *Proc. IEEE Conf. Wireless Sensors (ICWiSe)*, Nov. 2019, pp. 24–28.

[24] L. Malina, P. Dzurenda, J. Hajny, and Z. Martinasek, "Secure and efficient two-factor zero-knowledge authentication solution for access control systems," *Comput. Secur.*, vol. 77, pp. 500–513, Aug. 2018.

[25] T. Sathishkuma, G. P. Rao, and P. Arumugam, "Verifying the authenticity of employees entering nuclear complex," in *Proc. IEEE 1st Int. Conf. Control, Meas. Instrum. (CMI)*, Jan. 2016, pp. 146–150.

[26] N. Prabhakaran, V. Srivaishnavi, V. Srinaya, T. Preethi, S. Aishwarya, and M. Dinesh, "Automatic gate control for highly secure organization using RFID and GSM technology," in *Proc. Int. Conf. Comput. Commun. Informat. (ICCCI)*, Jan. 2020, pp. 1–4.

[27] S. Binder, A. Iannone, and C. Leibner, "Biometric technology in 'no-gate border crossing solutions' under consideration of privacy, ethical, regulatory and social acceptance," *Multimedia Tools Appl.*, vol. 80, pp. 23665–23678, Jun. 2021.

[28] E. Noma-Osaghae, O. Robert, C. Okereke, O. J. Okesola, and K. Okokpujie, "Design and implementation of an iris biometric door access control system," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2017, pp. 590–593.

[29] V. A. Chastikova, S. A. Zherlitsyn, and Y. I. Volya, "Development of a personal identification technique for automation systems," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1047, no. 1, Feb. 2021, Art. no. 012138.

[30] J. Zhang and S. Jian, "Design and implementation of fingerprint access control system based on ZigBee wireless network," in *Proc. MATEC Web Conf.*, vol. 139, Dec. 2017, p. 192.

[31] J. Sang, H. Wang, Q. Qian, H. Wu, and Y. Chen, "An efficient fingerprint identification algorithm based on minutiae and invariant moment," *Pers. Ubiquitous Comput.*, vol. 22, no. 1, pp. 71–80, Feb. 2018.

[32] R. M. Sari, E. Sabna, R. Wahyuni, and Y. Irawan, "Implementation of open and close a housing gate portal using RFID card," *J. Robot. Control*, vol. 2, no. 5, pp. 363–367, 2021.

[33] Y.-P. Chen, Q.-H. Chen, K.-Y. Chou, and R.-H. Wu, "Low-cost face recognition system based on extended local binary pattern," in *Proc. Int. Autom. Control Conf. (CACS)*, Nov. 2016, pp. 13–18.

[34] V. E. Vyanza, C. Setianingsih, and B. Irawan, "Design of smart door system for live face recognition based on image processing using principal component analysis and template matching correlation methods," in *Proc. IEEE Asia–Pacific Conf. Wireless Mobile (APWiMob)*, Nov. 2017, pp. 23–29.

[35] H. Xiong, "Research on face recognition access control system in universities based on convolutional neural network," *J. Phys., Conf. Ser.*, vol. 1915, no. 2, May 2021, Art. no. 022045.

[36] S. A. Radzi, M. M. F. Alif, Y. N. Athirah, A. S. Jaafar, A. H. Norihan, and M. S. Saleha, "IoT based facial recognition door access control home security system using Raspberry Pi," *Int. J. Power Electron. Drive Syst.*, vol. 11, p. 417, Mar. 2020.

[37] S. Mehra, A. Khatri, P. Tanwar, and V. Khatri, "Intelligent embedded security control system for maternity ward based on IoT and face recognition," in *Proc. Int. Conf. Adv. Comput., Commun. Control Netw. (ICACCCN)*, Oct. 2018, pp. 49–53.

[38] M. Ziqiang and G. Zhang, "Data science in face recognition system based on BP neural network," *J. Phys., Conf. Ser.*, vol. 1881, no. 2, Apr. 2021, Art. no. 022029.

[39] G. Puvaneswari, M. Ramya, R. Kalaivani, and S. B. Ganesh, "Smart home security system using facial recognition," in *Proceedings of Third International Conference on Sustainable Expert Systems*. 2023, pp. 239–252.

[40] I. S. Hutomo and H. Wicaksono, "A smart door prototype with a face recognition capability," *IAES Int. J. Robot. Autom.*, vol. 11, pp. 1–9, Mar. 2022.

[41] H.-W. Lee, "Design of multi-functional access control system," *IEEE Access*, vol. 9, pp. 85255–85264, 2021.

[42] M. I. Younis and R. S. Muhammad, "IFRS: An indexed face recognition system based on face recognition and RFID technologies," *Wireless Pers. Commun.*, vol. 101, no. 4, pp. 1939–1966, Aug. 2018.

[43] H. Lee, S.-H. Park, J.-H. Yoo, S.-H. Jung, and J.-H. Huh, "Face recognition at a distance for a stand-alone access control system," *Sensors*, vol. 20, no. 3, p. 785, Jan. 2020.

[44] M. E. Beqqal, M. Azizi, and J. L. Lanet, "Multimodal access control system combining RFID, fingerprint and facial recognition," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 20, no. 1, p. 405, Oct. 2020.

[45] E. Lee, I. Lim, H. Kim, K. Ok, D. Kwon, D. An, and H. Ju, "Development of gate security system based on mash-up framework," in *Proc. 3rd Asian Conf. Defence Technol. (ACDT)*, Jan. 2017, pp. 70–74.

[46] G. Saadouli, M. I. Elburdani, R. M. Al-Qatouni, S. Kunhoth, and S. Al-Maadeed, "Automatic and secure electronic gate system using fusion of license plate, car make recognition and face detection," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 79–84.

[47] J.-R. Tan, W.-K. Chin, J.-J. Chin, and V.-T. Goh, "Seamless personnel authentication using facial recognition and identity-based identification on mobile devices," *Int. J. Recent Technol. Eng.*, vol. 8, pp. 41–46, Oct. 2019.

[48] K. N. Baluprithviraj, K. R. Bharathi, S. Chendhuran, and P. Lokeshwaran, "Artificial intelligence based smart door with face mask detection," in *Proc. Int. Conf. Artif. Intell. Smart Syst. (ICAIS)*, Mar. 2021, pp. 543–548.

[49] T. Dixit, S. S. Kaustub, K. R. Waris, A. Bellal, and R. Bharathi, "Face mask detection system for smart door," in *Proc. IEEE 7th Int. Conf. Converg. Technol. (I2CT)*, Apr. 2022, pp. 1–6.

[50] A. Gupta, S. Maurya, N. Mehra, and D. Kapil, "COVID-19: Employee fever detection with thermal camera integrated with attendance management system," in *Proc. 11th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2021, pp. 355–361.

[51] A. Duth, A. A. Nambiar, C. B. Teja, and S. Yadav, "Smart door system with COVID-19 risk factor evaluation, contactless data acquisition and sanitization," in *Proc. Int. Conf. Artif. Intell. Smart Syst. (ICAIS)*, Mar. 2021, pp. 1504–1511.

[52] D. Syrlybayev, N. Nauryz, A. Seisekulova, K. Yerzhanov, and M. H. Ali, "Smart door for COVID restricted areas," *Proc. Comput. Sci.*, vol. 201, pp. 478–486, Jan. 2022.

[53] Y. M. Reddy, M. Nadampalli, A. K. Panigrahy, K. S. Divyasree, A. Jahnavi, and N. A. Vignesh, "Automated facemask detection and monitoring of body temperature using IoT enabled smart door," in *Proc. 2nd Int. Conf. Artif. Intell. Signal Process. (AISP)*, Feb. 2022, pp. 1–8.

[54] D. Dasgupta, A. Roy, and A. Nag, "Multi-factor authentication," in *Advances in User Authentication*. 2017, pp. 185–233.

[55] J. R. Lewis, *Usability Testing*. Hoboken, NJ, USA: Wiley, Feb. 2006, pp. 1275–1316.

[56] G. Pirelli, "Usability in public services and border control: New technologies and challenges for people with disability," in *Proc. Symp. Austrian HCI Usability Eng. Group*, 2009, pp. 532–552.

[57] R. Zahra, A. Shehzadi, M. I. Sharif, A. Karim, S. Azam, F. D. Boer, M. Jonkman, and M. Mehmood, "Camera-based interactive wall display using hand gesture recognition," *Intell. Syst. with Appl.*, vol. 19, Sep. 2023, Art. no. 200262.

[58] N. Nedjah, R. S. Wyant, L. M. Mourelle, and B. B. Gupta, "Efficient yet robust biometric iris matching on smart cards for data high security and privacy," *Future Gener. Comput. Syst.*, vol. 76, pp. 18–32, Nov. 2017.
[59] S. Khan, W. Iqbal, A. Waheed, G. Mehmood, S. Khan, M. Zareei, and R. R. Biswal, "An efficient and secure revocation-enabled attribute-based access control for eHealth in smart society," *Sensors*, vol. 22, no. 1, p. 336, Jan. 2022.

ABDULLAH M. ALMUHAIDEB received the B.S. degree (Hons.) in computer information systems from King Faisal University, Saudi Arabia, in 2003, and the M.S. (Hons.) and Ph.D. degrees in network security from Monash University, Melbourne, Australia, in 2007 and 2013, respectively. He is currently an Associate Professor in information security, a Supervisor with the Saudi Aramco Cybersecurity Chair, and the Dean of the College of Computer Science and Information Technology, Imam Abdulrahman bin Faisal University, Saudi Arabia. He has published two patents and more than 45 scientific articles in journals and premier ACM/IEEE/Springer conferences. His research interests include mobile security, authentication and identification, and ubiquitous wireless access.

MARIAM ELHUSSEIN was born in Khartoum, Sudan, in 1980. She received the B.S. degree in computer science and the M.S. and Ph.D. degrees in informatics from the University of Reading, U.K., in 2014. Since 2016, she has been an Assistant Professor with the Department of Computer Information Systems, College of Computer Sciences and Information Technology, Imam Abdulrahman bin Faisal, Dammam, Saudi Arabia. Her research interests include social media analytics, health informatics, machine learning, and data mining of organizational data. She has led multiple research projects and has successfully published in IEEE/Elsevier/ACM/Springer journals and conferences. She has been a HEA Fellow, since 2020.

REEM OSMAN received the B.S. degree in computer science from Omdurman Ahlia University, in 2001, and the M.S. degree in computer science and information from the University of Gezira, in 2003. She has CCNA, MCSA, and MCP certificates. She is currently a Lecturer with the Applied College, Imam Abdulrahman bin Faisal University, Saudi Arabia. She has published three articles in Q1 and Q2 journals. Her research interests include social engineering-cyber awareness, network security, and mobile security.

FATEMA ALHOLYAL, photograph and biography not available at the time of publication.

LEENA ALGHAMDI, photograph and biography not available at the time of publication.

MAJD AL-ISMAIL, photograph and biography not available at the time of publication.

MARAM ALAWAMI, photograph and biography not available at the time of publication.

ZAINAB KADOUR, photograph and biography not available at the time of publication.

RACHID ZAGROUBA received the Ph.D. degree in computer science from the University of Rennes 1, France, in December 2007. He has been an Assistant Professor with Imam Abdulrahman bin Faisal University, Dammam, Saudi Arabia, since September 2015. He has been involved in several French-funded and IST FP6/7 European projects. He is a co-supervisor of several Ph.D. students and the supervisor of several master's students in the areas of computer networking, wireless sensor networks, wireless network security, and the IoT security.