Journal of Information Systems and Management Research
Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi

http://dergipark.gov.tr/jismar

Araştırma Makalesi / Research Article

Cyber Security Based Visitor Control System Design

Mehmet NACAROĞLU[*,a], Çiğdem TARHAN[b], Murat KOMESLİ[c], Vahap TECİM[d]

[a]*Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, İZMİR, 35400, TÜRKİYE*
[b]*Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü - Bölgesel Kalkınma ve İşletme Bilimleri Araştırma ve Uygulama Merkezi (DEÜ-BİMER), İZMİR, 35400, TÜRKİYE*
[c]*Yaşar Üniversitesi, Uygulamalı Bilimler Yüksekokulu, Yönetim Bilişim Sistemleri Bölümü, İZMİR, 35030, TÜRKİYE*
[d]*Dokuz Eylül Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, İZMİR, 35400, TÜRKİYE*

ARTICLE INFO

Received: 09.12.2023
Accepted: 29.04.2024

Keywords: *:*

Raspberry PI,
QR code,
visitor control systems,
cyber security

Corresponding Authors

e-posta:
wnacaroglu@ gmail.com

ABSTRACT

In this study, a cyber security-based visitor control system has been designed to maximize participant security in institutions, to prevent unauthorized access, and to easily control participants. The Visitor Control System has been developed using Raspberry Pi 3 and the information of the visitors who will participate is uploaded to the system along with their pictures. Within the scope of cyber security measures, the Visitor Entry Card, which is created with a QR code to prevent fake ID or entrance cards, is sent to the participants days before the dates of programs such as meetings, seminars, interviews, symposiums, workshops, briefings, fairs, and they are requested to enter with these cards. At the entrance points of the institutions, the visitors' Visitor Entry Card is questioned by the security guards and the QR code on the card is scanned with the help of the camera to confirm whether the visitor is authorized or not. After it is confirmed by the security personnel that it is the same as the person's photo, it is allowed to enter.

DOI: 10.59940/jismar.1402494

Siber Güvenlik Tabanlı Ziyaretçi Kontrol Sistemi Tasarımı

MAKALE BİLGİSİ

Alınma: 09.12.2023
Kabul: 29.04.2024

Anahtar Kelimeler
Raspberry PI
QR kod,
ziyaretçi kontrol
sistemleri,
siber güvenlik

Sorumlu Yazar
e-mail:
wnacaroglu@gmail.com

ÖZET

Bu çalışmada kurumlarda katılımcı güvenliğini en üst düzeye çıkarmak, yetkisiz erişimleri önlemek ve katılımcıların kolayca kontrol edilmesini sağlamak amacıyla siber güvenlik tabanlı bir ziyaretçi kontrol sistemi tasarlanmıştır. Ziyaretçi Kontrol Sistemi, Raspberry Pi 3 kullanılarak geliştirilmiş olup, katılım sağlayacak ziyaretçilerin bilgileri resimleriyle birlikte sisteme yüklenmektedir. Siber güvenlik tedbirleri kapsamında, sahte kimlik veya giriş kartlarının önlenmesi amacıyla QR kod ile oluşturulan Ziyaretçi Giriş Kartı, toplantı, seminer, söyleşi, sempozyum, çalıştay gibi programların tarihlerinden günler önce katılımcılara gönderilir ve brifinglere, fuarlara bu kartlarla girmeleri rica olunur. Kurumların giriş noktalarında ziyaretçilerin Ziyaretçi Giriş Kartı güvenlik görevlileri tarafından sorgulanmakta ve kart üzerinde yer alan QR kod kamera yardımıyla taranarak ziyaretçinin yetkili olup olmadığı teyit edilmektedir. Kişinin fotoğrafıyla aynı olduğu güvenlik personeli tarafından onaylandıktan sonra içeriye girişine izin verilmektedir.

DOI: 10.59940/jismar.1402494

1. INTRODUCTION *(GİRİŞ)*

With the rapid development of science and technology, computer technologies have become indispensable in many areas of life. By greatly affecting human life, the traditional habits of coming together physically have almost disappeared. Many gathering activities such as seminars, talks, symposiums, workshops, briefings, and fairs are held in different parts of the world [25]. In institutions where physical participation is needed due to reasons such as time becoming more valuable with the developing technology and epidemic diseases, these activities are alternatively carried out online. The reliability of participant/visitor access control systems has recently become a much more important criterion in cases where online participation is insufficient and physical participation is mandatory. As a result, the organizers apply many different security measures to prevent unauthorized participants to increase the security of the participants in organizations such as meetings, fairs, and seminars. Some of those; security guards, identity checks, fingerprint checks, entrance cards, tickets are measures to prevent unauthorized participation. However, the mentioned security measures always contain a security vulnerability in their content; for example, such as fake ticket, fake ID, fake fingerprint [26].

Institutions take cyber security measures to protect their systems against cyber-attacks. However, despite this, many institutions experience inadequacies in visitor control processes. Visitor control is the first step that creates the security barrier of the institution, and it is important to manage this process effectively. Traditional visitor registration systems can introduce security vulnerabilities and increase the risk of visitor data falling into malicious hands. Therefore, institutions need cyber security-based visitor control systems. On the other hand, personalized entrance cards created with quick-response (QR) code, where the security personnel do not know what the participants clearly write on, provide extra participant security. The QR code was developed by a Japanese company in 1994 and has survived until today. Besides being easy to use, QR codes have high data processing capability [1, 2]. It was originally developed in Japan for use in the automotive industry. When QR codes consisting of black dots and lines are read by the camera of a mobile device, direct access to the digital information source on the internet or stored on a server can be provided [3].

Within the scope of this study, a cyber security-based visitor control system was designed to maximize participant security in institutions, to prevent unauthorized access, and to easily control participants. The designed visitor control system was developed using the Raspberry Pi 3 hardware and Python as the programming language. The information of the visitors who will participate in the institutions are uploaded to the system with their pictures, and only a visitor entry card with a specially prepared QR code is given to the visitors. Security officers can determine whether the person is an authorized participant or not when the entrance card given to them at the entrance to the institutions is read into the system by the visitors/participants. The security guard allows the participant to pass by checking everything from the person's photo to other identifying personal information on the screen. When trying to enter with fake entrance cards prepared with QR code technology, the security personnel will not be allowed to enter the participant, since no photo is displayed with an unauthorized entry warning on the screen. Within the scope of cyber security measures, a possible cyber-attack, infiltration of the system, changing fake identity or visitor information, or generating fake QR code, etc. provides an advantage in preventing situations.

It has been stated that, due to the rapid development of information technologies in the world, the use of computers and the internet has become an indispensable element of life. However, they [13] stated that while the rapid spread of the Internet around the world provides great convenience and freedom to users, it also causes the systems to be misused due to the security vulnerabilities that arise. These vulnerabilities can target individuals or large systems. The devices communicating with each other, that is, the Internet of Things (IoT) and the unpredictable increase in the number of devices connected to the Internet, will bring about cyber security problems [13].

The concept of cyber is used to describe concepts or entities that include computers and networks. The word cyber space is also used to describe the abstract or concrete area where interconnected hardware, software, systems and people communicate and/or interact. The concept of Cyber Attack is defined as "planned and coordinated attacks on the information systems and critical infrastructures of targeted individuals, companies, institutions and states."

2. LITERATURE REVIEW *(LİTERATÜR TARAMASI)*

With the developing technology, embedded computers, in other words embedded systems, are used in many areas of life today. Embedded computers; in mobile devices, vehicles, bank ATMs, televisions, white goods, toys, printers, smart home systems, factories, workplaces, security points, etc. It

is configured and used in many places to serve every need.

Türk and Lüy [14] have stated that embedded systems are microprocessor-based computer hardware systems that perform a specific task independently or as part of a larger system and also have their own software. Embedded computers; GPU (Graphics Processing Unit) technology, digital signal processors, microcontrollers or application-specific integrated circuits, etc. used on systems.

The program strings used in embedded computers constitute the software architecture of the system. Since a simple industrial microcontroller is designed to perform specific tasks, tuning power consumption, size, reliability, and performance is extremely important. These basic devices are programmed through the machine code of the CPU (Central Process Unit). Their software is implemented with C, C++, Java or similar programming languages. Embedded computers often use interfaces or language platforms suitable for embedded use, along with real-time operating environments. Examples of these are Linux, Windows IoT and Embedded Java. However, to give an example of embedded computers, or in other words, simple programmable computers; Arduino or Raspberry Pi can be given as examples.

Arduino is a type of development board that appeals to many users, from the lowest level to the engineering level, with its simple and easily integrated coding language. Arduino is also a microcontroller platform with open source software and hardware. For example, using Arduino, you can read data from sensors and control electronic systems, turn on and off lights or start the engine according to this data.

Raspberry Pi, on the other hand, is a small, low-cost credit card-sized computer that can be attached to a monitor, television or special display, and uses a standard keyboard and mouse. Although it is similar to the Arduino system, it is a platform that appeals to users of all levels and allows them to learn programming in languages such as Scratch and Python. The microprocessor, RAM (Random Access Memory), GPIO (General purpose Input Output) pins and all the features required for a computer are built on a single circuit board PCB (Printed Circuit Board) on the Raspberry Pi. These types of computers are also called Single Board Computers (SBC). Unlike the computers we use in daily life, SBCs consume less power and have a smaller size. While Raspberry Pi performs most tasks that a normal computer can do, it also has the ability to program and control many different electronic systems via the GPIO pins on it.

Access control systems with different technologies are used wherever access security is needed. Among these technologies, password use, radio frequency identification (RFID) card use, magnetic card usage and biometric measures (fingerprint, iris scanner, retina scanner, voice recognition, face detection, etc.) are used very frequently today. Along with these, it is used in the QR code system, which has become very common in recent years. However, the QR code system is used not only for identity verification purposes, but also to respond to needs such as internet address, stock inquiry, sharing bank account information, use instead of business cards, address directions, electronic menu display in restaurants, etc. The reliability of these mentioned technologies against cyber-attacks, which is increasing day by day in the world, is becoming a more important issue. In this context, a literature review has been carried out for access control systems with different technologies currently used in the world.

Karaca [4] used RFID system to develop instant Personnel Tracking System. With the RFID system used, considering the entry-exit times and current location information of the personnel, considering the importance of security in secret gatherings with limited participants, increasing the security level by monitoring and intervening unauthorized participations, increasing the security level of the institutions / organizations by processing the current personnel attendance list. It is aimed to make it easy to follow up.

Mamak et al. [5] designed a face recognition-based personnel control and tracking system to track the time entry and exit processes of the personnel in the workplaces quickly, effectively, and accurately. In the developed system, the images of the personnel were taken by installing a camera system at the entrance and exit of the workplace. By identifying the facial regions of the personnel and matching the personnel, the images taken are identified by the fisherface, eigenface and local binary pattern histogram methods. The entry-exit data of the found personnel are displayed on the screen, and they are archived by being processed into the personnel personal database.

Genli [6] developed an application that will report the use of this card to the system as an alarm when the card holder wants to enter any room or section in the building and prevent entry to the room or passing through the turnstile. If there is no access authorization, the system is provided to generate an alarm directly.

Musayevave and Yahyayev [7], with regard to fingerprint recognition technology, defined that each

human hand has a different skin structure, there are indented protruding bumps on the skin of the fingertips, and the fingerprints left on the surfaces as a result of the contact of these raised structures. They stated that fingerprints in humans have unique and unchanging biometric measurements.

Özkaya and Sağıroğlu [8] have stated that the use of fingerprint technology in identity verification is very old. The Automatic Fingerprint Recognition System (OPTS) history is based on fingerprint ink. Although OPTS is known as a secure system, malicious people stated that they managed to imitate using finger patterns. On the other hand, they stated that it is possible to eliminate this problem with systems that check whether an imitated fingerprint pattern is a live real finger or not.

Noma-Osaghae et al. [9] stated that biometric authentication systems use unique physiological and behavioral features to limit access.

Wahyudi and Syazilawati [10] stated that secure buildings are protected against unauthorized access by various devices. They explained that although there are many types of devices such as PIN codes, both traditional and electronic keys, ID cards, cryptographic and binary control procedures, human voice can also be used to guarantee system security. They argued that the ability to authenticate a speaker by analyzing speech or speaker verification is an attractive and relatively inconspicuous way of providing security for entry to an important or safe place, that a person's voice cannot be stolen, lost, forgotten, unpredictable, or fully imitated.

4. CURRENT ACCESS CONTROL SYSTEMS IN INSTITUTIONS *(KURUMLARDAKİ MEVCUT GEÇİŞ KONTROL SİSTEMLERİ)*

There are different access control systems in use, such as fingerprint technology, card access systems, password access systems and barcode systems.

4.1. Fingerprint Technology Passage System *(Parmak İzi Teknolojisi Geçiş Sistemi)*

Nowadays, considering the cost, applications for different entry systems can be found in different areas. Businesses and individual measures provide faster and more effective entry-exit control compared to traditional systems by using many technological entry methods. Many security control systems are used successfully. One of the most commonly used ones is the fingerprint-based security control system. Fingerprint technology is basically used as a key in entry-exit systems for security purposes because fingerprints have specific properties. With to this feature, maximum security can be ensured. The process of using the fingerprint as a control tool in input-output systems with the Minutiae (Detail) Matching Algorithm [15], [16], [17].

Fingerprint recognition systems require special software to work. Fingerprint recognition algorithms form the basis of this software [27]. Algorithms form the basis of all software-based devices we use. Hardware and software work together in personnel fingerprint reader systems. The fingerprint reading device detects the fingerprint by scanning the finger. Then the algorithm, the software side, comes into play to match the fingerprint. When the fingerprint matches, the entry is confirmed and the lock is unlocked. To put it another way, the fingerprint is scanned. This scanning process is actually the process of taking photos. The camera and optics take a photo of the finger placed on the device. The process is completed electronically. Fingerprint algorithms transform this photograph into a special digital model. The indentations and protrusions in the trace are used to create the digital model. The resulting numerical model is compared with the database on the computer. If there is a match in the database, fingerprint verification is completed. This process can be applied in different areas such as personnel tracking system and door unlocking system [28].

As shown in Figure 1, the access systems with fingerprint technology, unauthorized access is prevented by using the password or card sharing method. On the other hand, fake fingerprints of authorized persons can be made using various techniques. In this way, unauthorized people can also pass through.

Figure 1. Fingerprint Reader Access System *(Parmak İzi Okuyucu Geçiş Sistemi)*

4.2. Card Access System *(Kartlı Geçiş Sistemi)*

Card access systems; These are systems that record the entry and exit times of individuals, employees, visitors or vehicles entering the parking lot by scanning the cards given to individuals and enabling the opening and closing of turnstiles, doors or barriers

[29]. Card access control systems are among the frequently preferred control systems for personnel tracking. These systems are also called access control system, access control system and access control system [30].

Baykara and Sherzad [18] defined RFID Card Entry Systems as a technique used to manage information and access for people or visitors who want to enter a place from the main door. Accordingly, the system they developed was designed as a web application connected to a database to maintain information on the movements of residents or visitors within a secure area to control entry before gaining access to any home. It provides a measure of security for building occupants and can help minimize the risk of unauthorized access, increase security, reduce theft and accidents, and secure sensitive information.

Card access control systems are considered the ancestors of personnel tracking systems. The card access systems, shown in Figure 2, used to keep personnel under control in institutions or businesses, to record entry and exit times, to ensure that only authorized people can access certain areas in businesses and to prevent anyone other than them from entering.

Card access control systems are very practical, convenient and low-cost. Additionally, certain people are allowed to pass through permitted areas safely through the authorization feature of card access systems [31].

Figure 2. Card Access System
(Kartlı Geçiş Sistemi)

However, the biggest disadvantage of card pass systems is that unauthorized entries occur as a result of voluntary or unintentional use of the cards of people authorized to pass to a certain region or area by other people, creating a security vulnerability [19].

4.3. Password Access System *(Şifre Geçiş Sistemi)*

Password access systems are systems that allow turnstiles and doors to be opened with the help of a password [32]. Coded access systems, which have hundreds of different models on the market as shown in Figure 3, are generally used at building entrances, office rooms, hospitals, especially at the entrances of surgery and intensive care units, elevators, warehouses, etc. It is used in places. The working principle of password-protected passage systems is that the user who wants to pass must know the correct password. When the user enters the correct password, the system completes the circuit in the lock system on its own electronic circuit, voltage is instantly sent to the lock system inside the door and the door is unlocked [20].

Kolekar et al. [21] designed password-based door entry systems using 8051 microcontroller. They stated that the system works on the principle that the numbers entered from a key panel match the password previously saved in the 2 Kilobyte memory. As a result of entering the correct password, the motor interface connected to the microcontroller was activated and the door was unlocked or closed by rotating the motor forward or backward.

With the developing technology in password access systems, password entry is now used as touch buttons or panels instead of buttons. It is also possible to pass with a magnetic card in touch coded pass systems [33].

However, the biggest disadvantage of this system is that if the password is disclosed, that is, if the password is given to an unauthorized person or if an authorized person learns the password by watching from behind while typing it, it will create a security vulnerability [34].

However, a thief or someone with malicious intent who has good electronic technical knowledge can easily remove the password panel if it is not mounted securely. Even if he does not know the password, he can easily open the door by connecting the cable from the power supply to the door lock in a way that short-circuits it.

Figure 3. Password Access System
(Şifre Geçiş Sistemi)

4.4. Barcode Access System *(Barkod Geçiş Sistemi)*

In our world where technology is developing very rapidly, the security lock and access systems we use in daily life have also been subject to many changes. Card access systems are used in every aspect of our daily lives. Currently, public institutions, buses, universities, hospitals, dining halls, entertainment centers, hotels, etc. Card access system technology is used in many places.

San Hlaing and San Lwin [22] stated that card access systems are systems that allow entry when some voltage electricity is applied to the RFID door lock mechanisms without the need for a lock and key.

This technology is known both in the past and today as an affordable and reliable solution for users. However, the pandemic epidemic that affected the whole world in the past years has forced us to use alternative systems to the conventional cards. For these reasons, lately, solutions that are both safe and do not require contact have been preferred, especially at access control points, in order to minimize physical contact in public areas.

With the development of technology, access systems that can read RFID cards and also scan QR codes or barcodes have begun to take their place in the market. Some security technology companies work with public institutions, buildings, businesses, etc. that have existing access control systems. In places, they are transforming into passage systems with QR or barcode technology shown in Figure 4, without damaging the existing infrastructure systems.

However, these systems, like card pass systems and cards with QR or barcode technology, are used voluntarily or unintentionally by other than their real owners, resulting in unauthorized passage, which creates a security vulnerability for the institutions and businesses in question [23].

Figure 4. Barcode Access System
(Barkodlu Geçiş Sistemi)

5. VISITOR CONTROL SYSTEM DESIGN AND IMPLEMENTATION *(ZİYARETÇİ KONTROL SİSTEMİ TASARIM VE UYGULAMASI)*

During the Visitor Control System design development process, the System Development Life Cycle steps shown in Fig.5 were followed [11].

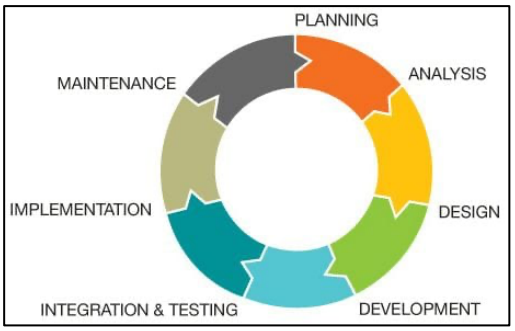

Figure 5. System development life cycle
(System development life cycle)

System Development Life Cycle consists of seven processes;

1. Defining Problems, Opportunities and Goals,
2. Determination of Information Requirements,
3. System Requirements Analysis,
4. Design of the Recommended System,
5. Software Development and Document Creation,
6. Testing and Maintaining the System,
7. Implementation and Evaluation of the System.

5.1. Defining Problems, Opportunities and Goals
(Problemlerin, Fırsatların ve Amaçların Tanımlanması)

It is known that cyber attacks targeting all information systems in the world can also damage exhibitor/visitor access control systems. If the cyber attacks in question affect the entrance control systems of the institutions, participant / visitor information can be changed and unregistered persons are also allowed to enter. Meeting, fair, seminar, interview, symposium, workshop, fair, etc. Since the security guards at the entrances of the buildings where the organizations are held have never seen or known the participants from different parts of the world, there is a possibility that they may make mistakes about whether they are real authorized participants or not.

It is aimed to upload the information of the visitors who will participate with the Visitor Control System, along with their pictures, to the system days in advance. In addition, participants/visitors can be provided with meetings, seminars, interviews, symposiums, workshops, briefings, fairs, etc. Within the scope of cyber security measures, within the scope of cyber security measures, Visitor Entry Cards with

their names on them, created with a QR code, were delivered to them and they were intended to enter with these cards.

In this way, the Visitor Entry Card of the participants is questioned by the security guards at the entrance points of the institutions through the Visitor Control System and it is aimed to confirm whether the visitor is an authorized/registered user by scanning the QR code on the card with the help of a camera. It is intended that the security personnel will be allowed to enter after the system confirms that the person's photo is exactly the same as the person's photo, that is, after double checking.

5.2. Determination of Information Requirements
(Bilgi Gereksinimlerinin Belirlenmesi)

While designing the Visitor Control System, access control systems currently used in institutions were examined. The operating principles, designs and security vulnerabilities of these systems have been identified in detail. The first of these systems to be examined is the encrypted access systems. Password pass systems are systems that allow passage by dialing a certain number of numbers in a correct order. However, it is not a very suitable system in terms of security. Because it is very easy for anyone who knows or obtains the password to gain access. Although it is low-cost, it is generally used in apartments, buildings, in-house doors, schools, hospitals, etc. It is used at the entrances of places.

When card access systems are examined, it is a system based on the principle that the door or turnstile opens when card holders bring the RFID-enabled card closer to the system. However, the biggest weakness of this system is that it allows an unauthorized person to access the system by scanning the card in case the card is given to someone else or if it is lost or stolen. Card pass system, just like the coded pass system, can be used in apartments, buildings, in-house doors, schools, hospitals, etc. It is used at the entrances of places.

Fingerprint reader access systems are one step ahead in terms of reliability compared to the mentioned password and card access systems. It is based on the principle that people physically identify their fingers to the system beforehand and then have their fingerprints read into the system if they want to pass through, and then the door or turnstile opens. Although it is better in terms of reliability than password or card access systems, fake fingerprints of people with access authorization can be imitated using various techniques. However, unauthorized persons may pass through.

Barcoded passage systems allow passage by scanning the ticket or card given to the participant/visitor into the system. However, when used alone, this system creates a security vulnerability by allowing unauthorized persons to pass in case the ticket is given to someone else or lost, as is the case with card pass systems.

While designing the Visitor Control System, the security vulnerabilities of the access control systems mentioned were examined and a system that could eliminate these vulnerabilities was developed. Within the scope of the system's information requirements, people's photographs and identity information are needed to upload real photographs of participants or visitors to the system days in advance. Within the framework of the photographs and information provided by the people, a Visitor Entry Card is prepared for the participant or visitor, which contains nothing but the QR code and the visitor's name. When the Visitor Entry Card is scanned into the system, the photo of the incoming participant/visitor is checked by the security guard, and if the photo displayed in the system matches the participant/visitor, passage is allowed, otherwise they are rejected. In this way, possible security vulnerabilities are prevented.

5.3. System Requirements Analysis
(Sistem İhtiyaçlarının Analizi)

When designing the Visitor Control System, the hardware and software required by the system differ from traditional access control systems. Traditional access control systems, which are widely available on the market, generally contain hard cards and embedded software. However, in the Visitor Control System design, it is planned to use Raspberry Pi, which has the same function as a computer but is very small in volume and size, Raspberry Pi LCD Touch Screen, Raspberry Pi Camera, power supply and Python programming language as software. The purpose of planning to use Raspberry Pi can be considered as its cost being much smaller in size and less than other computer-controlled or embedded systems.

The equipment used in the Visitor Control System are Raspberry Pi 3 (Fig.6), Raspberry Pi Camera (Fig.7), 16GB Micro SD Card, Raspberry Pi 7 inch LCD Touch Screen (Fig.7) and 2 x Power Adapters.

Figure 6. Raspery Pi 3 ands its camera
(Raspery Pi 3 ve kamerası)

Figure 7. Raspery Pi 7 inch LCD Touch Screen
(Raspery Pi 7 inç LCD dokunmatik ekran)

5.4. Design of the Recommended System
(Önerilen Sistemin Tasarımı)

During the Design process of the Recommended System, which is the fourth process of the System Development Life Cycle, the screens, cameras, etc. that make up the Visitor Control System. The operating system to be used was determined by assembling the hardware parts. The Visitor Control System Application is planned to be developed on the Raspberry Pi operating system using the Python programming language and the necessary libraries for the application.

There is a "QUERY" button on the Visitor Control System shown in Fig. 9. When the button is clicked, the QR Code on the Visitor Entry Card, shown as an example in Fig. 10, is scanned by the camera at the back of the system, and it is determined whether the visitor is authorized to participate by the system.

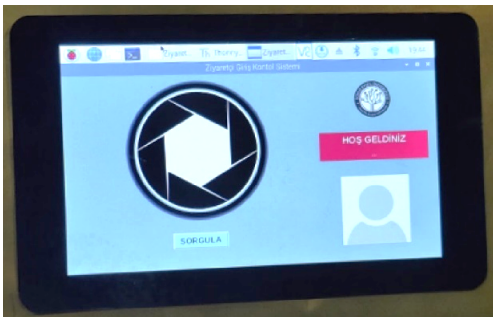

Figure 9. Visitor control system
(Ziyaretçi kontrol sistemi)

Figure 10. Visitor Entry Card Example
(Ziyaretçi kontrol kart örneği)

When the visitor shows the visitor entrance card with the QR code given to him before to the camera, it is shown in Fig. 11 together with the visitor's photo whether he is authorized or not. When the QR code is read with the Raspberry Pi camera in the application, if it is a registered participant, the message "ENTRY CONFIRMED" is displayed on the screen with the participant's name and surname on the Green Background as in Fig.11. Additionally, the photo of the participant previously uploaded to the system is shown, helping the visitor who wants to enter by the security guard to check over the photo.

On the other hand, when the Raspberry Pi camera reads the QR code, if it is not a registered participant, the message "INPUT NOT CONFIRMED" is displayed on the Red Background as in Fig. 12.

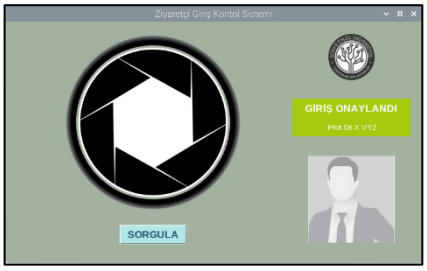

Figure 11. Screenshot of Visitor's Login Confirmation
(Ziyaretçi kontrol giriş onay ekran görüntüsü)

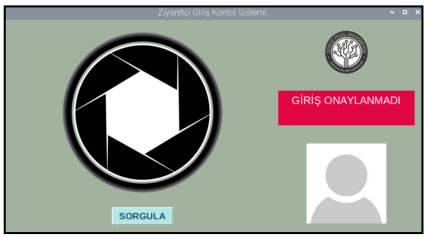

Figure 12. Screenshot of Visitor's Login Denial
(Ziyaretçi kontrol giriş ret ekran görüntüsü)

5.5. Software Development and Document Creation
(Yazılımın Geliştirilmesi ve Belge Oluşturulması)

Python programming language was used while developing the Visitor Control System application. In order for the codes and functions to be used in the design to work smoothly, the necessary libraries must be installed.

Raspbian Desktop Operating System (OS): Raspberry Pi does not come with an operating system inside. Therefore, to use Raspberry Pi, it needs to be installed an operating system. In this study, Raspian Desktop operating system was used for Raspberry Pi.

SD CardFormatter: Before printing the operating system on the SD card, it must be formatted. SD Card Formatter software is used for this.

Win32DiskImager: Win32DiskImager program is used to install Raspian Desktop operating system on the formatted SD card.

VNC Viewer: VNC Viewer program is used to remotely connect and control Raspberry Pi.

While developing the Visitor Control System application, Python programming language was used and the codes were tested online via the website https://snyk.io/code-checker/python/. Screenshots of the test and its results are shown in Figure 8.

As a result of the online test, it was determined that there was no security problem in the codes of the Visitor Control System Application. However, since the Visitor Control System Application is a system that works offline, it is a safe application against cyber attacks that can be made over the internet.

5.6. Testing and Maintaining the System
(Sistemin Test Edilmesi ve Sürdürülmesi)

After the software development process of the Visitor Control System application was completed, the system was tested. While testing the system, a few visitor photos and identification information were uploaded to the system as examples. Afterwards, the Visitor Entry Card with the QR code and participant/visitor information was scanned into the system. The information was checked by the QR code read by the system. As a result of the questioning, if the participant/visitor is registered or authorized, his/her photo is displayed to the security officer and his/her passage is approved. If the QR code is not registered or authorized as a result of the query, its entry is not approved and its passage is blocked.

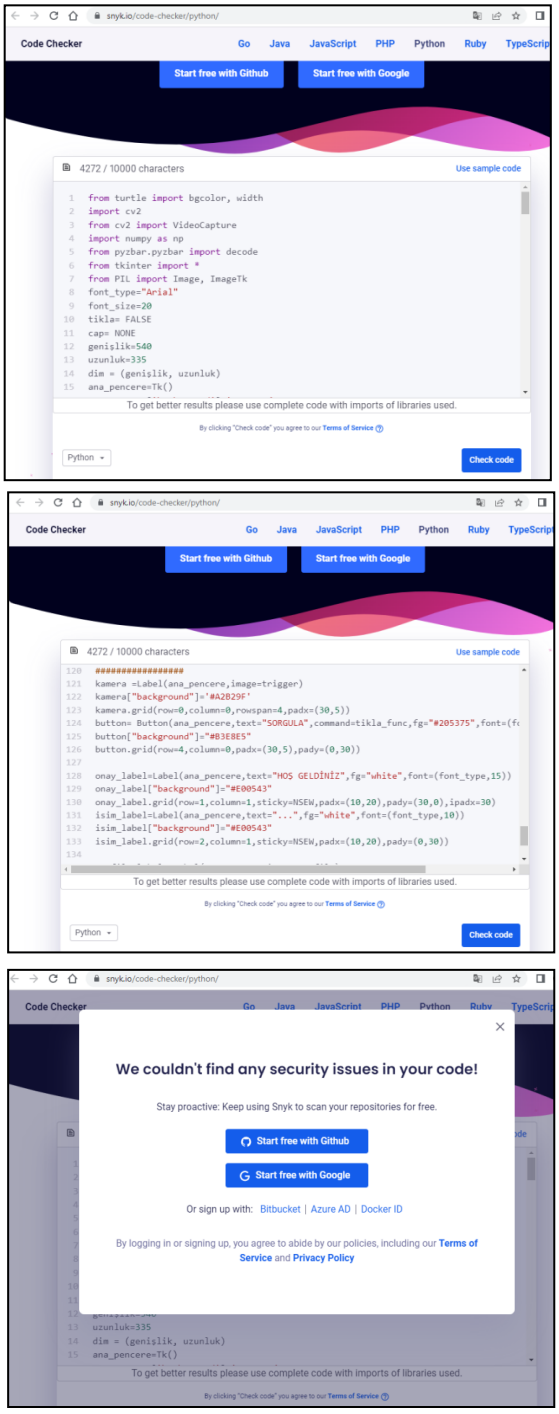

Figure 8. Test Result Screenshots of Application Codes *(Uygulama Kodlarının Test Sonucu Ekran Alıntıları)*

5.7. Implementation and Evaluation of the System
(Sistemin Test Edilmesi ve Sürdürülmesi)

The workflow for the visitor control system is presented in the Figure 13.

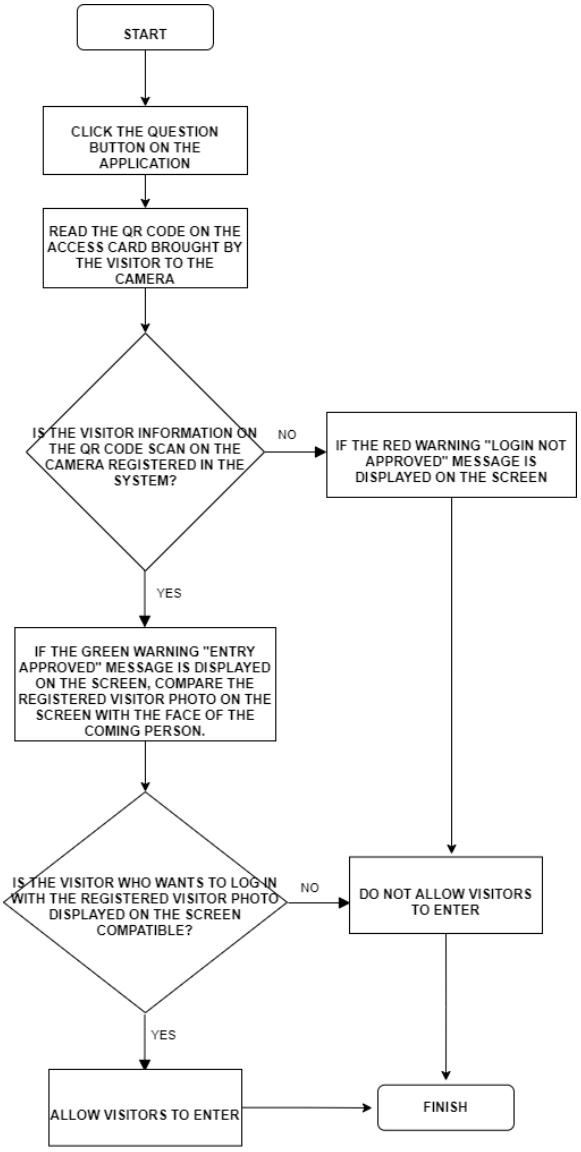

Figure 13. Workflow of Visitor Control System
(Ziyaretçi Kontrol Sistemi İş Akışı)

Visitor Control System can operate without being connected to any network or the internet. Thanks to its LCD Touch screen, it does not require any keyboard etc. It has been found that it can be used like a tablet without the need for hardware. Mobile power supplies, power banks, etc. are included in the system. It has been determined that when supported by devices, it has the ability to function in any environment without being exposed to power outages and cyber attacks.

5.8. Limitations *(Kısıtlar)*

In this study, the Visitor Control System Application was designed on the Raspberry Pi 3 board. It is not known whether the application will work on hardware or operating systems of other brands and perform the same functions. To give the simplest example of this from the Visitor Control System Application system, the developed application interface was developed in accordance with the Raspberry Pi 7 inch LCD Touch screen size (800 x 480 pixels). There is a possibility that the application interface may not work the same on different computers and screens and that there may be difficulties in using the system due to screen sizes.

Visitor Control System works with a Visitor Entry Card containing a QR code. The system works independently of the internet or any network. For this reason, it does not allow remote cyber attacks or remote modification of participant/visitor information. However, the reliability of the personnel who will upload photographs and identity information to the system is very critical. Because, as a result of the malevolent behavior of the personnel assigned to do these jobs, unwanted people will be able to pass, which may create a security vulnerability.

When the transition to the designed Visitor Control System is approved, the control of turnstile systems can also be integrated. This provides us with many opportunities to develop applications with the Raspberry Pi system. With the development of the system, statistics of participants/visitors who log in and records of people who are denied entry can be kept. In addition, the NFC feature of the new ID cards issued for use in Turkey can be integrated into the system and the participant/visitor security level can be increased to higher levels.

6. CONCLUSION AND DISCUSSION *(SONUÇ VE TARTIŞMA)*

The reliability of exhibitor / visitor access control systems in institutions has become a very important problem with the rapidly developing technology. When traditional visitor control systems are applied; In some cases, those who act in bad faith can use a fake ID, fake ticket, magnetic card belonging to someone else, shared password, etc. It is known that registered or unauthorized participants and visitors can log in with many different methods. This situation causes security gap in institutions. Today, it is known that cyber-attacks targeting all information systems in the world can also damage exhibitor / visitor access control systems. If the said cyber-attacks affect the access control systems in the institutions, the

participant/visitor information can be changed, and unregistered people are allowed to enter. Meeting, fair, seminar, conversation, symposium, workshop, fair etc. There is a possibility that the security guards at the entrances of the buildings where the organizations are held may make mistakes as to whether they are the real authorized participants since they have never seen and recognized the participants from different parts of the world.

In the study carried out within the scope of the study, it is aimed to develop a Visitor Control System to prevent these problems. While the Visitor Control System was being designed, the security vulnerabilities of the mentioned access control systems were examined, and a system was developed to eliminate these vulnerabilities. Within the scope of the information requirements of the system, the photos and identity information of the participants are required to upload the real photos of the participants or visitors to the system days before. Within the framework of the photos and information provided by the people, a Visitor Entry Card is prepared for the participant or visitor, which does not contain anything other than a QR code and the visitor's name. When the Visitor Entry card is scanned into the system, the participant/visitor's photo is checked by the security guard, and if the photo displayed in the system matches the participant/visitor, his/her pass is allowed, otherwise it is rejected. In this way, possible security vulnerabilities are prevented.

While testing the system, a few visitor photos and identity information were uploaded to the system as an example. Afterwards, the Visitor Entry Card containing the QR code and participant/visitor information was read into the system. The information was checked by the QR code read by the system. As a result of the inquiry, if the participant/visitor is registered or authorized, it was displayed to the security guard with his/her photograph and his/her pass was approved. If the QR code is not registered or authorized because of the question, its entry is not approved, and its passage is blocked. Visitor Control System can operate independently from any network or internet The LCD Touch screen can be used like a tablet without the need for hardware such as a keyboard. When mobile power supplies are supported by devices such as powerbanks, it can function in any desired environment without being exposed to power cuts and cyber-attacks.

The difference of the developed application compared to other security and transition systems is that it works offline and is not likely to be exposed to any cyber-attacks. Since the security guards do not know and see the participants at the entrance controls of the visitors before, they can make unauthorized entrances by malicious people with fake identities, apart from the real participants, and can engage in actions such as information spying, terrorist attacks, etc., according to their purposes. In this system, the information of the visitors is uploaded to the system by recording them together with their photos. Visitors are only given an entrance card with a QR code. In this way, it is almost impossible for an unauthorized user to log in, as the real photo and information of the person will be displayed when the QR code is scanned into the system, even if the ID is issued with fake photos.

There are access control systems produced by a wide variety of different companies in the market. However, these systems are not easy to maintain, requiring very high-cost annual maintenance contracts by companies. In addition, when a malfunction occurs in these systems in the following years, in cases where the company or the manufacturer cannot be reached, the system remains idle, and users must supply a new system. This situation has become a process that businesses and institutions do not want to encounter. Since the operating system used in Raspberry Pi, Raspberry Pi OS (formerly known as Raspbian), is a Linux-based operating system, Raspberry Pi was preferred when developing the Visitor Control System design and application because it is more stable than Windows and safer against cyber attacks.

Figure 14. Management Information Systems Pyramid *(Yönetim Bilişim Sistemleri Piramidi)*

Within the scope of this study, which is of interest to Management Information Systems, when the Management Information Systems Pyramid shown in Fig. 14 [24] is examined, the Cyber Security Based Visitor Control System in Institutions will play an active role in solving the problems that can be encountered from the lowest step of the pyramid to the top. Because when it comes to participant/visitor entrance security in institutions, it is a need that concerns everyone from the lowest employees to the highest-level managers.

However, if it is necessary to position this work exactly on the pyramid, the Cyber Security Based Visitor Control System in Institutions is within the scope of "Office Automation / Data Processing Systems", which is at the bottom of the Management Information Systems Pyramid. It is included in the scope of “Structural” within the scope of Problem Type, “Operational Decisions” in the scope of Decision Types and Operational Managers at the Managers level. However, when the Management Information Systems Pyramid is considered as a whole and an interrelated structure, it can easily see that all steps are needed.

REFERENCES *(KAYNAKLAR)*

[1] D. Hampton, A. Peach, and B. Rawlins, “Reaching Mobile Userswith QR Code,” *Kentucky Libraries*, vol. 75 (2), pp.6-10, 2011.

[2] X. Dou, and H. Li, “Creative Use of QR Codes in Consumer Communication,” *International Journal of Mobile Marketing*, Vol. 3, Issue 2, p. 61-67, 2008.

[3] N.-S. Chen, D. C.-E. Teng, and C. -H. Lee, “Augmenting Paper-Based Reading Activitieswith Mobile Technology to Enhance Reading Comprehension,”. in *The 6th IEEE Intenational Conference on Wireless*, DOI: 10.1109/WMUTE.2010.39, 2010.

[4] S. Karaca, “RFID teknolojisi ile anlık personel takip sistemi,” (Unpublished Master Thesis). İstanbul: Maltepe Üniversitesi, Fen Bilimleri Enstitüsü, 2010.

[5] U. Mamak, M. Z. Konyar, S. Solak, and M. H. Uçar, “Gerçek zamanlı yüz tanıma tabanlı personel kontrol ve takip sistemi tasarımı,”. *Avrupa Bilim ve Teknoloji Dergisi*, vol. (19), pp.497-504, 2020.

[6] M. M. Genli, “Bina Otomasyon Sistemleri,” (Unpublished Master Thesis), İstanbul: Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 2005.

[7] G. Musayeva, and M. Yahyayev, “Biyometrik Güvenlik Sistemleri,”, 2014.

[8] N. Özkaya, and Ş. Sağıroğlu, “Açık Anahtar altyapısı ve Biyometrik sistemler,” in *I. Ulusal Elektronik İmza Sempozyumu*, pp.283-290, Ankara, Türkiye, 2006.

[9] 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 *2017 International conference on computational science and computational intelligence (CSCI)*, pp. 590-593. IEEE, December 2017.

[10] W. A. Wahyudi, and M. Syazilawati, “Intelligent voice-based door Access control system using adaptive-network-based fuzzy inference systems (ANFIS) for building security,” *Journal of ComputerScience*, 3(5), 274-280, 2007.

[11] M. Dönerçark, and V. Tecim, “Kurumsal Karar Destek Sistemlerinde Yapay Zekâ Kullanımı: Tasarım ve Uygulama,” *Yönetim Bilişim Sistemleri Dergisi*, 6(2), 77-103, 2020.

[12] R. Rainer, “Introduction to information systems,” Hoboken, NJ: John Wiley and Sons, Inc. 2014.

[13] F. Aslay, “Siber saldırı yöntemleri ve Türkiye’nin siber güvenlik mevcut durum analizi,” *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24-28, 2017.

[14] F. Türk & M. Lüy, “Gömülü Sistemler ve Mühendislikte Uygulama Alanları,” *International Journal of Engineering Research & Development (IJERAD)*, 13(3), 2021.

[15] M. Merkepçi & M.S. Özyazıcı, “Parmak izine dayalı kapı kilit ve personel devam control sistemi,” in *Elektrik, Elektronik,Bilgisayar ve Biyomedikal Mühendislikleri Eğitim 4. Ulusal Sempozyumu*, 22-24 Ekim 2009, Eskişehir.

[16] M.K. Pehlivanoğlu & D.U.R.U. Nevcihan, “Üniversite Öğrencilerinin Devamlılığının Parmak İzi Okuyucu Cihaz Kullanılarak İzlenmesi,” *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 8(2), 9-16, 2016.

[17] A.B. Boydak, “İşyerlerinde Uygulanan Parmak İzli Giriş Kontrol Sistemine Hukuki Bakış,” *Türkiye Adalet Akademisi Dergisi*, (30), 321-336, 2017.

[18] M. Baykara & A. Sherzad, “Designing a securable smart home access control system using RFID cards,” *Journal of Network Communications and Emerging Technologies (JNCET)*, 10(12), 1-12, 2020.

[19] Komsek Elektronik Güvenlik Sistemleri Mühendislik İnşaat ve Reklam Tanıtım Hizmetleri Sanayi ve Ticaret Limited Şirketi. *Komsek Güvenlik Sistemleri, Kartlı Geçiş Sistemi Nedir ?* Available: https://www.komsek.com.tr/kartli-gecis-sistemi-nedir/. [Accessed: 14.05.2023].

[20] Perkotek Teknoloji Dış Tic. A.Ş. Şifreli Kapı ve Şifreli Kapı Kilidi. Available: https://www.perkotek.com/sifreli-kapi#:~:text=%C5%9Eifreli%20kap%C4%B1%20sistemleri%2C%20kap%C4%B1lar%C4%B1n%20kartlar,odalar%C4%B1nda%20da%20s%C4%B1k%C3%A7a%20tercih%20edilmektedir. [Accessed: 15.05.2023].

[21] S. D. Kolekar, V. B. Walekar, P. S. Patil, A. O. Mulani & A. D. Harale, "Password Based Door Lock System," *Int. J. of Aquatic Science*, 13(1), 494-501, 2022.

[22] N. N. San Hlaing & S. San Lwin, "Electronic door lock using RFID and password based on arduino," *International Journal of Trend in Scientific Research and Development*, 3(2), 799-802, 2019.

[23] BARFAŞ Otomasyon Teknolojileri Sanayi ve Ticaret Limited Şirketi. Kartlı Geçiş Sistemleri Tarihe Karışıyor, QR Geçiş Sistemleri Kolaylık ve Hız Sağlıyor. Available: https://www.barfas.com/blog-detay/kartli-gecis-sistemleri-tarihe-karisiyor-qr-gecis-sistemleri-kolaylik-ve-hiz-sagliyor. [Accessed: 26.05.2023].

[24] Tecim,V. (2023). Yönetim Bilişim Sistemleri (YBS). Available: https://vahaptecim.com.tr/yonetim-bilisim-sistemleri/, [Accessed: 12.06.2023].

[25] M. Oktaviandri & K. K. Foong. "Design and Development of Visitor Management System", *MEKATRONIKA*, vol. 1, no. 1, pp. 73–79, Jan. 2019.

[26] J. -J. Lin & S. -C. Huang. "The implementation of the visitor access control system for the senior citizen based on the LBP face recognition," *2017 International Conference on Fuzzy Theory and Its Applications (iFUZZY)*, Pingtung, Taiwan, 2017, pp. 1-6, doi: 10.1109/iFUZZY.2017.8311817.

[27] Alonso-Fernandez, F., Bigun, J., Fierrez, J., Fronthaler, H., Kollreider, K., Ortega-Garcia, J. "Fingerprint Recognition". In: Petrovska-Delacrétaz, D., Dorizzi, B., Chollet, G. (eds) *Guide to Biometric Reference Systems and Performance Evaluation*. Springer, London. https://doi.org/ 10.1007/978-1-84800-292-0_4. 2009.

[28] Cappelli, R., Maio, D., Maltoni, D., Wayman, J.L., Jain, A.K. "Performance evaluation of fingerprint verification systems," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 28(1), 3–18, 2006.

[29] R. Sanchez-Reillo & C. Sanchez-Avila. "Fingerprint verification using smart cards for access control systems," in *IEEE Aerospace and Electronic Systems Magazine*, vol. 17, no. 9, pp. 12-15, Sept. 2002, doi: 10.1109/MAES.2002.1039788.

[30] L. A Mohammed, Abdul Rahman Ramli, V. Prakash, and Mohamed B. Daud. "Smart Card Technology: Past, Present, and Future," *International Journal of The Computer, the Internet and Management* Vol. 12#1 (January – April, 2004) pp 12 – 22.

[31] Meng Zheng and Shi-Bao. "A common smart-card-based conditional access system for digital set-top boxes," in *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 601-605, May 2004, doi: 10.1109/TCE.2004.1309434.

[32] A. Conklin, G. Dietrich and D. Walz. "Password-based authentication: a system perspective," *37th Annual Hawaii International Conference on System Sciences*, 2004. Proceedings of the, Big Island, HI, USA, 2004, pp. 10 pp.-, doi: 10.1109/HICSS.2004.1265412.

[33] Ting-Yi Chang, Cheng-Jung Tsai, Jyun-Hao Lin. "A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices", *Journal of Systems and Software*, Volume 85, Issue 5, 2012, Pages 1157-1165, ISSN 0164-1212, https://doi.org/10.1016/j.jss.2011.12.044.

[34] Brumen, Boštjan. "*System-Assigned Passwords: The Disadvantages of the Strict Password Management Policies*". 1 Jan. 2020 : 459 – 479.