Designing a Securable Smart Home Access Control System using RFID Cards

Muhammet Baykara
Department of Software Engineering, College of Technology, Fırat University, Elazig, Turkey
mbaykara@firat.edu.tr

Sherzad Abdullah
Department of Software Engineering, College of Technology, Fırat University, Elazig, Turkey
sherzad80@hotmail.com

Published online: 30 December 2020

Abstract – The RFID Card Entry System describes a technique used to manage information and access for persons or visitors wishing to gain entrance through the main gate into a city house. This system has been designed as a web application connected to a database to maintain information regarding residents' or visitors' movement within a secured area to control entrance through the main gate before providing access to an individual house. It provides a security measure for the residents and can help minimize the risk of unauthorized access, increase safety, reduce theft and accidents, and secure sensitive information. The system can equally be used to control movement within a commercial organization. This study includes web application security clues and systems to prevent attackers from reaching highly classified information. This system is highly significant for controlling entrance through the main gate before providing access to an individual house, preventing the hackers from breaking through the security of the web application, and guaranteeing confidential data protection. This study's issue is that hackers/Intruders can easily penetrate any web application security via SQL injection (SQLI), brute force attack, cross-site scripting (XSS), and session hijacking. A brute-force attack in the web application is set to encrypt sensitive data such as username, password, and RFID card number. Therefore, to solve this problem and make the security of the database robust tremendously, the encryption of sensitive data must be utilized by advanced encryption standard (AES) algorithm, strong password policy, google captcha, prevent SQLI, reflect XSS, session hijacking. This system ensured that it could prevent those who intend to enter the main gate, lowers the hacking risk, and keep the data protected. The results also demonstrate that the proposed approach is straightforward and compelling to secure unauthorized procedures on electronic case data by encrypting classified information, which results in more powerful authentication to simplify the procedure of web application. Moreover, it helps web developers ignore and reduce the web application's high risks to minimize broken authentication risks and avoid leaving the login page.

Index Terms – Security, Database Security, Web Application, Security, RFID, Smart Home.

1. INTRODUCTION

Applications that are accessed using a web browser over a network and developed using web languages such as HTML5, Bootstrap, CSS3, JavaScript, and PHP are called web applications [1]. In today's world, web applications provide a range of facilities like e-school, e-governance, access control system, online shopping, and etc. Security is an important aspect in the design of web applications. When planning to store critical or sensitive data in your web application, such as username, password, RFID card number, several security techniques need to be implemented, including strong cryptography, detection, SQL injection prevention, and mitigation of cross-site scripting attacks. Cryptography is also a popular significant, and mainstream procedure to ensure that information is protected from attackers.

Encryption is a method of encoding information so that it is unreadable without a cryptographic key. This mechanism converts plaintext into an incomprehensible configuration known as ciphertext. Decrypting is the procedure that changes ciphertext back into plaintext. Current cryptography gives confidentiality, prevention, and verification [1]. There are currently several cryptographic techniques [2], with AES being the current industry standard [3].

1.1. Database Security

A database can be defined as a set of data stored on a computer system's hard disk. It allows any authorized user to view, quickly and easily access, enter, and analyze data. It is a set of tables, views, and queries [4]. The database user interface is called a database management system (DBMS). It helps to organize information by keeping indices for improved performance and quick retrieval. In a modern place of employment, a database can provide speed and efficiency.

Databases today face a different kind of attacks, and it is better to identify the attacks on the databases that can be carried out to have secure databases. We may classify the major database attacks such as SQL injection, brute force attack, cross-site scripting (XSS), session hijacking, weak authentication, and unmanaged sensitive data.

Database security is a set of aggregated measures required to protect and secure the database from internal and external threats and is one of the most significant concerns all over the DBMS [5]. It helps organizations to keep their databases safe and enables them to minimize their vulnerabilities while increasing the protection of their databases. Furthermore, utilizing some database security methods to protect SQLI, XSS, brute force attack and session hijacking, encrypting sensitive data, and using strong password policy.

In the modern world, database security is one of its most critical and daunting tasks that people face in every area of their lives around the world. Databases are complex, and the threats and safety problems connected with various databases are not fully understood by many database security practitioners [4].

The security utilizes various kinds of controls such as administrative, physical, and technical checks. Likewise, security has quality ingredients in the world of electronics. The security of databases is the privacy of personal data kept on a server. Several security levels, such as database and system administrator, developers, security officer, are included in a database [6], and an intruder could compromise safety in either of these layers.

Organizations have to protect and secure the databases from purposeful cybersecurity assaults and the spoil of information and database from the individuals who can get into them easily. Additionally, legitimate and sufficient database security is tremendously significant and required.

In many web applications, input information is taken from clients, and comparing SQL questions is executed on the server-side to bring or store appropriate information in the database [7]. Also, hackers insert malicious SQL codes in the input parameter using different methods, including retrieving data in the form of errors, conditions, and time. Conceptually, security threats can be divided into two primary categories of attacks: active and passive attacks, where the attacker gains unauthorized access to the system's resources.

The different types of SQLI are going on when client input isn't filtered to set up a getaway character and afterward passed them into a proclamation of SQL to the server. This problem utilizing a possible method for control of the SQL statement is, for the most part, conducted on the objective database legitimately by the end-client of the program. Moreover, web application SQL injection vulnerabilities are split into three levels. According to the complexity of detecting the leak, as seen below [8]:

- SQLI dependent on 1=1 is always true

To make a client avoid entering "incorrect" input, the client can enter some shrewd input this way: TxUserID: 12 OR 1=1; at that point, the SQL statement will look like this:

*SELECT * FROM Musers where TxUserID = 12 OR 1=1;*

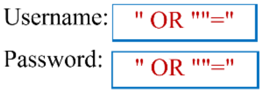
The SQL command above is valid and will restore all lines from the "Musers" table since OR 1=1 is, in every case, valid. Additionally, a hacker may gain access to all the client names and passwords in the database by inserting 12 OR 1=1 into the input field.

- SQLI dependent on ""="" is always true

The server takes the username and secret word to execute the accompanying SQL inquiry in the database when a client login on a site: username: sherzad80@hotmail.com and secret word: PassAcs#20.

*SELECT * FROM Musers where useremail= "sherzad80@hotmail.com" AND Password ="PassAcs#20";*

The attacker may gain access to usernames and passwords in a powerful web application by basically entering “OR ""=" into the usernames or secret word text box:



Username: " OR ""="
Password: " OR ""="

The code on the server will execute the following query:

*SELECT * FROM Musers where useremail="" or ""="" AND userpassword ="" or ""="";*

In the above example is valid and will restore all records from the "Musers" where, OR ""="" is always true.

- SQLI dependent on batched SQL statements

A bunch of SQL statements is a group of at least two or three SQL statements, isolated by semicolons. The SQL proclamation underneath will recover all lines from the "Musers" table and then remove the "accommodation" table.

*SELECT * FROM Musers; DROP TABLE accommodation;*

At the point when client id: 12; DROP TABLE accommodation. The up to date SQL statement would be as the following:

*SELECT * FROM Musers where MUserID= 12; DROP TABLE accommodation;*

$Userexpecteddata = 12;

*SELECT * FROM Musers where uid=$Userexpecteddata;*

To produce a malicious series

*SELECT * FROM Musers where uid=12; DROP TABLE Musers;*

Figure 1 shows a working diagram of SQL injection.

Cross-Site Scripting (XSS) operates by manipulating an insecure website to return the malicious script to clients. When the unauthorized code is executed within the victim's browser, the hacker will compromise its interplay with the application to the complete. Three key categories of XSS attacks exist:

• Avoid XSS from the current HTTP request where the malicious script originates.

• Stored XSS where the malware script creates from the web application;

• DOM based XSS, where client-side code is vulnerable instead of server-side code;

Example for prevent XSS vulnerability:

https://insecure-acs.com/level?msg= control entrance+ through the + main gate.

<p> level: control entrance through the main gate. </p>

Therefore, no processing of the data is done by the application, so an attacker can easily create an attack like this:

https://insecure- acs.com/level?msg=<script>/+ wrong +data+ in this place. + */ </script>*

<p>level: <script>/ wrong data in this place. */</script></p>*

An example of a stored XSS vulnerability. An application for a message board enables users to send messages that are shown to other users:

<p>Hi, my project is very interest!</p>

Here, no other data processing is carried out by the application, so an attacker can send a message that targets other users easily:

<p><script>/ wrong data in this place. */</script></p>*

An application, for example, uses JS code to read the textbox from an input field and write the value to a component in HTML:

var find = document.getElementById('Find').value; var output1 = document.getElementById('output1'); results.innerHTML = 'You finded for: ' + find;

If the attacker is able to manipulate the input field value, they can easily create a malicious value that causes them to execute their own script:

You look for: <img src=1 onerror='/ Poor employee here ...*/'>*

In a typical case, the input field, such as the URL query string parameter, will be filled from the request message section. It allows an attacker to execute an attack using a malicious Website in the same way as the reflected XSS.

Most of the web application databases contain three layers: the backend layer is a database server, the frontend layer is the client browser/server, and the middle layer covers most of the applications. It is enhanced more often by a web server-side scripting language such as PHP [9]. Figure 2 shows a working diagram of a web application server.

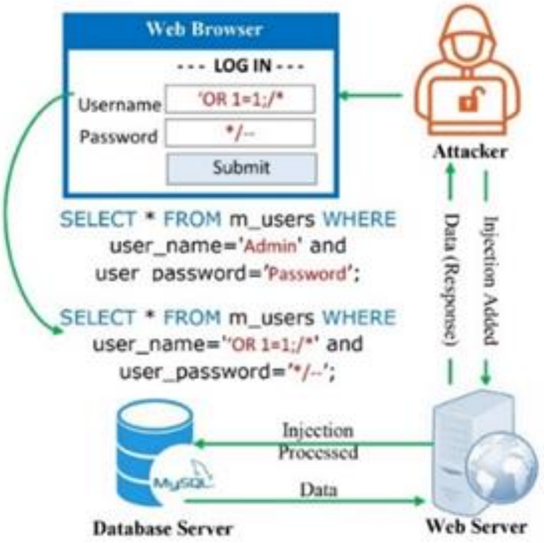


Figure 1 Working SQL Injection

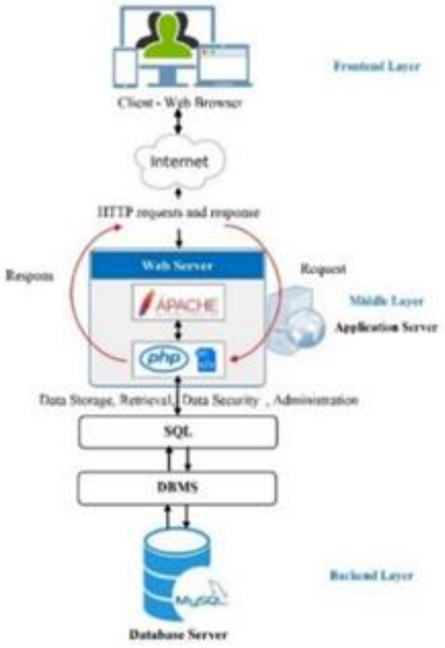


Figure 2 Web Application Server

1.2. Brute Force Attack

Brute force attack is a very well-known act among the intruders. It is an action that includes sequential and progressive endeavors of attempting different secret key combinations to break into any site. This endeavor is done enthusiastically by hackers who additionally utilize bots. They have been installed malignantly in different PCs to support the computing power needed to run such assaults. The general idea is good here, but you need to make yourself more transparent and precise [10].

Moreover, a brute force attack is an endeavor to beak a password or username or find a secret web page or the key utilized to encrypt a message, using a trial and glitch approach to anticipate properly. It is an old assault strategy, but it's still valid and well-known with hackers. For example, brute force attacks are regularly utilized to attack authentication and uncover secret content/pages inside a web application. These assaults are commonly sent through GET and POST requests to the server about authentication. Brute force attacks are frequently mounted when a record lockout strategy is not set up.

The purpose of a brute force attack is to obtain access to a resource that is otherwise limited to other users. It can be an administrative account, a password-protected site, or a specified website to list valid emails. Also, to access a legitimate account can mean compromising the entire platform that can be used by bad actors as part of their websites that are compromised. To avoid brute force attacks, there are several ways.

- Advanced Encryption Standard (AES)

One of the most popular and commonly symmetrical block cipher algorithms is the advanced encryption standard (AES) algorithm, trusted and unbreakable of the future used worldwide. It was originally named Rijndael that was published by the National Institute of Standards and Technology (NIST) of the United States of America in 2000 [11]. AES is typically considered invulnerable to all attacks, except brute force, which threatens to decode messages in the 128, 192, or 256-bit cipher using all possible combinations for heavy-duty encryption purposes [12]. It is the cryptographic algorithm used to encrypt electronic data that is FIPS-approved.

Another AES solution is a block cipher, an algorithm that records information on a per-block basis. Each block's size is typically measured in bits. E.g., the 128 bits (AES) are long, which means that AES will produce 128 bits of ciphertext on 128 bits of plaintext. The use of keys during encryption and decryption processes are required by almost all modern encryption algorithms (AES). It provides three keys of different lengths: 128-bit, 192-bit, and 256-bit keys. The lengthier the key, the better the encryption. AES 128 encryption is, therefore, the least efficient, while the strongest is AES 256 encryption. Therefore, each round's encryption process follows four steps, such as sub bytes, row change, column mix, and round key add. Each round inverse follows four steps for the decryption procedure, too.

- Strong Password Policy

Each web application should implement the use of strong passwords. Standard accounts for users needed to make at least eight characters in length consists of numbers, contain both upper and lowercase alphabetic and special characters until to secure the strong password from the hackers when the attacker tries to break the password [13].

Hence, a strong password is the easiest way to stop hackers from getting inside or attempt from users, do not forget some tips to create a strong password such as do not use personal information when creating a password, create unique passwords for each account, never write them down, change passwords frequently, never share, beef up computer security and do not click on checkbox remember password in the internet browser.

- google reCaptcha

Captcha is now widely used on websites. Bots prevent automated scripts from being executed, which are primarily used in brute force attacks. It is a good and highly efficient method of stopping bots and automated tools from performing website acts by offering them obstacles before they can even log in. The attacker uses automated programs to quicken the injection process. We are using re-captcha to solve this problem [14].

- Session Hijacking

Session hijacking is a type of attack on any user session running on an internet network connection. The user already remains logged into the active session of his profile or account. It helps protect the users as they have to create a new session to access the server.

It also stops session hijacking that creates a function, calls the function, and starts the header session on every page. It is also used to check it when every user wants to log in to the system requiring checking it before accessing it. If the session ID is valid, they will be able to log in, but if the session ID of the user is not valid, it will redirect the user to the page login.

Measures should be conducted by both the client and server sides to protect against session hijacking. Some other ways to prevent session hijacking are empowering the client-side protection as suggested by taking preventive measures for the session hijacking on the client-side. Users should have good antivirus and anti-malware applications, and the software should be kept up to date. Apart from monitoring the IP address and SSL session ID, the engines also monitor HTTP headers. Each header adjustment adds penalty points to the session, and as soon as the points reach a certain amount, the session gets terminated. This cap is configurable. It is reliable because it will have a different HTTP header order when an intrusion happens.

Most TCP connections use HTTP to communicate, so each link's unique identifier is necessary for every server. A session is a unique identifier created to identify the current interaction session stored in a cookie by a server sent to a client. For the identification of a specific client, a cookie is a short text file.

Data is transmitted over HTTPP since cookies on the PC. Session hijacking requires stealing the user's login information and using the information later to act as the user. The hijacking attack is hazardous from the security perspective [15]. To prevent session hijacking, one can use every page's header method to reduce the risk.

The best benefit of a session hijacking is that the malicious attacker can reach the server and access its data without registering it. Besides, to help him hack it in the future or simplify a data-stealing process, he may also change the server. Most methods of session hijacking concentrate on two aspects: the session ID and the sequence number of the session.

1.3. SQL Injection Attacks (SQLIA)

Currently, SQLI is recorded as one of the main and top 10 vulnerabilities to web applications between 2007-2010, which is certified by the open web application security (OWAS) [16]. It is a type of attack used by web application hackers. The attacker can access the database data via the internet to modify SQL statements using SQL code with a web form user input box to obtain unauthorized access to data from the website database server. It is also a backend database tool used by hackers to insert malicious SQL codes or input data from the client to the server to gain control of a web application. Also, a good SQL injection exploit can read sensitive database information [17].

1.4. Cross-Site Scripting (XSS)

It is a sort of injection that injects malicious scripts into otherwise benign and trustworthy websites and is unarguably the common reason for the demise of web applications. Besides, a hacker works by crafting a malicious URL into the browser to compromise the application's security. Eighty-two percent of vulnerabilities were located in the application code. XSS enables malicious code to be injected into the user script of pages viewed by other users [18].

2. RELATED WORK

This section reviews the literature on the database, requirements, and design of the ACS using ID cards. The access control was a security technique designed to provide rapid and convenient access for to the authorized person, saving the organizations while restricting access for unauthorized people, but other businesses that experience a lot of foot traffic from visitors or clients [19].

The previous research SHA-1, MD5, and SALT used algorithms. Each of them was used separately to encrypt sensitive data such as usernames and passwords. These algorithms are still straightforward and weak to be decrypted by hackers [20] using strong cryptography to encrypt sensitive information and prevent cyber-attacks compared to our research using the AES algorithm. It is a highly reliable, faster, and more efficient encryption algorithm. Due to its great skill, this algorithm is widely used [21].

According to previous studies, the microcontroller gathers data from sensors. All the data is stored in a text format on a memory SD-card. The text file will be kept on the SD card for a week or longer. After that, the machine deletes all the information and begins storing new information.[22]. Compared to this paper, using ESP32 connects to the RFID reader directly and saves more data in the MYSQL database than a text file.

RFID technology has yielded numerous benefits and advantages, making the library management processes efficient, saving time and workload of administrating users such as contactless payment, inventory control, shipment tracking, etc. Also, the exultation of RFID technology in libraries in a developed country such as India, for instance, has brought a substantial improvement in services like recharging itself materials handling, security, fast-moving stock storage, and turned them into safety tracking systems that combine safety with useful material tracking across the library, decreasing the data input mistake, enhanced client service, and updates [23]. On the other hand, RFID technology is used in various area such as enhanced self-checking in libraries, check-out, monitoring, shelf charging/discharge, reliability, fast inventory, and automated material handling [24].

In our study, it is used to secure any residential places. It can also be changed to a manual system, helping secure all the cities' gates and safe time to save, process, and retrieve. Hence, in this system, all users are identified according to their status: number one is used for resident users, number two is used for visitors, number three is used for shipment tracking, and number four is used for urgent statuses. Furthermore, you may add more statuses separately to control the data according to the system.

All the residents of this venue who have given RFID card can use it to enter the main gate of the city, but when other users such as visitors or shipment tracking trying to enter, they should send their full name, mobile number, and the timing of the visit to the resident’s portals. The information will be available to the checkpoints of the cities. But, urgent visitors should be made an RFID card by an administrator of the system entailing all the needed information allowing him or her to enter the city.

RFID systems have become famous for automated applications in the identification and supply chains. Additionally, in supply chain applications, the RFID tag is expected to replace the barcode. However, this system introduces new problems such as the invasion of user privacy and unnecessary access to information. While the RFID tag allows for more efficient supply chain management, it may also allow access to credit information and buying patterns without their consent.

ACS can be used to strengthen overall security while reducing the time-consuming control of access for a large number of candidates. Technologies that are widely used are RFID and smart cards. RFID ensures simultaneous reading of defined objects, and smart cards provide storage space and allow information processing.

A client-recognizing framework is created utilizing an RFID innovation to register, monitor, and control an access pass for security purposes. The framework performance shows validated and successful information records [25].

The study is intended to start preparing the correct models and designs for the RFID system, including domain models, requirements, business process models, and client interfaces, based on an access control framework and its architecture [26]. This paper study analyzes gate control engineering systems' works using an RFID card. It aims to an impenetrable protection system, especially in medicine, documents, and other valuable objects, and obligatory is within higher intelligence [27]. The main reason of the study is why the protocol design is not robust and why the protocol correctness cannot be guaranteed.

This paper work to layout and boost a clever garage system using a microcontroller with cloud-connected sensors through IoT units the system developed is a prototype designed with Arduino NodeMCUs to display the proposed framework [28].

Database security guarantees the secrecy, respectability, and accessibility of an association's databases. The protection of databases requires the usage of a wide range of security information measures to securing databases. Database management technology has gained worldwide popularity because of the heavy dependence on online record maintenance. Almost every business area such as finance, transport, education, culture, healthcare, etc. use the database technology. Built-in web applications with monitoring and validation techniques for privileged database access use PHP and MySQL [33].

The improved HTML material contains a malicious vector targeting web-related threats. Attacks by XSS are direct. PHP programming is essential for safety, and PHP provides a few tools to test database questions and the HTML display. The obligation requires to close the site to protect the cross-site scripting or SQL injection ambushes [29].

2.1. Microcontroller

The ESP32 NodeMCU is a low- power and cost system powered by the double-core Tensilica Xtensa LX6 microprocessor [30] microcontrollers Bluetooth and Wi-Fi abilities. Because of the platform's cost-effectiveness, the RFID program's usage for protection purposes is becoming increasingly widespread. The system combines Arduino UNO and RFID technologies. The initial design of the electronic circuit was carried out using the Proteus software. RFID and Arduino have serial communication links [31]. It gathers data from sensors and stores the data on the memory SD-card in a text format. The text file is stored on the memory SD card for a week after the system, and new data erase all the information recorded [22] [32]. Figure 3 shows the connection between microcontroller and a servo motor.

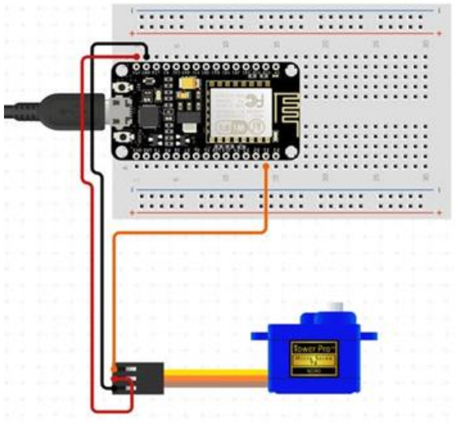


Figure 3 Connected Microcontroller with a Servo Motor

RFID technology was used the access control system because RFID technology facilitates data transformation and vastly reduces human effort and error. Radio waves are used to pass data to a reader from the tag.

2.2. Servo Motor

A servo motor is an electric device that can precisely move or rotate an object. If an object needs to be rotated at a certain angle or distance, then a servo motor is required. An electrical pulse decides the position of a servo motor and positions its circuit next to the motor. It is a machine containing an encoder that transforms the mechanical motion (shaft turns) into digital pulses that a motion controller interprets. It also involves a driver, and together they make up a circuit that regulates the position, torque, and velocity. It also receives data from the ultrasonic sensor. If the data is valid, the gate will be open. If not, the gate will remain closed while the servo motor is connected to the chip microcontroller (ESP32).

2.3. Ultrasonic Sensor

The sensor is a device, module, machine whose reason for existing is to detects and responds to some contribution from the physical condition and send the data to different hardware. It operates by transmitting sound waves at frequencies that are too high to be detected by humans. It then waits to observe the sound reflected, measuring the distance based on the required time. It is similar to how radar tests the time it takes for a radio wave to return after it reaches an object. Many embedded systems exist to gather information from the sensors. The microcontroller profound rest abilities to save power, and it is wakeful just when we have to take reading.

2.4. Problem Statement

Security is a serious problem, especially for the residents and foreigners who live in city houses. Due to the increase of crimes, these buildings' security protocols are paramount to create safe and better life protection for residents. DBMS's major attacks can be categorized: SQL injection, cross-site scripting (XSS), brute force attack, session hijacking, weak authentication, and unmanaged sensitive data.

Generally, the manual system is slow because all users do not identify and do not utilize RFID cards when residents or visitors wish to check-in and check-out needed signature. It increases size, loses data, and searching for the person's or visitors' names take a long time. The manual system of each person needs authentication to enter the workplace or building. These people's full should be registered on the list, mobile number, date, and time of visit. Also, registration of the plate number of many cars will be done manually. Furthermore, using notification in the manual system was considered a complicated process in renewing or extending the cards because it needed to inform the administrator.

2.5. Objectives

These studies aim to provide a solution to the problem in the existing system, to create a new system that will help city houses to facilitate the entry of residents, visitors through the main gate, and to help find any accidents in the area with information recorded about everyone who has checked-in. This system can also help speed the entrance process, ensuring that people do not need to stand in long queues and wait to be checked by a control officer.

This study utilizes a security system for residential buildings or workplace entrances that use ACS and implement security measures to prevent unauthorized access. And it aims to protect data privacy, and to improve a secured web application by using some methods such as preventing SQLI, XSS, and brute force attack, encrypting sensitive data, stopping session hijacking and using strong password policy.

3. PORPOSED MODELLING

- In this study we implemented a security system for residential building or workplace entrances that uses ACS and implements security measures to prevent unauthorized access and to protect data privacy, securing database from brute-force attack in the web application to encrypt sensitive data such as username, password, and RFID card number and stored, that protects the (AES) algorithm. It is also transferred from client to server, storing in MySQL database to secure them from hacking, and it is also a great algorithm to protect texts.
- This study implements a security system for residential buildings or workplace entrances that uses ACS and implements security measures to prevent unauthorized access, protect data privacy, prevent SQL injection, cross-site scripting (XSS), and session hijacking.
- The main purpose of sending SMS to mobile phones by using the bulk SMS API to renew the RFID card and during the payment process is to receive service payments.
- The system can easily monitor each person entering the main gate by using RFID cards and keeping the area safer, such as reducing crimes, robbery, and secure sensitive information within a limited time.
- The system can easily monitor each person entering the main gate by using RFID cards and keeping the area safer, such as reducing crimes, rubbery, and secure sensitive information within a limited time.
- It manages the system automatically and accurately, controlling user access and recognizing an individual RFID tag to match and transmit infrared signals.

3.1. Radio Frequency Identification (RFID)

The access control system uses Radiofrequency identification technology because this technology allows data transformation dramatically decreases human effort and mistakes. It can be used as an access control system (ACS) as a high-security for a specific area.

Moreover, it holds information about the holder, such as names, an invalid date, date, time, action status of card (active and de-active), and the user's type status (resident, visitor, and shipment tracking). Hence, it is flexible to renew or extend RFID card validity and needs a reader to access its information. The reader can easily read more cards, as approximately 40 RFID tags can be read per second.

RFID tags can run over much larger distances. At up to 300 ft, the details can be read from a tag. Its tags can store more data, be durable, reusable, and encrypting or greatly increased [33]. The RFID system consists of a transponder, an antenna, and a transceiver with a decoder. From reader-connected antennas, they emit a radio signal. The energized tag of the card modulates the information saved in its memory and transfers it to the reader; the tag's information is obtained. The RFID reader decodes the data and transfer it to the application server [34].

The proposed system is a low-power and low-cost system powered by the double-core Tensilica Xtensa LX6 microprocessor that monitors and controls every resident or visitor entering through the main gate in which an (IoT) unit including the ESP32/ESP8266 is protected and maintained, a series of Wi-Fi and Bluetooth-capable chip microcontrollers. This system aims to attach a microcontroller to the RFID card reader and the servo motor. It also incorporates security measures to avoid unauthorized access and protect the privacy of data.

In this system, all users are identified according to some status, such as resident users, visitors, and shipment tracking—also, separate data in the system. Depending on the statuses to control the data, it depends on the cards' action status, such as "active card" and "de-active card". That shows allowed and unauthorized cardholders by each user, respectively. Hence, information on the ID card, such as the valid date and name, is included. To grant/deny access to the house, it can be used against a database. The system provides access to the cardholder and records the date and time of whether the card is active. However, if the card is invalid, the machine rejects the card and records the date and time of the attempt for safety purposes, and an admin may use the card to know the number of attempts recorded at a later date and time. Intelligence departments will do this to investigate and gather data on the suspects who committed the murder in the case of crime.

Most access control systems nowadays often have three forms, namely access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). According to Adole, Môm, and Igwue (2016), the system alerts mobile SMS to consider using a GSM modem [35], but in this paper, we use the bulk SMS API in the PHP file for access cards when an extension is invalid or required.

3.2. Hardware and Software Requirements

The system has the following specifications for hardware and software:

- Software Requirement

The majority of databases for web applications include three layers:

A Database Server is the backend layer.

A customer's browser is the frontend layer.

Most of the applications occupy the middle layer.

A web server-side scripting language such as PHP is most frequently used [9].

- Frontend Layer: The user interface (UI) is a web-based (HTML, CSS, Bootstrap, JQuery) framework.
- Backend layer: The functioning of applications and pages is under the responsibility of the backend. The MySQL database is used for storing information using web technologies.

- Hardware Requirements

A monitor, microcontroller (ESP8266/ESP32), servo motors, MFRC522 RFID reader, RFID tags, jumper wires, breadboard, and micro USB cables are included in the IoT unit. A general working diagram is given in Figure 4 for Access Control System.

Speed is the considerable difference between manual and computerized systems. In access control, data processes and reports are generated much faster than manual systems. The manual system is generally slow, increasing the data size, and takes long time to search for the individuals or visitors' names to find prior check-in. In fact, if individuals or guests try to gain entry to a city house via the main gate, they may get into difficulty.

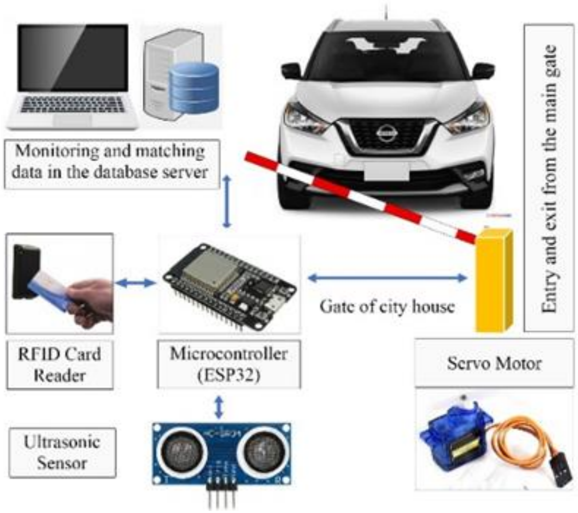


Figure 4 A general Working Diagram of Access Control System

The program can be automatically calculated by software programs to eliminate errors and maximize performance. The system will produce reports and backups literally by pressing a button in a computerized system once data is entered. However, by no longer having staff members and reducing paperwork, and making information retrievable, searchable, and storable, this method can increase accuracy [36].

3.1. Methodology

This study helps to minimize the constant threats and attacks to database security by using numerous approaches. The methodology's study consists of AES, SQLI, XSS, session hijacking, using captcha, connecting (IoT) devices, and backup and restores the database.

- Advanced Encryption Standard (AES)

AES is a specification for encrypting sensitive information, storing your passwords in the database, and using the AES algorithm to encrypt. Secret key encryption or symmetric encryption as a key to encrypting and decrypting data is also known to use a single key.

- Encrypt sensitive data by secret coding.
- The process is reversed when decrypting data.
- Retrieve from the database the secret details and encryption key.

Using the following procedure to decrypt with the same password key (ACS%byRFIDCard):

```
$decrypted =
openssl_decrypt(base64_decode($user_encrypted_TRFID
Card1), $methood, $ky1, OPENSSL_RAW_DATA, $iv1);
```

- Session Hijacking

Session cookies are intended to be accessible to the logged-in user's browser session. The following method is used:

```
<?php session_start();
if(!isset($_SESSION['valid']))
{ header('Location: index.php');}
?>
```

- Using Captcha

To utilize captcha in the web application. following line of code is placed between the <head> tags:

```
<script src='https://www.google.com/recaptcha/api.js'></script>
```

- Connecting (IoT) Devices

This project is a security measure for the residents or visitors wishing to gain entrance to city houses at a specific time and saves their records in the database. This project uses an ESP32, RFID reader, servo motor, and ID card/tag. The microcontroller provides the principle MCU to connect with the RFID reader and read the different users' RFID cards. Likewise, the ESP32 sends the ID card number to the database, and it connects to the servo motor.

Furthermore, this method utilizes to save and send data via a Wi-Fi connection to the web server by using SSID and password. Also, it sends a POST request to send our RFID card value to our server. The URL must be changed to the file PHP's name to request data and insert it into the database. It should be changed the following lines of code looks like this:

```
const char* ssid = "KL21";
const char* password = "KLCC2021";
const char* serverName = "http://acs-solution.info/Admin_ACSID/DB_AddEntrance.php";
```

After editing the codes, plugin your NodeMCU with a USB cable, and on Arduino software, click the upload button. The project stores all of the relevant user information. The system first registers a new customer, and the corresponding data is transferred to the RFID card. In this case, when a user comes to the point of entry and puts their RFID card into the reader, the RFID card will be accessible through the system. The system checks and matches the data in the database to see whether it is registered.

To connecting IoT devices, include two steps below:

- Steps of connecting microcontroller with servo motor:
  - GND connect to ESP32 GND pin;
  - Power connect to ESP32 VIN (5 V) pin;
  - Signal connect to D14.
- Steps of connecting microcontroller with RFID card reader:
  - Hook GND pin connect ESP32 with GND from RFID card reader.
  - Hook 3V pin connect ESP32 with 3V from RFID card reader.
  - Hook SDA pin connect ESP32 with D5 pin from RFID card reader.
  - Hook SCK pin connect ESP32 with D18 pin from RFID card reader.
  - Hook MQSI pin connect ESP32 with D23 pin from RFID card reader.
  - Hook MISO pin connect ESP32 with D19 pin from RFID card reader.
  - Hook RST pin connect ESP32 with D22 pin from RFID card reader.

Figure 5 shows the flowchart of access control system.

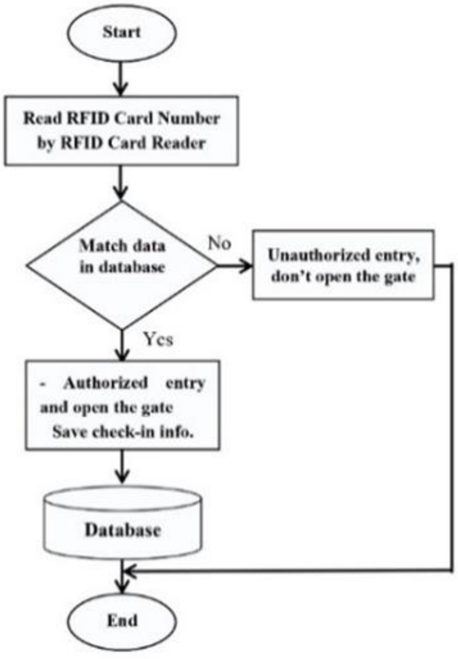

Start
Read RFID Card Number by RFID Card Reader
Match data in database
No
Unauthorized entry, don't open the gate
Yes
- Authorized entry and open the gate
Save check-in info.
Database
End

Figure 5 Flowchart of Access Control System

If the card is active and is not been valid, it gives access to the cardholder and records its date and time. The gate opens and sends a command to the microcontroller ("gate open") to allow the user's entrance after effective authentication and automatically closes after a specified interval of time. This command is sent by Wi-Fi and is stored as user information, such as the ID card number, date and time of entry, and status check-in, in the system. But, if the card is invalid, then the system rejects the card/cardholder.

- Admin

The admin is responsible for the data's security and integrity, creating user accounts, and assigning passwords. The main admin can log in to the database and access it to insert, edit, delete, and can view tables containing information such as city, project name, zone, accommodation type, tower name, floor number, accommodation number. Admin can also add a new authorized person for accommodation and generate new ID card status.

- User

When a user creates an account with the admin, a username, and password, they will receive an email from the database, which must be confirmed to activate it. Any user can access their account anywhere; they can also easily add a record to list visitors, such as a visiting relative or friend or a taxi driver.

- Control Gate

The control manages unlimited gates and shares or revokes access. It also makes sure that people with authorization gain access to different facility areas. In this way, security can be guaranteed, and any part of the facility can be monitored. System control is widely used in residential zone, commercial zone, universities, etc. ACS is typically administered in a central location. Anyone can enter the area or city house using their ID card.

4. RESULTS AND DISCUSSIONS

According to the OWASP [37], the popular security vulnerabilities are brute force attack, unencrypted data, and session hijacking in the top ten most common database security problems.

This study implements a security system for residential buildings or workplace entrances that uses ACS and implements security measures to prevent unauthorized access and protect data privacy. Moreover, this study make the system more sensible to prevent and make more secure against SQLI, XSS, brute force and session hijacking attacks. The system encrypt sensitive data such as username, password, and RFID card number and use strong password policy in web application using AES algorithm. Thus, it becomes robust to brute force attacks.

Types of AES Key Size +	Data Block Size	Matrix Block	No. of Round
AES 128	128	4 x 4	10
AES 192	128	4 x 6	12
AES 256	128	4x 8	14

Table 1 Structure of AES

In addition, there is a transformation method used for the encryption process that includes some substitution, transposition, and mixing functions, with the achievement of producing a higher production of ciphertext. The round number is associated with each key size, which provides a highly secure system [38]. Table 1 shows different AES algorithm and its specifications.

- AES is a cryptographic algorithm with a block size of 128 bits.
- For AES, three different key sizes are allowed: 128, 192, or 256 bits. The majority of our argument will presume that the key size is 128 bits.
- For encryption 128-bit keys, it requires 10 rounds for 192-bit keys. It requires 12 rounds for 256-bit keys.
- It should be remembered that higher performance specifications come with a longer key and more rounds.

The results demonstrate that the proposed approach is straightforward and compelling to secure unauthorized electronic case data procedures by encrypting classified information, resulting in more powerful authentication to simplify web application design. Moreover, it helps web engineers ignore and lessen the web application's high risks to minimize broken authentication risks to avoid leaving the login page. As a result of the (IoT) devices, this method can help speed up the entrance process, ensuring that people do not need to stand in long queues and wait to be checked by a control officer.

The device has a computer controller with the user's check-in and check-out information record. The user must have an RFID card holding personal data to control the gate by servo motor automatically—the servo motor functions as an actuator that, in real-time, the gate will open and close. In real-time, the reader detects the RFID card: if the user is active, the gate opens and, after a given time, closes again. In this study, information about user authentication is matched on the database. If the user is null or has no registered database record, then the gate will not open.

This system was successfully implemented in a secured residential building and workplace so that only an authenticated individual could access the secure place. When the user's RFID card is matched in the MySQL database, the user can enter the city house through the opened gate. The user can add a visitor name in their account, which allows the name/s to be displayed directly in the control point's visitors list.

This software helps every residential building and workplace in various ways. It helps in creating and renewing the ID card and in gathering service payments in a timely fashion. It's possible to install the system in various safe places. A user's record can also be updated by the system, such as how many times the user checked-in. All user transactions are stored in the database server. Administrators can access the database server and see all the records. Also, they can notify people by using bulk SMS API to send SMS messages.

An internet browser's graphical UI (GUI) enables web administrators to deal with the appearance and highlights accessible in the UI (Figure 6). When designing a database, the GUI needs to be user friendly. Initially, we ordered and classify the modules into the following parts: admin, user, control point, visitor, city name, project name, zone, type accommodation, tower name, floor number, and accommodation number.

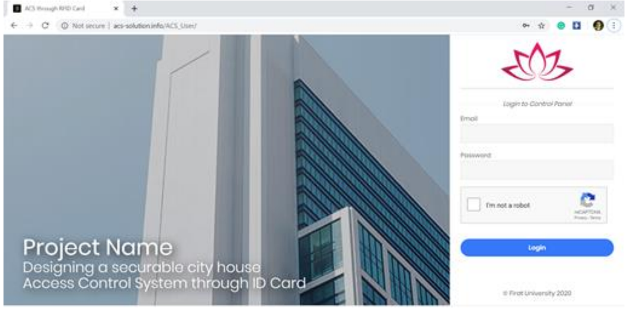
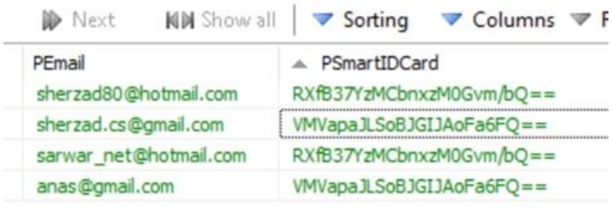


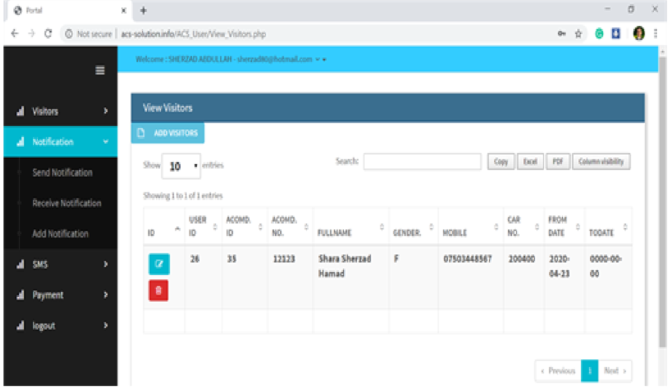
Figure 6 Login to User Account



PEmail	PSmartIDCard
sherzad80@hotmail.com	RXfB37YzMCbnxzM0Gvm/bQ==
sherzad.cs@gmail.com	VMVapaJLSoBJGIJAoFa6FQ==
sarwar_net@hotmail.com	RXfB37YzMCbnxzM0Gvm/bQ==
anas@gmail.com	VMVapaJLSoBJGIJAoFa6FQ==

Figure 7 Encryption RFID Card Number by AES Algorithm

The Figure 7 shows the RFID card information encrypted with the AES algorithm in the database. Figure 8 shows the visitor user information display on the administrator page.

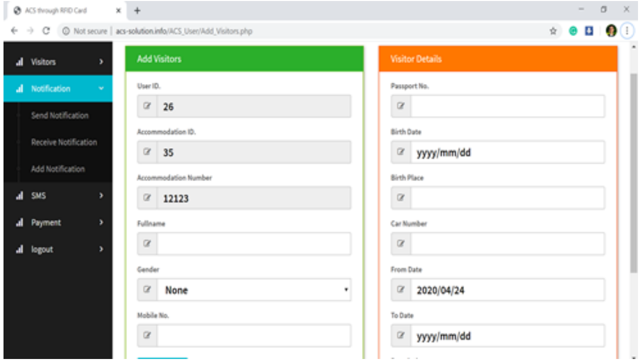


ID	USER ID	ACOMD. ID	ACOMD. NO.	FULLNAME	GENDER.	MOBILE	CAR NO.	FROM DATE	TODATE
	26	35	12123	Shara Sherzad Hamad	F	07503448567	200400	2020-04-23	0000-00-00

Figure 8 View Visitors in User Account

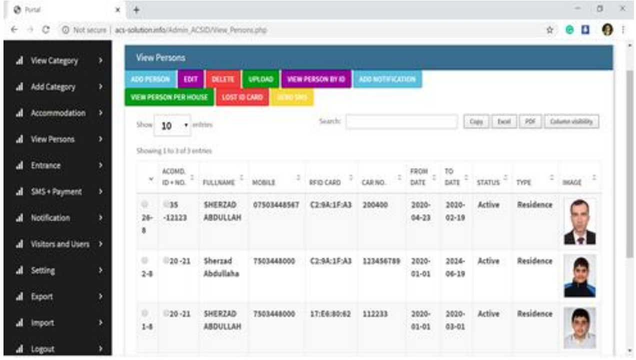
Figure 9 is the interface for adding a new user or visitor to the system and showing the requested information.

Figure 10 is the interface showing the administrators registered on the system with high authority.



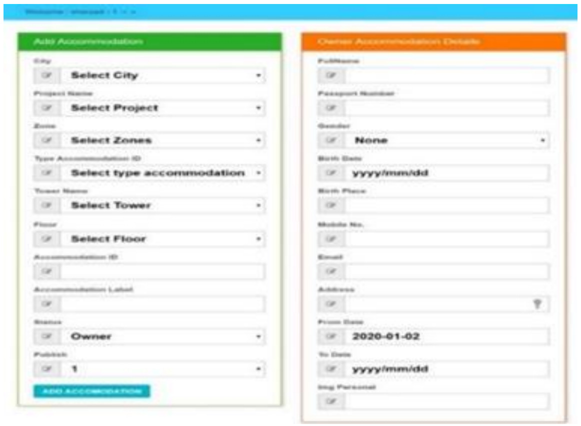
User ID.: 26
Accommodation ID.: 35
Accommodation Number: 12123
Fullname:
Gender: None
Mobile No.:
Passport No.:
Birth Date: yyyy/mm/dd
Birth Place:
Car Number:
From Date: 2020/04/24
To Date: yyyy/mm/dd

Figure 9 Add a New Visitor in User Account



	ACOMD. ID + NO.	FULLNAME	MOBILE	RFID CARD	CAR NO.	FROM DATE	TO DATE	STATUS	TYPE	IMAGE
26-8	35 -12123	SHERZAD ABDULLAH	07503448567	C2:9A:1F:A3	200400	2020-04-23	2020-02-19	Active	Residence	
2-8	20 -21	Sherzad Abdullaha	7503448000	C2:9A:1F:A3	123456789	2020-01-01	2024-06-19	Active	Residence	
1-8	20 -21	SHERZAD ABDULLAH	7503448000	17:E6:80:62	112233	2020-01-01	2020-03-01	Active	Residence	

Figure 10 View Users in Administrator Account



City: Select City
Project Name: Select Project
Zone: Select Zones
Type Accommodation ID: Select type accommodation
Tower Name: Select Tower
Floor: Select Floor
Accommodation ID:
Accommodation Label:
Status: Owner
Publish: 1

FullName:
Passport Number:
Gender: None
Birth Date: yyyy/mm/dd
Birth Place:
Mobile No.:
Email:
Address:
From Date: 2020-01-02
To Date: yyyy/mm/dd
Img Personal:

Figure 11 Add Accommodation (Building, Office)

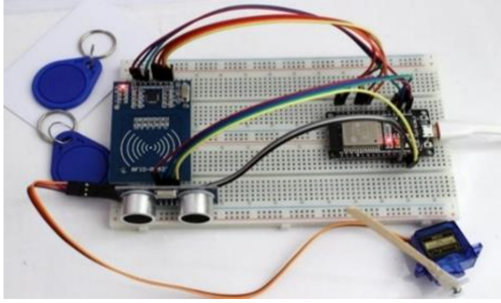


Figure 12 Test the RFID Card Reader, ESP32, and Servo Motor

5. CONCLUSION

This study focused on its use of RFID tools to manage information and access for persons or visitors wishing to gain entrance through the main gate into a city house by designing a web application and centralized database to provides a security system for residential building or workplace entrances that uses ACS and implements security measures to prevent unauthorized access and to protect data privacy. For instance, increase safety, reduce theft, and robbery. It is also used to secure sensitive information such as username, password, RFID card number against brute-force, SQLI, XSS, and session hijacking attacks via encrypting data, and strong password policy the web application.

This study utilizes an advanced encryption standard (AES) algorithm, which is protected strong cryptography from encoding confidential information and session hijacking and providing a robust architecture for designing a securable city house. Access control system uses RFID cards.

Also, to ensure your dynamic web application's security in a professional way to prevent brute force attack and seldom to choose passwords for every account, a secure password manager is used to prevent hackers from breaking into the web application and database. Therefore, this study will assist you in continuing to lower the risk of intrusion, and enhancing programming patches to close up possible attack channels is perhaps the most ideal approach to protect your database servers safe.

Finally, this project configures SMS API to send SMS messages to mobile while renewing the RFID card, either individually or as a group, and gathers payments monthly or yearly. Furthermore, any person living in the building can add a visitor's name to their account and show visitors to the control point office.

REFERENCES

[1] M. Abdullah and R. H. H. Aziz, "New approaches to encrypt and decrypt data in image using cryptography and steganography algorithm," International Journal of Computer Applications, vol. 143, no. 4, pp. 11-17, 2016.

[2] G. Singh, "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security," International Journal of Computer Applications, vol. 67, no. 19, 2013.

[3] A. Abdullah, "Advanced encryption standard (aes) algorithm to encrypt and decrypt data," Cryptography and Network Security, vol. 16, 2017.

[4] M. Malik and T. Patel, "Database securityattacks and control methods," International Journal of Information, vol. 6, no. 1/2, pp. 175-183, 2016.

[5] A. Mousa, M. Karabatak, and T. Mustafa, "Database Security Threats and Challenges," in 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020: IEEE, pp. 1-5.

[6] S. Imran and I. Hyder, "Security issues in databases," in 2009 Second International Conference on Future Information Technology and Management Engineering, 2009: IEEE, pp. 541-545.

[7] R. M. Thiyab, M. A. Ali, and F. Basil, "The impact of SQL injection attacks on the security of databases," in Proceedings of the 6th International Conference of Computing & Informatics, 2017, pp. 323-331.

[8] H. Hu, "Research on the technology of detecting the SQL injection attack and non-intrusive prevention in WEB system," in AIP Conference Proceedings, 2017, vol. 1839, no. 1: AIP Publishing LLC, p. 020205.

[9] W. H. Abdulsalam, "Security For Three-Tiered Web Application," Ibn AL-Haitham Journal For Pure and Applied Science, vol. 28, no. 2, pp. 193-199, 2017.

[10] F. Ayankoya and B. Ohwo, "Brute-force attack prevention in cloud computing using one-time password and cryptographic hash function," International Journal of Computer Science and Information Security (IJCSIS), vol. 17, no. 2, 2019.

[11] J. Simarmata et al., "Implementation of AES Algorithm for Information Security of Web-Based Application," International Journal of Engineering & Technology, vol. 7, no. 3.4, pp. 318-320, 2018.

[12] A. Berent, "Advanced Encryption Standard by Example," Document available at URL http://www. networkdls. com/Articles/AESbyExample. pdf (April 1 2007) Accessed: June, 2013.

[13] J. C. P. Lee, "Strong password by convention methods and systems," ed: Google Patents, 2020.

[14] V. Agrawal, R. K. Paliwal, P. Sharma, and A. Shrivastava, "Web Security Using User Authentication Methodologies: CAPTCHA, OTP and User Behaviour Authentication," in Proceedings of 10th International Conference on Digital Strategies for Organizational Success, 2019.

[15] A. K. Baitha and S. Vinod, "Session Hijacking and Prevention Technique," International Journal of Engineering & Technology, vol. 7, no. 2.6, pp. 193-198, 2018.

[16] E. G. Demesa, "Implementation of a Hands-on Attack and Defense Lab on Insecure Direct Object References," 2018.

[17] Z. S. Alwan and M. F. Younis, "Detection and prevention of SQL injection attack: A survey," International Journal of Computer Science and Mobile Computing, vol. 6, no. 8, pp. 5-17, 2017.

[18] B. K. Ayeni, J. B. Sahalu, and K. R. Adeyanju, "Detecting cross-site scripting in Web applications using fuzzy inference system," Journal of Computer Networks and Communications, vol. 2018, 2018.

[19] R. Patel, M. Nicholl, and L. Harju, "Access control system for implementing access restrictions of regulated database records while identifying and providing indicators of regulated database records matching validation criteria," ed: Google Patents, 2017.

[20] A. Iskandar et al., "Web based testing application security system using semantic comparison method," in IOP Conference Series: Materials Science and Engineering, 2018, vol. 420, no. 1: IOP Publishing, p. 012122.

[21] F. J. D'souza and D. Panchal, "Advanced encryption standard (AES) security enhancement using hybrid approach," in 2017 International Conference on Computing, Communication and Automation (ICCCA), 2017: IEEE, pp. 647-652.

[22] I. Allafi and T. Iqbal, "Design and implementation of a low cost web server using ESP32 for real-time photovoltaic system monitoring," in 2017 IEEE electrical power and energy conference (EPEC), 2017: IEEE, pp. 1-5.

[23] P. Golding and V. Tennant, "Work in progress: Performance and reliability of radio frequency identification (RFID) library system," in 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07), 2007: IEEE, pp. 1143-1146.

[24] M. S. P. Vyalij, "The Use of RFID Technology in Libraries and Role of Librarian," Studies in Indian Place Names, vol. 40, no. 49, pp. 18-23, 2020.

[25] O. A. Allah, S. Abdalla, M. Mekki, and A. Awadallah, "RFID based Access Control and Registration System," in 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), 2018: IEEE, pp. 1-4.

[26] T. Nowicki, M. Kiedrowicz, R. Waszkowski, A. Chodowska, and A. Lach, "Access control system for RFID-tagged documents in supply chain management," LogForum, vol. 13, 2017.

[27] M. M. R. Komol, A. K. Podder, M. N. Ali, and S. M. Ansary, "RFID and Finger Print Based Dual Security System: A robust secured control to access through door lock operation," American Journal of Embedded Systems and Applications, vol. 6, no. 1, pp. 15-22, 2018.

[28] Z. MUKADAM and R. LOGESWARAN, "A CLOUD-BASED SMART PARKING SYSTEM BASED ON IOT TECHNOLOGIES," Journal of Critical Reviews, vol. 7, no. 3, p. 2020, 2019.

[29] S. Gupta and B. Gupta, "XSS-SAFE: a server-side approach to detect and mitigate cross-site scripting (XSS) attacks in JavaScript code," Arabian Journal for Science and Engineering, vol. 41, no. 3, pp. 897-920, 2016.

[30] A. Maier, A. Sharp, and Y. Vagapov, "Comparative analysis and practical implementation of the ESP32 microcontroller module for the internet of things," in 2017 Internet Technologies and Applications (ITA), 2017: IEEE, pp. 143-148.

[31] P. Eze, P. Achebe, L. Jeremiah, and T. Ageh, "Anti-Theft System for Car Security using RFID," 2018.

[32] R. W. Kräwinkel, "The effect of writing and transmitting SD card data on the consistency of SD card write performance," University of Twente, 2020.

[33] S. Rajeshwari, "RFID Technology: Mechanism and usage in Library."

[34] Fernando K, "ESP32 With RFID: Access Control", Instructables.com, 2019. [Online]. Available: https://www.instructables.com/id/ESP32-With-RFID-Access-Control.

[35] P. Adole, J. M. Môm, and G. A. Igwue, "RFID Based Security Access Control System with GSM Technology," American Journal of Engineering Research, vol. 5, no. 7, pp. 236-242, 2016.

[36] Padakuu, "Difference Between Manual And Automated System - Manual System vs Automated System | PadaKuu.com", www.padakuu.com, (2019). [Online]. [Accessed: 24- Jun- 2020] Available: <http://www.padakuu.com/article/1-difference-between-manual-and-automated-system-manual-system-vs-automated-system#:~:text=Ans%3A%20What%20is%20manual%20system,minimizing%20errors%20and%20increasing%20efficiency>

[37] Y. Ayachi, E. H. Ettifouri, J. Berrich, and B. Toumi, "Modeling the OWASP Most Critical WEB Attacks," in International Conference Europe Middle East & North Africa Information Systems and Technologies to Support Learning, 2018: Springer, pp. 442-450.

[38] T. Guy-Cedric and R. Suchithra, "A comparative study on AES 128 bit and AES 256 bit," International Journal of Scientific Research in Computer Science and Engineering, vol. 6, no. 4, pp. 30-33, 2018.

Authors

Muhammet Baykara was born in Elazig, Turkey. He received his BS and MSc. in Computer Engineering from Firat University in 2006, 2009 respectively. He received his Ph.D. in Software Engineering from Firat University in 2016. Currently, he is an assistant professor in the Department of Software Engineering at Firat University. His research interests are Information Security, Honeypots, Intrusion Detection and Prevention Systems and deep learning.

Sherzad Abdullah was born in Erbil, Iraq. He received his BSc. in Computer Science from Dijlah University in 2013, in Iraq – Erbil. His experience background in PHP, MySQL, SQL Server, ASP.net (C#), C++, HTML5, Ajax, CSS3, Bootstrap, Angular JS and WordPress, Security web application, IoT devices. His participated in E-Government in South Korea from date 22 June 2014 to 05 July 2014.