SECURE IOT ENTRANCE USING MOBILE APPLICATION AS REPLACEMENT FOR ID CARDS DURING COVID-19 IN BANKS, UNIVERSITIES, AND CORPORATE BUILDINGS

MARWA ISSAM ABDULKAREEM ABDULKAREEM

JULY 2022

SECURE IOT ENTRANCE USING MOBILE APPLICATION AS REPLACEMENT FOR ID CARDS DURING COVID-19 IN BANKS, UNIVERSITIES, AND CORPORATE BUILDINGS

A THESIS SUBMITTED TO THE

GRADUATE SCHOOL

OF

BAHÇEŞEHİR UNIVERSITY

BY

MARWA ISSAM ABDULKAREEM ABDULKAREEM

IN PARTIAL FULFILLMENT OF THE

REQUIREMENTSFOR

THE DEGREE OF MASTER OF CYBER SECURITY

IN THE DEPARTMENT OF COMPUTER ENGINEERING

JULY 2022

T.C.

BAHÇEŞEHİR UNIVERSITY

GRADUATE SCHOOL

30/06/2022

MASTER THESIS APPROVAL FORM

Program Name:	Cyber Security Master Program
Student's Name and Surname:	MARWA ISSAM ABDULKAREEM ABDULKAREEM
Name of The Thesis:	SECURE IOT ENTRANCE USING MOBILE APPLICATION AS REPLACEMENT FOR ID CARDS IN DURING COVID-19 BANKS, UNIVERSITIES, AND CORPORATE BUILDINGS
Thesis Defense Date	30/06/2022

This thesis has been approved by the Graduate School which has fulfilled the necessary conditions as a Master thesis.

Prof. Dr. AhmetÖNCÜ

Institute Director

This thesis was read by us, quality and content as a Master's thesis has been seen and accepted as sufficient.

	Title, Name	**Signature**
Thesis Advisor:	Ass. Dr. Yucel Batu Salman	
2. Member:		
3. Member:		

I hereby declare that all information in this document has been obtained and presentedin accordance with academic rules and ethical conduct. I also declare that, as requiredby these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname : Marwa Issam Abdulkareem Abdulkareem

Signature :

ABSTRACT

SECURE IOT ENTRANCE USING MOBILE APPLICATION AS REPLACEMENT FOR ID CARDS DURING COVID-19 IN BANKS, UNIVERSITIES, AND CORPORATE BUILDINGS

Marwa Issam Abdulkareem Abdulkareem

Cyber Security Master Program

Supervisor: Ass. Dr. Yucel Batu Salman

June 2022, 78 pages

The major impact of cyber security attacks increases worldwide, implementing the security standards for protecting the data in the cyber environment working in a good manner, but the assets also face the risk of exploiting the physical security of institutions. Considering on the potential risk of RFID cards being lost, stolen, or threatened by third parties to use the privileges of another person. A design was proposed for secure access control system working on android mobile with multifactor authentication enabled to achieve secure access control systems. The privileged person is registered in authenticated user's database and can access through the access control system by authenticating his/her identity with a biometric fingerprint or face recognition technology in his/her registered android mobile phone. When the user is within 10m from the access control system, he/she uses his/her 2-factor authentication technique to generate a secure key sent from his/her mobile application to the database. The database compares the two keys of the same person, which the user can access after providing a correct authentication. This design was proposed to decrease the cases of reaching an unauthenticated person to a restricted institution's assets. The results satisfy the needed security for physical access control systems.

Keywords

IoT, Smart lock, Android application, secure physical access, cyber-physical systems

ÖZ

SECURE IOT ENTRANCE USING MOBILE APPLICATION AS REPLACEMENT FOR ID CARDS DURING COVID-19 IN BANKS, UNIVERSITIES, AND CORPORATE BUILDINGS

Marwa Issam Abdulkareem Abdulkareem

Cyber Security Master Program

Supervisor: Ass. Dr. Yücel Batu Salman

Haziran 2022, 78 Sayfa

Siber güvenlik saldırılarının dünya çapında en büyük etkisi, verilerin siber ortamda korunmasına yönelik güvenlik standartlarının iyi bir şekilde uygulanmasıyla artmakta, ancak varlıklar aynı zamanda kurumların fiziksel güvenliğini sömürme riskiyle de karşı karşıya kalmaktadır. RFID kartlarının kaybolması, çalınması veya üçüncü şahıslar tarafından başka bir kişinin ayrıcalıklarını kullanılması, potansiyel tehlikeler ortaya çıkarttırır. Güvenli geçiş kontrol sistemlerine ulaşmak için çok faktörlü kimlik doğrulaması etkinleştirilmiş android mobil üzerinde çalışan güvenli geçiş kontrol sistemi için bir tasarım önerilmiştir. Ayrıcalıklı kişi, kimliği doğrulanmış kullanıcının veritabanına kaydedilir ve kayıtlı android cep telefonunda biyometrik parmak izi veya yüz tanıma teknolojisi ile kimliğini doğrulayarak erişim kontrol sistemi üzerinden erişim sağlamaktadır. Kullanıcı erişim kontrol sisteminden 10 m uzakta olduğunda, mobil uygulamasından veri tabanına gönderilen güvenli bir anahtar oluşturmak için 2 faktörlü kimlik doğrulama tekniğini kullanmaktadır. Veritabanı aynı kişiye ait iki anahtarı karşılaştırır, kullanıcı doğru bir kimlik doğrulama sağladıktan sonra erişim sağlamaktadır. Bu tasarım, kimliği doğrulanmamış bir kişinin kısıtlı bir kurumun varlıklarına ulaşma vakalarını azaltmak için sunuldu. Sonuç olarak, fiziksel erişim kontrol sistemleri için gerekli güvenliği karşılamaktadır.

Anahtar kelimeler: IoT, Akıllı kilit, Android uygulaması, güvenli fiziksel erişim, siber-fiziksel sistemler

DEDICATION

To my mother Rawaa Hayder, I’m lucky to have you. Thank you for being my biggest supporter in every step of my life, and for always encouraging me to achieve my master's degree. Also, I would like to thank all my family members for always standing for me.

ACKNOWLEDGMENTS

I wish to express my deepest gratitude to my supervisor Ass. Dr. Yucel Batu Selman for his guidance, advice, criticism, encouragement, and insight throughout the research.

I would also like to thank IALD and its president Dr.Mouath Alrawi for their great support, furthermore for believing in me as a member of their hope scholarship program.

Many thanks to every supporter during my master's program. Big thanks to Mr.Edip Vural for his support and encouragement.

CONTENT

LIST OF FIGURES

Chapter 1

1.1 Introduction

The widespread of the internet led to the continuity of developing the technologies, depending on the needs of the communities and governments. After the industrial 4.0 revolution (fourth industrial revolution) which was held by the German government that came up with new technologies, like advanced robotics, additive manufacturing, augmented reality, big data analytics, cybersecurity, cloud computing, internet of things, system integration, and simulation. Huge efforts start being invested in these technologies. In this research, a combination of cybersecurity needs and IoT technology will be presented.

The IoT technologies started to take a part in the everyday life of humans, in smart homes, maintenance management, water supply, traffic monitoring, and other application available depending on the needs. The functionality provided by IoT systems of remote management and control the connected devices to the network by using computer systems or smartphones to control every “thing”, the IoT (Internet of things) technology was discovered to connect more than 40 billion devices “things” to the internet.

As a result, the world is going toward smart cities, where everything will be controlled by smartphones. Using Bluetooth low energy (BLE) / WIFI, to produce communication between devices and smartphones.

Smart doors or smart access control systems were one of the most requested IoT technologies, a lot of research was published regarding this subject, but each one had issues need to be fixed.

Keeping in mind the actual necessity for securing physical access at banks, hospitals, universities, and corporate buildings depending on IoT technology to connect and control smart doors and access control systems by smartphones.

The purpose of implementing secure lock systems or smart access control systems is to achieve a secure environment from any intrusion. Furthermore, secure smart access control systems take more place in corporate buildings like banks, hospitals, universities,

and corporate businesses. This research aims to implement the CIA cybersecurity standards in every corporate business, or corporate building to keep all sensitive data secured and prevent any unauthorized access to restricted and secured areas.

The cyber security CIA trade is standing for Confidentiality, integrity, and availability. The term Confidentiality endeavors of an association to ensure information is kept in mystery or private. To achieve this, any access to data should be monitored and controlled to prohibiting unapproved sharing of data whether intentional or accidental. A critical part of keeping up with confidentiality is ensuring that individuals without appropriate approval are kept from getting to resources vital to the data. Then again, Conversely, an effective system likewise guarantees that the individuals who need access should use their authentication.

Integrity involves making sure your data is trustworthy and liberated from altering. The integrity of data is maintained by the data being authentic, accurate, and reliable.

Availability means the data, network, the application should be available and functioning as they should to functioning for authenticated usage of authorized users whenever needed.

The smart access control systems have a variety of types, biometric-based access control systems that depend on human biometrics (figure prints, Aries, voice recognition, face recognition [55]) to authenticate through the restricted area. Also, a smartphone implemented access control system which works in many different procedures, like OTP (One Time Message), GPS-based smartphone application connection [36], smartphone authentication through cloud database[65], smartphone authentication with username and password [60], also most of these researches reviewed and discussed in the literature review, these researches in somehow have some issue in the application security, process delay time, or vulnerable to security threats, high cost, hard to implement in the real time environment compared with the old fashion ID cards, which has security threat itself, and may also threats user privacy.

1.2 Problem Identification

One of The current extremely used techniques is the ID card to authenticate the identity of the authorized person to access the secure building or restricted areas, where every authenticated person owns an ID card, this card has a serial number or bar code linked to a personal credential in the database; when a person is close enough to scan the card on the access control system screen, the door open if there is matching between the serial on the card with the one located in the database. The usage of ID card has its benefits of delivering no delay process, and low cost; but also vulnerable to misusing by the owner by sharing the card with another person to access a secured restricted area, losing the card, or being stolen by others, by other words losing, stolen identity lead to unauthenticated access which may cause data leakage, steal sensitive data, and, hold data as a hostage as a part of a ransomware attack. Which impacts the CIA security triad of organizations.

The second most implemented technique as access control systems for corporate buildings and governmental institutions is the usage of biometrics as a fingerprint reader in the access control system. Where the users registered to the database with their identity and fingerprint; whenever users need to access through the access control system, they use their fingerprint to authenticate their identity.

This method also delivers some drawbacks over its benefits, like time-consuming, undetected fingerprints if the user's fingerprint is affected by weather or being injured. Also, since we live in the covid-19 pandemic period; it's not healthy to use fingerprint scanner used by others. Furthermore, it's too difficult to decontamination the fingerprint scanner after each user passes through. Also, I believe keeping the user's biometrics in database that could be threatened by hacking is a breach to user privacy. So, this research delivers a safe, secure, ease of use and installation keep the users safe in the covid-19 pandemic.

1.3 Proposed Solution

This research aims to deliver a method to achieve secure access control systems for corporate buildings, and governmental institutions, considering the CIA security triad, which stands for confidentiality, integrity, and availability.

The main concept in cyber security and/or data security is implementing the CIA security triad in businesses and governmental corporations [9][10].

The proposed solution will consist of three main parts, the user's smartphone, the smart lock, and database containing all user's credentials to access an identified areas with identified privileges.

The process will start when the user is close enough (within 10m) to the access control system; the smartphone's application will transfer a packet of data to the smart access control system containing the user's credentials, after the credentials submission done by the user for the first time then, the credentials will be saved in the smartphone application's memory to make it easier, and less time-consuming process, the access control system will check for the authentication of the credentials by sending a request to the cloud database. If the authentication process was completed correctly; the second step of authentication will be required from the user using his/her fingerprint or face recognition in the application's interface, the biometrics authentication is designed to be achieved inside the smartphone to keep the user confidential data fully protected inside his/her smartphone as privacy point of view. considering that the smartphone is not lost or stolen, likewise in RFID cards. After the second step of authentication is completed, if the biometrics are delivered correctly, which means the authenticated user tries to access. The access control system will allow the user to pass through, otherwise, the access will be denied.

In this case, the users keep access through restricted areas with their privileges. Without being in touch with devices publicly used by others, furthermore, maintain the security of data from unauthorized physical access. And each facility will be accessed by authorized users with identified privileges in terms of the time can access, which facilities can be accessed, and many other customizations.

Chapter 2

Literature Review and Background

2.1 Literature Review

The author in [60][15] presents a smart access control system connected to the database for user management controlled by software on smartphones that uses a username and password as an authentication method, the software has two different interfaces, administrator interface, and user interface to implement a smart access control system.

The method used in this research delivered by connecting four components (Arduino with Bluetooth module, solenoid door lock, web server, and user)

The process will start whenever the user opens the application, the Bluetooth starts to discover and connect to the access control system nearby, and if the connection is created, the user will be able to use his/her credentials to log in [29].

Now, it's the web server's responsibility to check the user credentials, if it was registered in the database the user will be able to generate access to the wanted facility.

The design in [60] delivers Software on smartphones that uses a username and password as authentication. Arduino with Bluetooth module, solenoid door lock, and a web server implemented to achieve the required design. The design total delay is 2-5 seconds with a 9m distance. The design total costs 2.000.000 IDR equals 134$.

The slow process of this system compared with RFID, or fingerprint considered a Drawback of the system, otherwise, it remains a secure system delivered with a low budget and user-friendly

This research [36] aims to deliver a control access system without any intervention from the user while remaining secure depending on GPS used by an application installed on smartphones.

The application checks for access control systems nearby, every five minutes, whenever the user is within 10m distances, the application sends a command to the smart control system to unlock the access control system. Otherwise, the access control system remains locked. The system needs improvements in terms of quality, power efficiency, and area tracking.

The author in [55] emphasizes the importance of investing in smart cameras for secure access controls avoiding the delay in accessing the facilities of long process fingerprint access control systems. A Histogram Object Gradient HOG algorithm was implemented to achieve accurate face detection. The system works in a few stages, face recognition, face encoding, face location, and authentication. The process accuracy depends on the HOG algorithm that split the input image into blocks, each block divided into smaller cells. HOG is created for each cell.

The action starts with capturing the image of the moving person, then face encodings, features extractions, RFID, and face recognition steps will start to process the captured image. If matching accrues with the registered image in the database, the access control system will open, otherwise, it remains closed. The research with the used algorithms could be invested in a real-time environment. To produce an effective security system.

In this paper [42] a digital door lock system that works with an IoT environment is presented, this system is implemented as a try to enhance the security system of offices and homes depending on the usage of smartphones. This paper presents a high-security solution for control access systems, by using an alarm and image transfer function, that sends the attacker's image to the administrator y smartphone when someone tries to apply a physical force or input an invalid password many times. Also, if a valid user tries to access but the password was forgotten, the image transfer function will send the image to the administrator to approve or decline the access.

The paper implements a microcontroller to control the digital lock, furthermore, to communicate the digital lock with the door a Bluetooth module was implemented, also ultrasonic sensor to recognize the nearby users, OpenWRT as an operating system, also a web server and database is implemented.

The proposed process will be depending on the action taken by the user, physical force, mistype the password, forgotten password, known password, the microcontroller will behave according to the action, and the valid user records in the database.

The Research found that the research presented works perfectly and can be implemented in a real-time environment and could be commercialized as a product.

This paper [42] attempts to analyze the existing researches in the field of secure access control systems, the way its developed and improved, and how multifactor authentication is embedded over time. After the analysis, the researcher presented a safer access control system, which has many features to improve security. The main idea is implemented by activating face recognition and detection and mask detection for safety reasons, especially in a pandemic.

The researcher implemented 4 parts to present a safer system which consists of Proteus, face recognition, face detection, and mask detection. Proteus uses an Arduino which is used also to store the password of authenticated persons with high privileges. Before the process started the images of authenticated persons were collected, and each person has a folder of all his/her images (with and without masks separately in different folders). If an authenticated person passes through the system will check his/her face with the database, and his/her name with appear on the screen, otherwise will not be allowed to access it. The researcher implemented Haarcascade which is a built-in function in OpenCV to detect masks, also Flask API to detect face masks through live stream videos.

The researcher concludes that the system with the implemented features is presenting more security from hacker attacks, and also cost-effective and simplified management. The mask features are applicable till the covid-19 pandemic finishes. For less complexity, a hardware substitution with Raspberry-pi will be more successful.

The paper [65] presents a secure access control system, using a WIFI bridge device connected to the cloud database server, BLE, and smartphone-controlled by the end-user. Two types of users can access the secure access control system, normal users, who use an encrypted ID with AES256 key, the look authenticates the ID with the data in the database, whenever the authentication succeeds the look will process the following command,

otherwise, it will not. Admin users which have administered keys, which give privileges to add new ID and keys, delete an existing ID, and other features.

The system has two statuses to operate in, first with an existing internet connection, the smartphone transmits data to the cloud server, the cloud server communicates with the bridge, and the bridge sends the data to the lock to operate the operation. Access approved or denied according to the authentication of the credentials. In case no internet connectivity is available, the smartphone communicates with the bridge using BLE, and the bridge transmits data to the lock if credentials authentication is done, the access control system will open. The researcher finishes the research with the importance of applying the research in a large-scale environment to test all features. Also, the featured customers will not be reassured by the idea of saving the keys in a third-party cloud server, storage of the ID and keys on the bridge will be an advantage. the cloud server in its current implementation has too much access, and most individuals would be hesitant to trust a third party to unlock their properties.

The paper [64] proposes a human-based control access detection and path examination, to decrease false automatic access control system framework activities whereas increasing the included values for security applications. based upon the need for an automatic door control system based on the detection and deliberate examination of individuals. once a person is detected in the region of interest (ROI), the trajectory of his face can be tracked and then analyzed by a statistical analyzer to calculate the corresponding cumulative probability and will be used as the estimation of the intention.

The proposed system can determine the user's intention and provide access to the access control system by detecting his position and tracking his trajectories of movement in the image sequence. To implement the system, a DSP-based multimedia module, TI DM368, is selected as the hardware platform. The algorithms developed were programmed in C and executed under the Linux platform.

In this paper, an automatic access control system is implemented on a DSP platform. The system can first identify a target as a person by face detection, and then analyze the path trajectory to determine whether the person has the intention to access the access

control system or not, thus, controlling the access control system accordingly. It is noted that the system has advantages of a low false rate (near 0%), high correct activating rate (99.6%), and short response time (within 2 s) from detecting the target, confirming his intention, to activate the access control system opening. Moreover, via statistical analysis of the detected face in consecutive time sequence compared with traditional ones, not only reduces the false action rate but offers power-saving benefits it is possible to add disaster or crime prevention functions that this can be applied to surveillance applications.

The research in [36] [19] presents smart homes using door automation depending on Arduino to automate access control of smart homes controlled by Bluetooth-based smartphones. This research aims to present a better and safer value of living.

The Researcher implements an Arduino microcontroller using IC ATMega328P-PU, which is programmed using C language, and an Android smartphone that connects with Arduino using Bluetooth module series HC-05 to complete the order of opening or closing the door. The end-user uses 6 pins to authenticate the credentials, and it takes 1 sec to go further with the command requested. Every test shows that all goes as indicated by plan associations. It additionally gives security and simplicity to Android phone/tab clients. This research is dependent on Android and Arduino the two of which are Free Open-Source Software.

The research [50] tries to make an elective access control system, where card scanners are supplanted with uninvolved RFID tags, and all the correspondence is done employing the client's smartphone's Wi-Fi. Taking in mind the examination of existing ways to deal with the advancement of access control frameworks. Whenever higher security is mentioned, the biometric credentials (fingerprint, face recognition) are mentioned, so this research offers higher security guarantees when entering a gateway without requiring video reconnaissance cameras.The identification verification processes using passive RFID labels, can store adequate data for our structure and are significantly more affordable [35]. By holding the device near a reserved tag, the application will be normally started. All information about the access gate to which the tag is joined will in like manner be subsequently sifted. Moreover, to avoid the need for a free video surveillance camera foundation, an image on a person's forward-looking camera will be

required starting there forward, information from the tag similarly to the customer's data, including customer id, region, and photographs, is sent off the server through a corporate Wi-Fi association to complete the authentication process, and the access control system will be locked/unlocked depending on the data entry of the credentials.

The paper [53] presents a multiuser multidevice smart home control system, multiuser environment normally faces conflicts, complexes, and dynamic changes that confuse the control systems. But this paper implemented **Kratos** which permits clients to characterize unique policies for smart home devices, indicating their necessities. It additionally carries out a policy negotiation algorithm that naturally improves the conflict policy demands from numerous clients by utilizing client jobs and needs.

Finally, Kratos administers a unique policy for various clients, looking into the aftereffects of the policy negotiation and also upholding the negotiation results over the smart home devices and applications. Kratos was carried out in the Samsung SmartThings platform which has the biggest portion of the overall industry in buyer IoT, upholds the largest number of off-the-rack smart home devices, and open-source applications for Implementation and Data Collection, Samsung SmartThings hub was utilized, and associated with different smart devices and sensors to the hub. The setup included four distinct kinds of devices: smart light, smart lock, smart access control, and smart camera. also, three unique kinds of sensors are used to give independent control, movement, temperature, and contact sensors, to sum up, Kratos executes a priority-based policy negotiation technique to determine conflicting user demands in a shared smart home system.

Kratos effectively covers the clients' necessities, and our broad assessments showed that Kratos is powerful in settling conflicting solicitations and authorizing the strategies without a huge overhead. Likewise, we tried Kratos against five distinct threats and observed that Kratos adequately distinguishes the dangers with high precision.

The paper in [61] research present more secure access control systems using Cryptography and steganography methods to reduce the impact of man-in-the-middle attacks that IoT systems face. Where Cryptography works with AES encryption to encrypt

the data sent through Bluetooth, and steganography to embed the encrypted ciphertext in an image.

The research implements smartphone applications for user-side and raspberry-pi as server, the user nearby access control system, enter his/her passkey through the smartphone application, then it will be encrypted to ciphertext and embedded in an image, then it will be sent to raspberry-pi to be decrypted, then the server compares the send passkey with the one stored in the database, if correct the lock will open, otherwise it will remain locked. To sum up, such an approach might conceivably help research Eid the Security in IoT and brace the eventual fate of BLE-empowered IoT devices.

The thesis [56] presents a smart access control system lock connecting to the internet and able to recognize employees that work in the office. Not only but also, the research focuses on the security aspects and security challenges in IoT systems. The researcher implements photon devices as a microcontroller, Bluetooth beacon for Bluetooth connection, Azure cloud, spark cloud, door API, and auth API.

The process starts with action from the android smartphone application by sending a username and password to auth API requesting authentication to pass through the door. Auth API requests an access token from Azure AD, depending on the credentials sent previously by smartphone to auth API, if the username and password are identical to what exists in the database, the Azure cloud will provide a token valid for 2 hours, will transfer back to the smartphone through auth API.

Then, the smartphone will attempt to access by sending a request to the door implementing the username, password, and the established token, Furthermore, the door will send HTTPS request to spark cloud the request contains the unique access token and device ID for the Particle device. Spark will send a function “open door” to the door, then the photon will return a value to observe whether the function is executed or not for spark cloud, then it will be transformed to door API after that value will be transformed to the smartphone.

The project effectively verifies a client and opens the door, the user authentication is achieved, and managed easily depending on Azur active directory, authentication API

and DoorAPI are effectively transferred to Azure Cloud and can be accessed by HTTPS requests. The research was reliable, and unique to deliver such secure access control depending on Bluetooth Beacon, Google Beacon API, and Google Messages API which are new technologies

The research [59] tries to identify the smart home devices and software, and all the threats and attacks that face this smart environment. As a first step, the researcher classifies the smart environment into three Perceptual layers Network and Application layer, and empathizes that each layer has its threats and attacks. After exploring each layer and its threats and possible attacks the researcher concluded that no one solution fits all devices or all smart environments. So, the trick here is to guarantee the CIA of the data, no matter which device or software was used, which refers to confidentiality, integrity, and availability of the data transferred among applications and devices through the networks.

The research [44] describes the importance of security for smart access control, from all aspects, but it emphasizes three breach aspects of smart access control, which are relay attack, replay attack, and unauthorized access. To begin with, the solution is delivered to prevent a relay attack which is a type of man-in-the-middle attack, where attackers gain access by relaying the signals between authenticated objects. so, the researcher designed a smart lock system using a core Bluetooth API, where the user authenticates the credentials, then if the authentication is done, the lock checks the distance proximity of the device nearby the lock, and the unlocking process will start, otherwise, it remains locked.

For an Access Revocation attack, normally the server sends a certificate of authentication to the user's device then the certificate will be transferred to the lock to be opened, but if the user's device is operating in offline mode, it doesn't push logs to the server and it also still connecting to the lock, in this case, the lock doesn't know where to open or block the request. In this case, the researcher proposed a one-time token to be sent to the user's device and the lock at the same time, then the user transfer the token to the lock in a limited time interval to access through the lock.

The last attack discussed in this research is a replay attack which is also a type of man-in-the-middle attack, where the attacker copies the identity packet sent to the lock and uses it at other times. For this case the researcher proposes to deliver a timestamp embedded before the authentication, in this case, the lock will detect if this is a real signal or copied from a previous time.

Depending on the experimental results the researcher discussed and shown in this research, the researcher concluded that these solutions are easier and cheaper and prevent most attacks facing IoT or smart lock systems. due to the security leaks in smart home access control systems [61], this research proposed a secure smart mobile app for the smart home environment (SSMASHE), which content of three modules for authentication considering that improper authentication is one of the existing security leaks.

Mobile applications, IoT devices, and big data platforms are implemented in this project to deliver access control depending on authentication and authorization, so the user's smartphone uses a public key that is shared with the user's device during the registration, and credentials to authenticate him/herself to access control system.

the process works firstly by establishing Wireless connectivity to access the control system with a bar code of smartphone scanning for interaction, then, the user transfers his/her credentials to be verified. If the credentials verification notifies with matching credentials with the existing big data platform (cloud database) the access control system will permit the access, otherwise, the access will be denied, and the Alarm system will notify with unauthorized access.

The suggested method about connecting to IoT devices and users operate their data wirelessly to the big data platform. In addition, the access control system is responsible for detecting unauthorized Access of people and theft, if such a situation is recognized; a message will send to the access control systems' admin through his/her smartphone. These smart access control systems normally cause some delay, but the proposed system has compared to other systems, and it delivers less delay has been concluded.

The paper in [8], IoT-Enabled Door Lock System presents Application checks for access control systems nearby every five minutes, the access control system opens when the user is in range. Raspberry Pi based, and MINDS android applications implemented. The system is user-friendly, power effective, and area tracking and indoor accuracy that delivers a secure access control system. On the other hands Automatic opening for the access control system, consider a drawback since no authentication is required as RFID cards.

The research [39] delivers a design of the Smart Lock system, which keeps the functionality of the Access control system the same while incorporating the possibilities offered by the chip to the new system. In a smart lock system, security is paramount. To rule out possible attacks and malfunctions necessitates extra care and analysis. So, the research explains security from four aspects, The first is to capture and investigate the security configurations of the current smart lock of Lukoton, examine its assets and vulnerabilities, And present a developed version. secondly, the aim is to analyze the proposed EEPROM chip and investigate the potential outcomes it offers to work on the security of the smart lock framework. This chip requires a trustworthy setting to accomplish an ideal configuration. Third, the aim is to propose another upgraded security configuration for the framework, by considering significant security issues and keeping it lightweight and appropriate for B2B applications. The fourth aim is to assess the security of the proposed design.

The EEPROM chip was not secure, furthermore, organizations began to design and deliver secure chips with implanted cryptography. One of these organizations is Atmel. The Atmel AES132A chip is a fundamental piece of the smart Lock Access Control Framework. The ATAES132A chip gives both authentication and confidential data storage. the AES132A chip is a fundamental piece of giving security to the framework It permits flexibility and efficiently sets up the vital security in the framework. It involves AES encryption in a standard mode, suggested by NIST, which also gives authentication and furthermore message integrity by utilizing the MAC. Likewise, the chip is protected on both the hardware and the software side.

The chip manufacturer ensures that the keys put away in the Key Memory can't be perused under any conditions. We utilized the open doors given by the chip to layout a safe smart Lock Access Control Framework. Two elective implementations emerged during the work cycle. In the chip-based solution, the chip creates the one-time number required for the confidentiality and integrity algorithm, while in the cloud-based solution the cloud is responsible for this task. As the result of this analysis, the cloud-based solution

The research [61] tries to present secure smart lock systems that aim to prevent unauthorized access through access control systems controlled by smartphone applications and remote servers.

This research focuses on four attackers

1. A physically present attacker

2. Revoked attacker

3. Thief: Mallory steals Alice’s authorized device.

4. Rely attack

As the researchers conclude depending on the previous related work all the smart lock systems were vulnerable to the mentioned attack vectors. The research presents defenses that can be implemented today without any hardware changes to existing devices. The second class of attacks is more challenging to stop without sacrificing usability, and no existing system provides an adequate defense.

The research [17] proposed a secure smart mobile app for smart home environment (SSMASHE), which content of three modules for authentication considering that improper authentication. Mobile applications, IoT devices, and big data platforms are implemented in this project. A username and password are used for authentication The delay is in the range of 30 to 72 ms depending on IoT devices connected after the credentials are delivered correctly. is responsible for detecting the unauthorized persons and theft recognition. The total delay was compared and calculated as low. is comfortable to real-time heterogeneous smart home IoT devices because this process follows the asynchronous authentication procedure. Otherwise, It has a continuous background

process and message exchange between the 3 modules in smart mobile, so battery maintenance is required.

The sources [39] This design of the door locking system includes features that make the action of locking the door more reliable to the user than the system. increase security access with an accurate detection system is provided by this research. The delivered system is operated by mobile phone through short message service (SMS) transferring operation from any spot of the world where a mobile network is available. This research aims to deliver a smooth and robust locking mechanism and the mysterious door-moving control device is used for the efficient operation of controlling the door. The system implements LDR sensor to discover the entrance attempts of any person, the GSM shield alert the user if any person wants to enter, and the implemented microcontroller act as the controller for the system overall. It verifies the user's cell phone number to avoid unwanted entries. The research provides information about the status of the door by sending SMS. Also, the user can operate the system with more than one subscriber identity module (SIM) card. The device operates with the lowest cost estimation benefit. Finally, the performance of the real-time operation of it found satisfactory performance.

The research [56] aims to deliver and develop a secure design for home security system, using remote auditing technologies and human face recognition technology [49][24], to verify the visitor identity and to control access through an access control system using the Internet of Things and implements raspberry pi as controller and also, the implementation and deployment of the wireless control system to a home environment for only authenticated people. The architecture of this researcher contains 5 parts. Firstly, the inputs unit, like webcam with widescreen, noise-reducing microphone, true color technology for video, and a universal attachment. Secondly, the communication interface. Thirdly, the intruder detection module used the raspberry Pi 3 and power supply. the last one is the door lock system. and the fifth one is the application-specific unit. The main purpose of this implementation is to provide a high-security face detection system on the Raspberry Pi board and send an alert to the authorized person via GSM (Global System for Mobile) module. This design will start the process by Interfacing of input unit to capture a live Face image. The system will compare the authentication of visitors with a

pre-created database of authorized house members and relatives. Capture the face at the doorstep and compare with the database image then, the Interface GSM(SIM300 GSM) module take action by sending an alert to the authorized admin then, furthermore, a commend sent to the lock system interface relay. If any visitors arrive, the Raspberry pi sends an appropriate text alert which is done by a separate python code that is running in the background. The server will send to the homeowner the name and photos of visitors for further action. Webiopi GUI webpage is used by the owner which gives the ability to directly log in and interact with the real-time embedded devices without the need of an additional server.

The research delivered a complete secured system through a login E-mail and Webpage password-based authentication. The design is completely wireless and integrated with software to a low-cost, robust, and easily operatable system. Thus, this will form a fully automated security system.

The research [42] tries to boost the security of smart doors and access control systems and aims to improve the trustworthiness of smart door lock systems. The project implemented Arduino and IoT to deliver these functions. This design could be implemented in various types of doors, main access locks, and locks depending on the knocking pattern. The authorized person knocking pattern is stored in the register. When the knocking pattern is detected by the sensor, it transfers the pattern to the Arduino board microcontroller. Based on the trustworthiness of the pattern. The researcher implements a motor drive to control the door. and for the door lock, IoT, and bylynk app for receiving the status of the door. and the last component is the DC motor which is used to convert electrical energy into mechanical energy.

The process of this home security system goes through two steps. The first step is where the user could mark the thump impression and successively the thump impression will be stored in the database of authenticated users. In the second step, the time gap between the thump impression codeword is generated. If the code is correct, then the door will be unlocked. When the client wants to open the door, the thumping data were collected. To detect the thumping, piezo electric-based vibration sensors were used.

These sensors collected data transferred to the Arduino. If the data was authenticated data, then a flag will be set to open the door. All activities are connected to the user's mobile. So, the status of the door was continuously monitored by the user. If an unauthenticated user tries to open the door immediately alert will be given to the admin mobile. The proposed framework is very simple and low-costly, also as the bylynk is a free application. The accuracy of the system is very high. So, the admin can control the access remotely. Based on the thumping on the door. this security system works properly but, many advanced features like, remote monitoring and controlling of the door could be added as feature work.

2.2 Background Related to Internet of Things

The purpose of writing on this topic is to familiarize the reader with the idea of the Internet of Things, including its fundamental operating principle, architecture, areas of usage, as well as benefits and drawbacks associated with its implementation.

The Internet of Things (IoT) is a term that refers to a trend that is constantly developing for smart gadgets that are linked to the internet or another network and are able to interact with one another. The Internet of Things may be defined differently depending on who you ask or when you ask them [8].

OECD definition:

"The term "Internet of Things" refers to a network that connects all gadgets and physical items whose states may be altered via the use of the internet, whether or non-human intervention is required. Even though connected objects may necessitate the connection of devices that are regarded as being part of the "traditional Internet," this definition does not include laptops, tablets, or smartphones because these devices are already included in the OECD's metrics for broadband connectivity.[7]" (Report published by the Organization for Economic Cooperation and Development for the Year 2018)

A definition of Gartner is as follows:

"The Internet of Things (IoT) is a network of physical items that future's built-in technology for communicating and detecting or interacting with their internal states or external environment," according to Cisco. "The Internet of Things" is also known as "the

Fourth Industrial Revolution." (Gartner undated). It encompasses a large variety of hardware with a wide variety of functions. They are managed by a user interface, the majority of which are apps. The application makes use of the device's sensors to offer information on the current state of the device or the environment it is located in. Based on this knowledge, we have the ability to subjectively program the smart gadget to behave in a manner that is congruent with our requirements in a variety of environmental contexts.

The Internet of Things (IoT) is seeing explosive development for a variety of reasons, including. Companies and farmers alike save money and time as a result of the production efficiencies afforded by this practice. It keeps an eye on the machines' upkeep and wards off any potential breakdowns they could have. Facilitates a simpler and more pleasant way of living in private residences. Patients get better medical treatment in settings such as hospitals and operating rooms as a result of faster illness diagnosis and earlier disease detection. The manufacture of these goods is significantly reduced in cost thanks to the development of new technologies, making them more accessible to smaller businesses as well as the public. (Buyya and Dastjerdi 2016).

According to research conducted by IoT Analytics in 2018, the total number of active Internet of Things devices throughout the globe reached 7 billion. Not individual sensors but active Internet of Things devices and gateways that focus on end sensors are listed here. However, this total number of active Internet of Things devices does not include more complex devices such as mobile phones and tablets, laptops and desktop computers, and landline telephones. In 2018, the worldwide total number of Internet of Things (IoT) devices and other connected devices that were actively connected was roughly 17.8 billion.

It is anticipated that the total number of Internet of Things devices that are actively linked across the globe will reach 21.5 billion units in the year 2025, while the total number of all activities connected devices across the globe will climb to 34.2 billion in the same year. As a result of the rise in IoT applications around the globle Consumers who utilize smart gadgets, for instance in their homes, and business owners who employ smart equipment in manufacturing are the primary users of the devices.

The study period began in 2015 and continued through 2018, at which time there was 3.8 billion actively connected Internet of Things devices and nearly 14 billion all actively linked devices. A rise of around ten percent from one year to the next in the number of actively connected devices is anticipated, and a growth pattern similar to this one may be anticipated even in the years to come. (Lueth 2018) It is a novel approach to putting things together. The Internet of Things brings together preexisting infrastructure with various devices and systems (internet, computer network, mobile network). Give you the ability to remotely operate these gadgets. Things are capable of either receiving data or sending data or both. The data that devices connected to the internet generates is more important than the devices themselves. The Internet of Things gathers a vast quantity of data from various sensors. Following processing and analysis, all these data are retransmitted to the user [54].

The Internet of Things enables us to develop solutions that are smarter, more rational, and overall superior. We put it to use in a wide variety of sectors, including medicine, supply chain management, energy, transportation, meteorology, finance, retail, manufacturing, inventory management, and smart homes, among others. It is able to control infrastructure as well as structural modifications, which may prevent any potential hazards. Finding parking spots and maximizing the efficiency of energy use in autos are both important. Real-time monitoring of our package delivery or cab service. The initial goal behind the development of smart homes was to make life more comfortable for persons of advanced age or those who have physical limitations. These days, anybody may have one if they so want. The Internet of Things has the potential to make our routine tasks less taxing and more pleasurable.

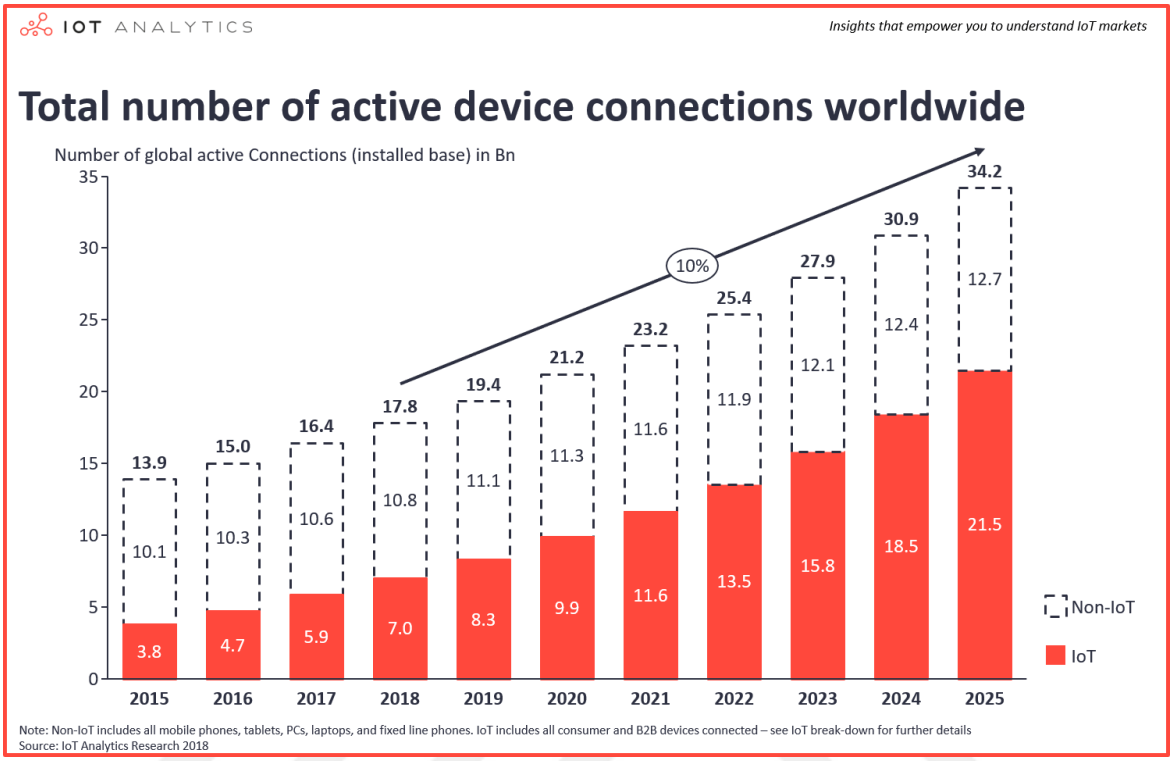

Figure 2.1 Total number of devices that are actively linked throughout the globe (Lueth 2018)

The total number of devices that are shown on the graph only takes into account those that are now active connections; it does not take into account inactive devices that were previously acquired

The mechanism behind the IoT.

In order to get started, we will need some Internet of Things devices. It may be anything from a surveillance camera to a doorbell to a voice assistant or any other kind of smart gadget. Each one of these devices is equipped with sensing technologies or sensors that continuously gather and communicate data on the current state of the device, what it is doing, and perhaps also the environment in which the device operates.

In most cases, these devices communicate with an Internet of Things gateway, which is a piece of hardware that runs application software and acts as a facilitator for the connectivity of various data sources and targets. The Internet of Things gateway facilitates

communication not only between individual IoT devices but also between individual IoT devices and cloud servers. As a result, it functions as a middleman between the Internet of Things and the end-user.

In addition to this, we have the Internet, which is the only communication route for the Internet of Things gateway. Our Internet of Things gateway will interact with a cloud server or data storage by using this particular communication route. Here, all of the information that is sent by our Internet of Things devices will be saved and evaluated. After the information has been reviewed, it will be delivered back to the end-user in the application that he is using, such as on a mobile device. 2018 according to Meredith, the figure that follows provides a graphical depiction of what was discussed.

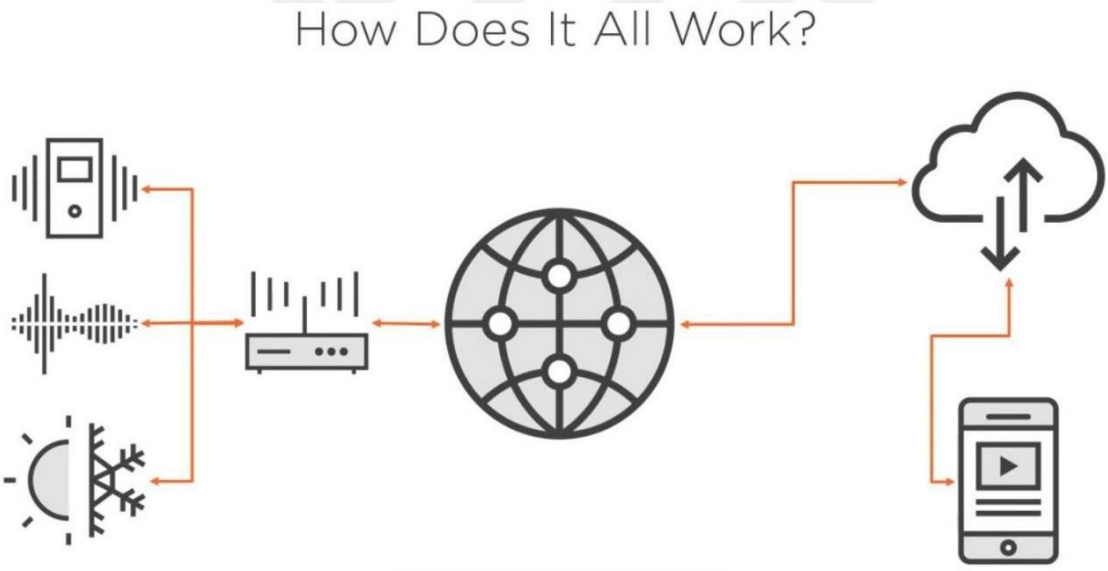

Figure 2.2: IoT working concept according to Meredith

2.3 IoT Architecture

The infrastructure that supports the Internet of Things may be broken down into a few different levels. It is sufficient to comprehend a three-tier architecture in order to grasp the fundamentals. The first layer is called the sensor layer, although it's also called the perception layer. This layer incorporates all the hardware components, such as readers and sensors, in addition to the actual physical devices themselves. She oversees accumulating

knowledge and determining the nature of things. This layer may gather a variety of information, such as the position of the device or sensor, the speed of the wind, the temperature of the surrounding environment, vibration, humidity, and movement. Following its collection at the sensor layer, data is sent further to the network layer in order to be received by the central information processing system. This system may function as a server or storage for data on the cloud [18].

The second layer of the Internet of Things architecture is known as the network layer. This layer is sometimes referred to as the transmission layer. The primary objective of this layer, as suggested by its name, is to ensure the safe transmission of information. Through the use of communication technologies such as 3G, 4G, UMTS (Universal Mobile Telecommunications System), WiFi, RFID (Radio Frequency Identification), NFC (short distance communication) [38], Bluetooth satellite, and so on, the data that is gathered in the first layer by physical objects and sensors is sent to a centralized information processing system [13]. The network layer is also responsible for connecting smart devices, network devices, and the network itself. The information that is sent between these different types of devices may either be wireless or wired.

This three-tier design concludes with the application layer as the most recent layer. The management of application services that make use of IoT technology is within it's purview. Services provided by applications may differ from one another depending on the information gathered by devices and the sensors on those devices. The monitoring of health, the tracking of animals, the administration of smart homes or cities, and an endless number of additional services are examples of applications that make use of the Internet of Things. (Burhan et al. 2018; Kraijak and Tuwanut 2015)

2.4 Areas of Application

The Internet of Things may be used in a wide variety of contexts, and the use of smart devices is on the rise. This is mostly attributable to the fact that these devices are getting more affordable and provide a wider range of capabilities. One of the first things that come to mind, for instance, wearable electronics or a smart house, both of these things

are part of the consumer market. Another area of use for our technology is in the administration of states, for example, in the form of smart cities or the management of infrastructure. The Internet of Things is also gaining popularity in a variety of other fields, including manufacturing, agriculture, health, and social services, and more. (Buckwheat 2020) Buckwheat

2.4.1 Electronics that may be worn

Wearable electronics consist of intelligent gadgets that may be worn on the body or clothing and often linked to an application that is housed on the user's mobile device. A smartwatch is one of the most typical examples of a piece of wearable electronic equipment that we may encounter. This watch does a lot more than just show the time; it also has a lot of additional features. Monitoring might include checking our sleep pattern at night, as well as the number of steps we take, our heart rate, and the number of calories we burn when participating in sporting activities. They are able to monitor our health and let us know if our level of physical activity is adequate based on these readings. Once we have connected them to the phone, we are able to utilize them to either answer incoming calls or get alerts of new messages that have been sent to us. In this category, you may also add virtual reality glasses, hands-free headphones and microphones, and any number of other types of electronic gadgets. (IoT portal 2016a)

2.4.2 The internet-connected house

The capacity to automate mundane aspects of everyday life is quite appealing to a lot of different individuals. Devices connected to the internet of things enable us to automate an almost limitless variety of activities and responsibilities in our homes. In the morning, when we are still in bed but the coffee maker is all set up and ready to go, we are able to enjoy the convenience of having freshly brewed coffee brought to us. Many people place a high premium on safety, which may be ensured by installing motion sensors, smoke alarms, or surveillance cameras in their homes. These devices keep an eye on our property and can notify us of any suspicious behavior or potential danger, no matter

where we are. The fact that it reduces energy consumption is still another important advantage. If you leave a room or the home, the lights will turn out by themselves, the plugs will be turned off, and the thermostat will be set to a lower temperature. A smart home may make living much less difficult for those who struggle with mobility, such as the elderly or people with disabilities. (Internet of Things Portal (2016) b; Patrick (2017))

2.4.3 Smart cities

Cities are home to a wide variety of use cases for Internet of Things devices. They are able to assist with road monitoring and help improve traffic signals and railway crossings to make the flow of traffic more seamless. They will assist drivers in more quickly finding a spot to park by using an intelligent parking space search. In the field of waste management, sensors will monitor the filling of the container, which will make the whole process more effective while also optimizing both financial resources and the amount of time spent on it. The quality of the air and the decibel level of noise may both be measured by IoT devices. (Meola 2020a)

2.4.4 Agriculture

In the field of agriculture, technological advancement is nothing unusual, and the internet of things is not an exception to this rule. Agriculture will reach a whole new level as a result of the many possibilities offered by the usage of IoT. Farmers are rapidly adopting the usage of smart agricultural practices, such as deploying drones and installing sensors. They increase productivity and automate routine job operations throughout the production cycle, including as watering, fertilizing, and controlling pests.

The cultivation of crops in the right and effective manner requires the use of sensors that are embedded in the soil in the fields. These sensors collect data on the soil's temperature, acidity, and other characteristics.

Farmers now have the ability to remotely check the status of their equipment, crops, and animals by using mobile apps. They are provided with information on the quantity of crops

produced, as well as information on the feeding and production of animals, by means of detailed statistics. They are also able to forecast future agricultural and livestock statistics based on data that has previously been collected thanks to the technology. These forecasts will make it possible to distribute items more efficiently and at a lower cost.

Farmers also employ drones in agriculture to get a bird's eye view of their fields and collect the most recent data on the growing season of crops and how well they are doing overall. Farmers will employ drones to spray the rejuvenating substrate if plants begin to wilt. This helps them minimize losses. The future of agriculture is in the collecting and analysis of massive amounts of data, with the end objective of increasing crop output and distribution efficiency while decreasing costs. This will be accomplished via the use of big data. (Meola 2020b)

2.5 Advantages and Disadvantages

Utilizing the Internet of Things confers many advantages and conveniences into our daily life. The protection of our homes, companies' warehouses and places of employment may be ensured by installing security cameras that monitor the areas visually. We are able to monitor their transmission from any location using our mobile devices and PCs. There are also motion sensors built into some of these cameras, which send us messages whenever there is an activity in the vicinity of the camera. The use of smart locks is also counts as benefit because, even if we are hurried and prone to forgetting things, we can use a mobile application to check the status of these locks and possibly lock or unlock them remotely [27]. This is especially helpful in situations in which we are prone to forgetting things. One other reason we invest in smart technology is to reduce our overall energy footprint. In this sense, the exterior temperature sensors, in conjunction with the data from the weather prediction, let us save money while simultaneously optimizing the room heating.

The Internet of Things has several potential drawbacks, the most significant of which relate to the safety of individual devices and the vast amounts of information such devices gather about their environments and the people who use them. Because of

negligent usage on the part of customers or inadequate security measures taken at the manufacturing facility, some gadgets no longer have adequate protection [31] [32]. They are thereby rendered an easy target for attackers, as well as a source that may be used for the latter's nefarious purposes. In the next chapter, which is titled "IoT Security," we will discover how attackers may take advantage of IoT devices that have a low level of security or none, as well as what the most typical places of vulnerability are in IoT devices. (2017), Quarry and Pibyl

2.6 Applications

There are many different uses for IoT, which we can simplify by dividing it into the following categories: the Industrial Internet of Things and the Commercial Internet of Things. Internet of Things (IoT) for Consumers.

2.6.1 Internet of things in the industrial sector

The majority of IoT expenditures and applications are concentrated in the field of industrial IoT (IIoT). It developed what is known as machine-to-machine, or M2M, communication, which is communication between machines that do not include the involvement of people. There are usually existing automated industrial systems in factories; however, these systems are frequently too old, and it is extremely difficult to connect these devices so that they can support the internet of things (IoT). Additionally, these businesses need assistance over an extremely extended period [5]. The Industrial Internet of Things is an integral component of the digital transition. The so-called "fourth industrial revolution," often known as "Industry 4.0," is already underway. [42] As a result of this transformation, smart factories are being created, which will replace humans with robots in the performance of labor that is routine and straightforward. It is anticipated that the implementation of this adjustment would result in cost and time savings as well as an improvement in the firms' degree of adaptability.

The Industrial Internet of Things is used in industries such as manufacturing, agriculture, smart cities, and building automation. Inventory management, smart farming,

optimizing energy use, and many more fields are only some of the applications of this technology. Through the monitoring of processes and the quality of products, IIoT enables improvements in production efficiency. Enhancing already in place processes and generating forecasts, it may result in time and financial savings.

2.6.2 The internet of Things for Commercial Purposes

This category is in the middle between Consumer IoT and Industrial IoT. It often needs to understand each of these perspectives. These networks may consist of a few devices or as many as thousands. The healthcare industry, hotel services, and retail are examples of businesses that employ commercial IoT. [42] In order to provide a more positive experience for patrons of establishments that get a high volume of visits, such as office buildings, supermarkets, hotels, and hospitals, these kinds of devices are regularly installed there.

2.6.3 The Internet of things for consumers

The Internet of Things (IoT) geared for consumers focuses on helping individuals make better choices so they may enhance their lives and the job they do. focuses on individuals or families the majority of the time. The primary function of consumer Internet of Things devices is to carry out actions and provide services on our behalf. The hardware is often fairly cheap, but it requires very little maintenance and has a short lifespan. [42] It is rather common practice to trade them in for more recent versions. The majority of the time, you'll find them installed in smart homes, where they serve various purposes, such as providing home security and monitoring systems, smart thermostats, domestic robots, and many more. The Internet of Items is also employed in healthcare to help us live better lives, in wearable technology, and in the monitoring of our treasured things, such as our pets and cats.

2.7 Blockchains Designed with IoT in Mind

There are several approaches that may be taken to the challenge of connecting the end devices and gateways of the internet of things with the distributed blockchain technology and the networks that support it [6][12].

2.7.1 Approach That Combines Both

In this particular architecture, sensor nodes, along with other devices that are a part of the Internet of Things infrastructure, also serve as the backbone of the blockchain network. Because the blockchain records every contact made by Internet of Things devices, it is possible to track every transaction and communication made across a network. Given the general status of existing blockchain solutions as well as the increased bandwidth and data storage needs of this model, it is very unlikely that this model will ever be implemented using the "regular" blockchain solutions. It is necessary to develop a blockchain model that is tailored uniquely for the interaction of the internet of things and blockchain [47]. The IOTA project, which is centered on Internet of Things (IoT) blockchain scenarios and also leverages lightweight nodes that may be operated on sensor nodes, is the blockchain that comes closest to this approach [37].

2.7.2 Method with a Divided Approach

The internet of things (IoT) network and the blockchain network are kept fundamentally distinct in this paradigm. In order to link the two networks while ensuring that none of them suffers any damage, intermediary gateways are used. All of the information and communication is routed via the gateway, which is communicated with by the end devices of the Internet of Things network. The gateways are generally devices that are able to do actions that need more resources and, as a result, function as complete blockchain nodes. If a closed IoT network has many gateways, then some of those gateways may be able to run a lightweight blockchain client to alleviate some of the strain placed on the primary gateway. The least amount of configuration and interference with the existing networks is required by this architecture. As the interactions between IoT

devices take place independently of the blockchain, the latency and speed of these transactions shouldn't be impacted. Nevertheless, it is a little departure from the concept of blockchain functioning as the central nervous system of an Internet of Things network [28]. We are moving toward a more centralized architectural design by giving a gateway the ability to carry out all blockchain-related actions, even if the gateway itself will continue to be kept secret. Despite this, it may still prove to be a valuable approach in some circumstances, such as those in which an existing network of sensor devices must be linked to blockchain technology and the interactions between IoT devices must take place with a minimum amount of lag time. One example of a scenario in which such a model could be implemented is in the context of a smart home. In this scenario, an existing Internet of Things (IoT) infrastructure of a smart home would be connected to a blockchain solution via a central powerful gateway. This would allow the smart home to take advantage of the capabilities of blockchain technology without the need to alter the devices that are already part of the IoT home network.

2.7.3 Method combining both

This model depends on the presence of light blockchain nodes, which are designed to communicate with the blockchain network but do not necessarily directly perform mining or signing of transactions. Instead, light blockchain nodes only store relevant data fragments and do not perform these other functions. A portion of the Internet of Things devices are able to function as full nodes, a portion of the sensor devices run light blockchain clients, and the remaining portion of the devices are able to work solely to collect sensor data or perform other tasks necessary in IoT use cases and communicating the data to devices that are running blockchain clients [17]. Because a portion of the internet of things network can continue to be optimized for task-specific operations while still benefiting from the properties of the blockchain, careful execution of this model could be the most optimal way of combining both technologies. This is because of the fact that blockchains are distributed ledgers. This model is currently more realizable as a combined one because it permits the gradual incorporation of the blockchain technology into the sensor devices and because an increasing number of blockchain solutions come with light

clients or Application Programming Interfaces (APIs) that are able to communicate with the blockchain network without taking on the responsibility of being a full node. Both of these factors contribute to the fact that the combined model is currently more realizable [16].

2.7.4 Exploration and Experimental Development

The article [58] presents and compares three alternative topologies, each of which is centered on the front-end portion of blockchain-based IoT applications. A stand-alone Ethereum node, a remote client with a local key store, and a remote client with a remote key store are the three designs that may function with the Ethereum blockchain. The differences between these architectures lay in the placement of the blockchain clients and key stores. Their demonstration experiments indicate that a situation in which a complete Ethereum node is operating on an IoT device is not currently particularly practical. This is something that they have shown.

IOTA [56] is a cryptocurrency that was developed specifically with the Internet of Things and micropayments between machines in mind. The emphasis placed on the Internet of Things is evident in features such as high scalability, the absence of transaction fees, and rapid confirmation of transactions. There is no entire ordering of transactions in a chain of blocks as there is in typical blockchains; instead, a Directed Acyclic Graph (DAG) of transactions is employed. This contrasts with standard blockchains. The decentralized application graph (DAG) is referred to as the tangle, and it is constructed from transactions that are coupled by edges that reflect approvals of transactions. Each node in the network is responsible for validating and approving two transactions from two other nodes at random before it may add a new transaction to the graph. There are no benefits to be gained by doing this. In order to prevent spam and Sybil attacks, each node is required to solve a cryptographic hash problem (using the SHA-3 hash function) [14], however, the proof-of-work procedure is only carried out once for each transaction at the moment it is generated. With this method of constructing the tangle, the scalability of the network and the speed at which transactions may be processed both improve along with the number of nodes and transactions that are participating. There are two distinct kinds

of nodes in IOTA: core and light (for resource-restricted nodes). In essence, Ethereum [25] was the first blockchain-based platform to present the idea of smart contracts to the public. A smart contract is a self-executing bit of computer code, the behavior of which is predetermined and can be seen by anybody on the blockchain. The Ethereum Virtual Machine must be running on each node before smart contracts can be put into action. Additionally, it incorporates a high-level programming language known as Solidity, which can be used to write smart contracts. In addition to being applicable in non-financial contexts, Ethereum makes use of its own native money, which is known as ether. In addition to its usage as a standard form of money, Ether may also be put to use as a form of payment for calculations carried out (through smart contracts) by other peer nodes. Ethereum is one of the most active communities of developers and technology enthusiasts, making it one of the most popular technologies to speak about and utilize when it comes to the topic of blockchain for IoT. There are now various interesting blockchain systems that are undergoing study and development, such as the Taraxa [57] and Radix [61] projects, both of which evolved from the NANO cryptocurrency project [NANO]. [NANO] "a solution to the double-spending issue utilizing a peer-to-peer network of nodes with logical clocks to provide temporal evidence of the chronological sequence of events" is what the Radix project is attempting to uncover. Taraxa is an exciting new blockchain that includes smart contracts in its architecture. These smart contracts have revolutionary concurrent schedules that allow them to execute in parallel. Speculative concurrency techniques are used as the foundation for the creation of concurrent schedulers.

In [33], a blockchain is presented that aims to enhance the properties of Bitcoin and is improved for IoT. [33] The architecture that has been suggested is composed of three levels: dazzling home, overlay, and distributed storage. The overlay is a decentralized peer-to-peer network with hubs grouped together in bunches. They make use of a cloud-based system for archiving their data. Within each level, elements are communicated with one another through the use of exchanges. A proof-of-concept implementation that illustrates the combination of the Internet of Things, which is communicated with by LoRa hubs [39], and blockchain, which is communicated with by a private Ethereum organize, is represented in [60]. They make use of blockchain technology in order to "promote a

decentralized IoT stage and standardize the handling of information between the end devices and the IoT framework."

IoTChain [63] is focusing on the safety aspects of blockchains for Internet of Things applications. They propose a blockchain-based security architecture for the internet of things, in which the blockchain provides "an adaptable and trustless approach to deal with approval." In essence, they are suggesting the replacement of a centralized approval server with a decentralized record.

Many organizations, including enormous partnerships like IBM, Amazon, and Cisco, among them, started investigating the potential outcomes of combining IoT and blockchain, and every one of the plans or at the very least investigated at some level a methodology of how to use these new innovations. In this proposition, we take a look at the various approaches that are being taken in the minds and flow of research that is currently being done. See the [62] for a comprehensive rundown of other available papers and activities related to blockchain and the internet of things. This overview paper documents and analyzes blockchain-related Internet of Things (IoT) papers and projects according to the scenario for which they are most proposed, which are as follows: Smart Home, Smart Industries, Smart Grid, and Smart City. Additionally, it considers the current development levels of several blockchain solutions for the Internet of Things (IoT).

2.8 Storing Data on Blockchains

Wrapping the data in regular transactions is the method of storing data using distributed ledgers that is the quickest, easiest, and most basic way to do it. The vast majority of blockchain implementations make it possible to send individualized transaction details alongside the standard information required for the transfer of a transaction. For instance, information may be saved on the IOTA tangle if one so chooses. On the other hand, this strategy is often quite unsuccessful since the quantity of PoW that has to be computed rises in proportion to the size of the transactions being processed. In addition, transactions, and blocks each have their own size constraints and often enable only very tiny data to be attached. For the purpose of providing context, the size of a single IOTA transaction at this time is 1650 bytes.

In [36], a proof-of-concept approach for Internet of Things devices to store data and exchange it with one another using IOTA is detailed. They provide further evidence that there is a significant opportunity to integrate sensor data into a distributed ledger without the use of complicated database management solutions. However, the findings also demonstrate that resource-constrained devices are not currently capable of performing PoW, which is essential for IOTA transactions. Instead, the test nodes are being operated on desktop computers at this time. There are blockchain systems that are compatible with cloud storage, the majority of which are descended directly from Internet of Things solutions. It does go against the nature of blockchains to be decentralized, but in some private network scenarios, for example, cloud storage could work and could even be a more reasonable solution than a more complicated decentralized one. An example of this would be if a blockchain were to be stored in the cloud. IoT use cases often include the exploitation of cloud storage, and blockchain is only a supplemental service that is offered in conjunction with the whole system.

A strategy that makes use of cloud storage is investigated in the context of a smart home setup in [30]. The structure that has been presented is organized into three levels: a smart home, an overlay network, and cloud storage. Within tiers, communication between entities is accomplished through the use of transactions. The cloud organizes the storage of data into identical blocks, each of which is assigned a different block number. When a user accesses the data, they are required to authenticate themselves using a combination of the block numbers and hashes of the data that was stored.

Making the storage itself decentralized is the most logical course of action to take in order to realize the goal of completely decentralized blockchain solutions (which include data storage capabilities). Given that scalability and fault tolerance are two of the most important characteristics of Distributed Hash Tables (DHT), this seems to be the most appropriate use for them. "Distributed hash tables, often known as DHTs, are decentralized systems that provide routing and look-up services. The key-value pairs are stored in the system in a decentralized fashion. Any node can access any other node in the network by providing only its identifier and using it to retrieve the associated value for a key. Due to the lack of any form of central coordination, DHTs may be thought of as a

kind of organized peer-to-peer network [52]. DHTs may also be used in a variety of different contexts. It is possible to use their efficient implementation of node lookup in order to either disseminate information across the network or engage in confidential communication between nodes. [46] outlines "a distributed data storage strategy that makes use of blockchain and certificate-less cryptography." A storage solution for Internet of Things devices that makes use of blockchain is detailed. The system that has been presented makes use of edge computing in order to handle connectivity with devices and to execute storage activities using blockchain. They suggest using a DHT as a means of data storage. The files themselves are kept in the Distributed Hash Table (DHT), while links to those files are recorded on the blockchain [23].

Within the context of the Internet of Things (IoT), a proposal for a blockchain that features distributed access control and data management has been presented in [63]. They employ a P2P overlay routing technology in conjunction with a DHT to achieve a distributed storage. They also improve encryption, compression, and search capabilities over the material that is kept on DHT.

Enigma [50] is yet another P2P blockchain technology that uses DHTs to solve the issue of inadequate data storage. It makes it possible to store data and enables other nodes to do calculations on them while maintaining the confidentiality of the data. In order to accomplish this goal, it implements several strategies for pseudonymization, in which the data are dispersed throughout the peer nodes and isolated from their references. In addition to that, the data that is being distributed is encrypted. "a modified version of the Kademlia [50] DHT protocol for storing shared secret data chunks and an external blockchain to govern network monitoring, access control, and identities" are the primary components of the Enigma system. [59] It is possible to do computations on privately shared data by adhering to the procedures outlined in Secure Multi-Party Computation [40][43].

Holochain [41] is a scalable framework for distributed computing that makes use of DHT for data management. "Holochain application consists of a network of agents maintaining a unique source chain of their transactions, paired with a shared space implemented as a validating, monotonic, sharded DHT where every node enforces validation rules on that data in the DHT as well as providing provenance of data from the

source chains when" "Holochain application consists of a network of agents maintaining a unique source chain of their transactions, paired with a shared space implemented as a [41]

2.9 Attacks on IoT

This chapter's objective is to familiarize readers with the security concerns associated with the Internet of Things devices, especially the numerous assaults that target these devices. In addition to this, readers will get familiar with the OWASP Foundation and their IoT security project, which outlines the 10 aspects of IoT device security that are considered to be the most important. At the conclusion of the chapter, the audience will be provided with information on the many security choices for Internet of Things (IoT) devices, which they may then use in their own IoTs at home [4].

Concerns over the safety of the Internet of Things are growing in tandem with its expansion. Not only is the Internet of Things devices popular with end-users and business owners, but also with cybercriminals. Because it has so many security flaws, the Internet of Things offers a broad attack surface and many potential entry points for hackers. (Revue 2019).

During manufacture, many Internet of Things devices has safety flaws. The functioning of these goods is often given a higher priority by the manufacturers than their overall level of safety. The primary motivation for carrying out this action is for marketing purposes. They want to introduce a high-tech product that will be sold at an affordable price and will have several different applications for its users. One of the reasons why manufacturers do not engage in open warfare with one another in the market is because of pricing and price competitiveness[11].

The security of Internet of Things devices is also dependent on the end-users who own and use these devices. When this happens, consumers, particularly those who do not care about the security of their smart gadgets, are more likely to fall victim to security flaws. They do not update the software, use passwords that are either default or insecure,

and outright buy Internet of Things devices that have no security at all. They leave many open doors for hackers to break through and launch attacks. 2016 according to Matthews

2.9.1 Different types of online attacks

Because they have so many flaws in their security, Internet of Things devices are susceptible to a high volume of separate cyberattacks. It's possible that the primary target of these attacks is not the direct users of Internet of Things devices, but rather other businesses or organizations and the Web services or servers they use. The following are some of the most well-known forms of cyberattacks that, among other things, can target or exploit Internet of Things devices. (Caravelli and Jones 2019)

2.9.1.1 DDoS

An assault that uses distributed denial of service, or DDoS for short, is known as a distributed denial of service. The purpose of a distributed denial of service attack (DDoS) is to prohibit users from accessing the targeted server, network, website, or service by either partly or totally interfering with its normal functioning. This might result in financial harm as well as damage to the operator's reputation and goodwill if it is not remedied immediately. An incident of this kind takes place whenever the network is inundated with a huge number of requests that the target server is unable to handle and, as a result, it crashes [51].

An adversary, in order to carry out this kind of assault, must first take control of a number of different devices that are linked to the internet. Computers, laptops, and the Internet of Things (IoT) devices are included in this category of electronic equipment. In order for them to take control, they take advantage of flaws and security vulnerabilities in not just IoT devices but also in the command and control software, which eventually morphs into a bot or a boot. After then, the attacker has remote control over a collection of these compromised computers, also known as bots, which is referred to as a botnet. The attacker will then utilize the remote control to input a command into the botnet, which will subsequently be carried out by the device bot. For instance, every bot will submit a request to a certain server or service, but since there is an excessive amount of data, the request

will be ignored, and the bot's activity would be halted. It can be challenging to differentiate between normal traffic and an attack due to the fact that each bot is typically considered a legitimate Internet device. (CISA 2019, undetected by Cloudflare)

2.9.1.2 Brute force

An assault using brute force is a method that may be used to discover user credentials, as well as perhaps a hidden website or encryption key. The method is based on the concept of learning by experience. Even if this tactic of assault is no longer used, it is still widely used because of its effectiveness.

An adversary makes an effort to find the right credentials by attempting a number of different random combinations of username and password. Because it would take an unreasonable amount of time to crack the username and password manually, hackers have developed a variety of tools to speed up the process and make it much more efficient overall. On the other hand, the amount of time needed to break into a user account might range anywhere from a few seconds to units, tens or hundreds of years, or even longer in certain cases. The length and level of difficulty of the password are the primary determining factors in this regard.

A brute force assault is carried out with the use of specialized tools and, for the most part, makes use of either one or two lists. This is determined by whether the attacker is in possession of any login information, which may be in the form of a name or a password. The first list on this page comprises names, while the second list has passwords. Both of these lists contain various types of login information. The tool then puts every combination from these two lists through a series of tests, gets rid of any combinations that don't work, and then stores and catalogs the ones that do.

2.9.1.3 Man-in-the-middle

In the field of computer science, the phrase "man in the middle," which is shortened to "MITM," is used to refer to the name of an assault against cryptography, or more

specifically, an attack on encrypted communication between two systems or individuals. This assault may take place in any type of online communication, such as communication carried out via e-mail, social media, programs, or websites. 2019 edition of Norton

The aggressor makes an effort to break into the communication channel between the two subjects and act as a middleman between them as a result. As a result, he will be able to listen in on this conversation without the participants noticing, which will give him access to a wide variety of information, including that which is private, confidential, and other types of data. Alternately, it is possible that it may change the substance of the messages in a covert manner by stopping and diverting the receipt and transmission of the communication channel. This would hopefully discourage the use of fake hacked subscriber information. However, they are unaware of this fact and continue to think that they are speaking with one another directly. Given that the attacker is in possession of the information included in the first communication, there is a chance that he will be able to convince these people that the altered message is genuine. (DuPaul undated)

Having said that, the communicating party can be anything from a person to an Internet of Things device or even something else entirely. An adversary may, for instance, submit fake data on the temperature of the device, which would result in the gadget overheating, which would then lead it to malfunction. This might result in the actual equipment breaking down, in addition to causing financial harm to the companies who own the equipment. (Simko 2016)

2.9.1.4 Ransomware

Ransomware is a sort of malware or malicious code that is used to encrypt files or data and limit access to devices such as computers, phones, Internet of Things devices, or whole networks. It is also often referred to as extortion software. Ransomware is used to extract money from victims. Users are often held hostage for financial gain using this tactic. The infected entity must pay the attacker a certain sum of money before the attacker will reopen the device and decode the contents. The infected user has a limited period of time to execute the request and failing to do so will often result in an increase in the amount of money that the attacker has asked. The payment of the predetermined amount does not, however, provide a 100% guarantee that the offender will uphold his end of the

bargain. When a user opens an infected attachment in an email, visits a website that hosts ransomware, or it spreads across a local network, ransomware is introduced into the system. It is simple to determine whether or not the system has been compromised. The user may either be prevented from accessing certain files or the whole device, or they will be sent warning messages that flash up on their screen.

The ransomware in its most basic and least harmful version will just attempt to fool a user into believing that something is wrong with their device—for example, that it is infected with a virus—and will demand money from the user in order to cure it. This particular strain of ransomware makes itself known by producing windows that come up incessantly with a cautionary message on the infection of the machine. However, because I just use them to frighten the user of a truly non-existent danger, it does not really encrypt any data or the system itself. In this scenario, the user has at least some level of control over the system; thus, the main issue he is facing is the persistent appearance of warning windows. These bothersome windows may be removed in a number of different ways. Anti-malware programs are used to do this, which the user either does by switching the device into its security mode or by downloading the tool to a removable disk and then connecting the disk to the device in order to run the tool via the disk.

Ransomware that encrypts files is a far more dangerous type. In addition to locking the user's device and preventing him from signing on to the system, they encrypt the data that is stored on the user's device. Because they employ very robust encryption techniques, it is often impossible to remove them after they have been installed. You need the key that the attacker uses to decode them, and the attacker will not provide it to the user if the user does not pay the ransom. Users of devices should back up their data on a regular basis, ideally in a location where it will not be visible online. This is because there is no reliable method of protection against these forms of ransomware; thus, there is no alternative except to advise users to back up their data. (Zahra and Chishti 2019)

2.10 OWASP (Open Web Application Security Project)

Mark Curphey established the Open Web Application Security Project (often known as OWASP) on September 9, 2001. OWASP's full name is the Open Web Application Security Project. It is concerned with the safety of software and programs used on the internet. It makes papers, approaches, documentation, tools, and technologies that deal with security and security challenges in software and online applications publicly accessible to businesses, developers, and technologists, as well as the general public. (OWASP undated; Wikipedia 2020)

OWASP Internet of Things

2014 was the year that saw the beginning of the OWASP Internet from Things project. This project's objective is to assist software developers, hardware manufacturers, individual customers, and commercial enterprises in gaining a better understanding of the risks associated with the Internet of Things and the security of connected devices. The Top 10 initiative aims to address the ten most pressing concerns about safety and security.

The OWASP IoT Top 10 project's most recent version was released in 2018, and the primary focus of this iteration is on simplification. (OWASP 2019) This list is geared at all parties involved, including businesses, customers, developers, and manufacturers. The following are the outcomes of the project that was carried out in 2018:

OWASP Internet of Things Top 10 Risks:

1. Passwords that are either easy to guess or are hard-coded.

2. Services on the network that are not encrypted

3. Ecosystem interactions that are not adequately protected

4. An update method that is not sufficiently secure

5. The use of components that are either insecure or outdated

6. Inadequate protection of personal privacy

7. the transport and storage of data without adequate security

8. Insufficient equipment management

9. Settings by default that are not safe

10. Insufficient resistance to physical exertion

2.11 Security of IoT in The Home for Users

The end users themselves are the ones who should be responsible for ensuring the safety of their Internet of Things devices both inside and outside the house. It is not a good idea to put all of your faith in the fact that a certain Internet of Things device will be adequately secured from the manufacturer [1]. Therefore, it is important for the user himself to take specific precautions in terms of security in order to assist avoid assaults on Internet of Things devices. It is vital for the user to pay attention to the correct security of their equipment since even the finest protection from the manufacturer will not assist protect against some dangers.

2.11.1 Survey

Before an end-user makes the purchase of their "dream" Internet of Things gadget, they should take the first and most essential step in securing their smart home. The essential safety features are not included in every Internet of Things device currently on the market. Therefore, it is essential to begin by doing research on both the equipment and the company that made it. Check to discover whether the device has ever been the subject of a security breach and if it has, investigate the reasons for the incident. In addition, it is important to make certain that IoT is still interested in the product and continues to give continuing system upgrades after it has built the device. If this is not the case, then there is no use in having it made in the first place. It could be beneficial to find out what others think of the company's reputation and whether or not they put their faith in it. The price of a thing should be, in the end, the deciding factor in whether or not to purchase that product. It is not recommended to purchase a device for the eye that is very cheap, as it is

highly possible that the maker of such a product has not spent anything, or has invested very little and not enough, in the safety of a smart gadget. Because making an investment in the security of an Internet of Things product is not a low-cost endeavor, it is appropriate for customers to avoid cutting corners in this area. (Chauhan 2019)

2.11.2 Passwords

Passwords provide not just on the Internet of Things but also elsewhere one of the most significant and widespread security challenges. IoT devices that have a password that is simple, the factory default or that can be broken in another way are vulnerable to attack, and the greatest efforts of manufacturers to safeguard them won't help protect them. They become an easy target for the attacker, and as a result, consumers, corporations, and organizations are put at a higher risk of being subjected to a cyber assault.

The user who sets the default password for a device is led to believe that the gadget is more secure than it really is. These passwords are almost always the same for a given category of products, and as a result, they are simple to uncover. As a result, it is essential for each individual end user to alter it as soon as possible after the activation of the device. (Poremba 2020).

It is not considered to be very proper to use the same passwords for many devices and potentially even accounts. If an attacker launches an attack, for instance, on a website where the user has an account and is successful in obtaining the user's password and other credentials, the attacker may then track other accounts linked with that user and access sensitive data from sources other than IoT devices. Experts in the field of cyber security advocate for the use of passwords that are both robust and one of a kind. This is done to provide protection against cyber assaults, the theft of data, and other security risks [45].

"A strong password is at least 10 characters long and includes a combination of uppercase and lowercase letters, numbers, and symbols," says Thomas F. Duffy, senior vice president of operations and services for the Center for Internet Security (CIS), which provides the following definition of a secure and unique password: A password is considered to be "unique" when it is only used for one particular account. (Duffy 2016) On the other hand, a secure password should not include any common terms, even if the

letters are substituted with characters that have a similar form or another pattern that may be guessed. The brute force attack, in which customized dictionaries are used in conjunction with the approach, may be used to crack passwords generated in this manner [34].

On the other hand, it might be challenging to commit a large number of secure and unique passwords to memory. On the other hand, this is something that may be delegated to the password manager. A program is known as "Password Manager" is one that safely keeps passwords. In addition, certain password management solutions come equipped with the capability to generate a random and robust password on the fly. Appropriate countermeasures In addition to using robust and one-of-a-kind passwords, it is always recommended to alter these passwords every once in a while.

2.11.3 Update

If the user does not keep the firmware or software on his Internet of Things devices and other devices up to date, he puts himself at a higher risk of being attacked by malicious actors. The maker of this device releases updates on a regular basis, and one of the purposes of these updates is to repair various mistakes in the software code, including those related to security. Every user ought to upgrade their own gadgets as quickly as they can, and they shouldn't put it off until a later time. This improves the overall security of your devices and decreases the likelihood that an attack will be successful.

2.11.4 Settings

The manufacturer may be able to modify the default settings of the device and the programs it contains in a way that is more advantageous to the manufacturer than to the user. It is helpful to learn what information the device gathers about the user of the device and to think about adjusting the user's privacy and security settings. Alternately, you might deactivate some functions that the user does not need at the moment, such as voice control, motion detection, the user's current position, or remote access. The user has the ability to re-enable these features at any point, should he choose that he needs them and wants to

make use of them [26]. Disabling features that aren't essential will make the system less vulnerable to attack. (Brown 2016)

2.11.5 Terminal equipment

The majority of devices connected to the internet of things can be controlled by a terminal device. One example of such a terminal device is the cell phone, which is by far the most widely used electronic device today; however, it might also include PCs, laptops, tablets, or central control units. Not only should users protect their Internet of Things devices, but also the end devices that connect with those devices. This is of the utmost importance. This is due to the fact that they are capable of containing personal as well as other private important data and information that is not limited to that which is obtained via IoT device apps. It is essential to use a password, PIN, fingerprint, or facial recognition that is both robust and one of a kind in order to protect the terminal. In addition to this, it is important to remember to do routine software upgrades on the terminal.

Chapter 3

Methodology

3.1 Introduction

The project activities are done according to the flow chart in Figure 3.1. The procedure shows the activity from the beginning of the project until it is completed. The first two steps have been discussed in previous chapters.

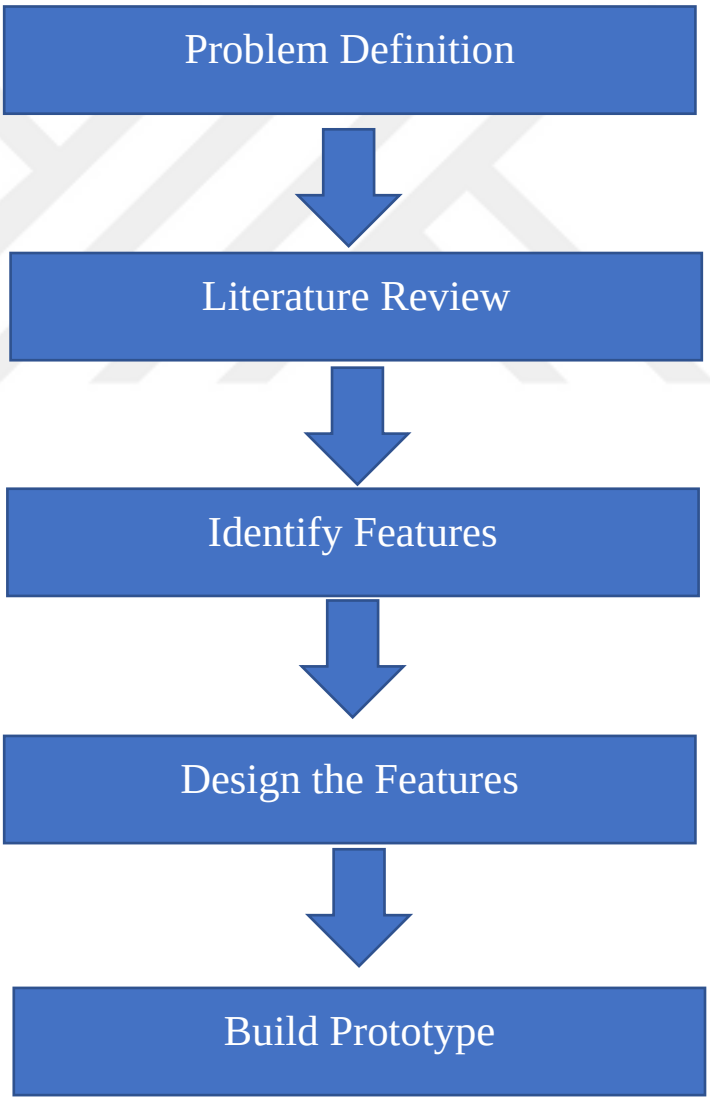

Figure 3.1: Methodology

3.2 Identify Features

3.2.1 Android application

We have developed an Android application using java programming language with android studio IDE, Android application is used to check the access control system access by using a username, and password portal to access the second-factor authentication interface of the access control system. Furthermore, He/she could open the access control system by implementing his/her biometrics authentication using fingerprints or face recognition. In figure 3.2 the flow chart of the app.

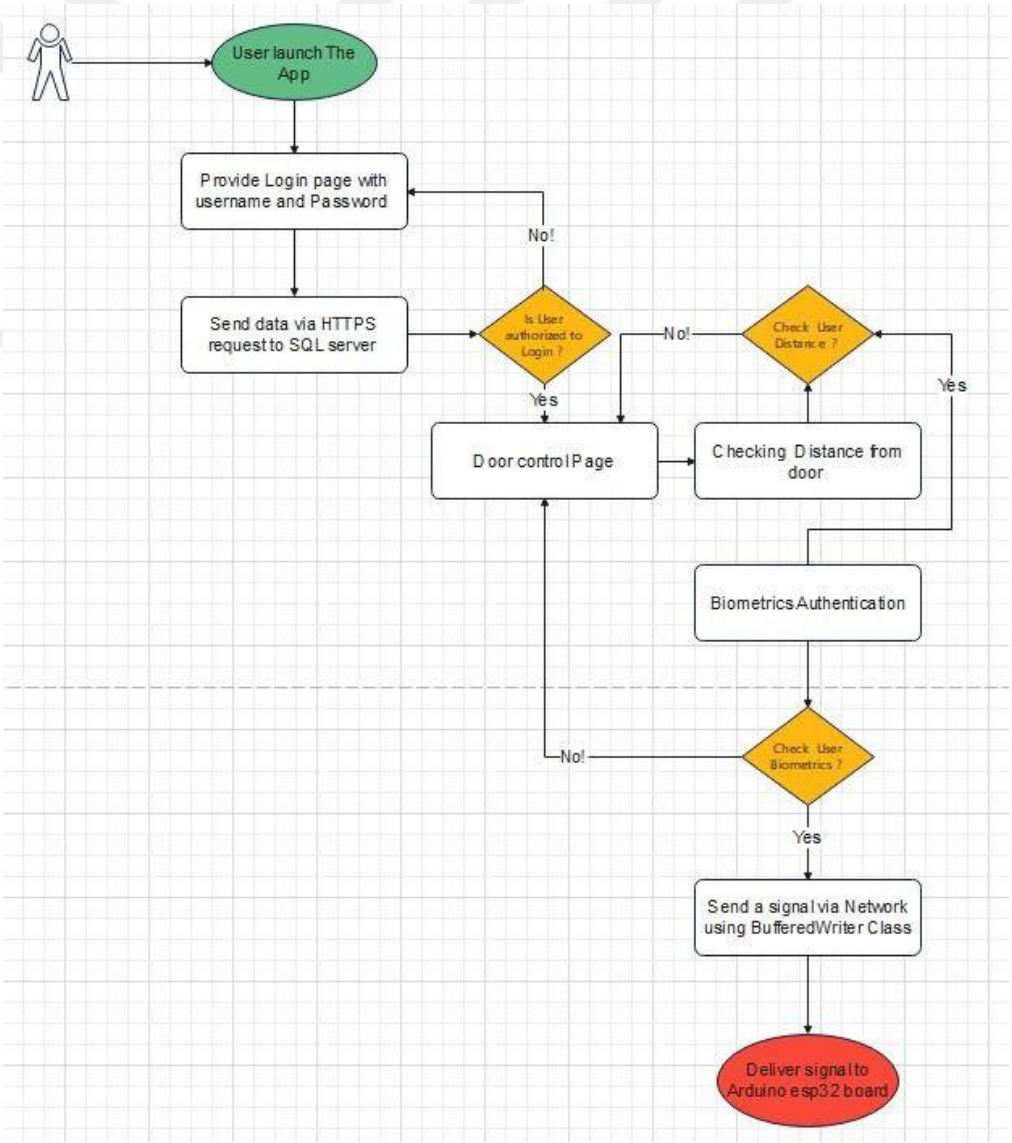

Figure 3.2: The flow chart of the app.

3.2.2 Login page

First, the user provides the page with ID or username and password to get the ability to use the access control system control page. This application checks if the user has privileges to log in and moves on to the second-factor login interface. We have used MySQL server and Apache server to verify users and store users' data as shown in figure 3.3. We have used the PHP programming language for checking and confirming users' authentications.

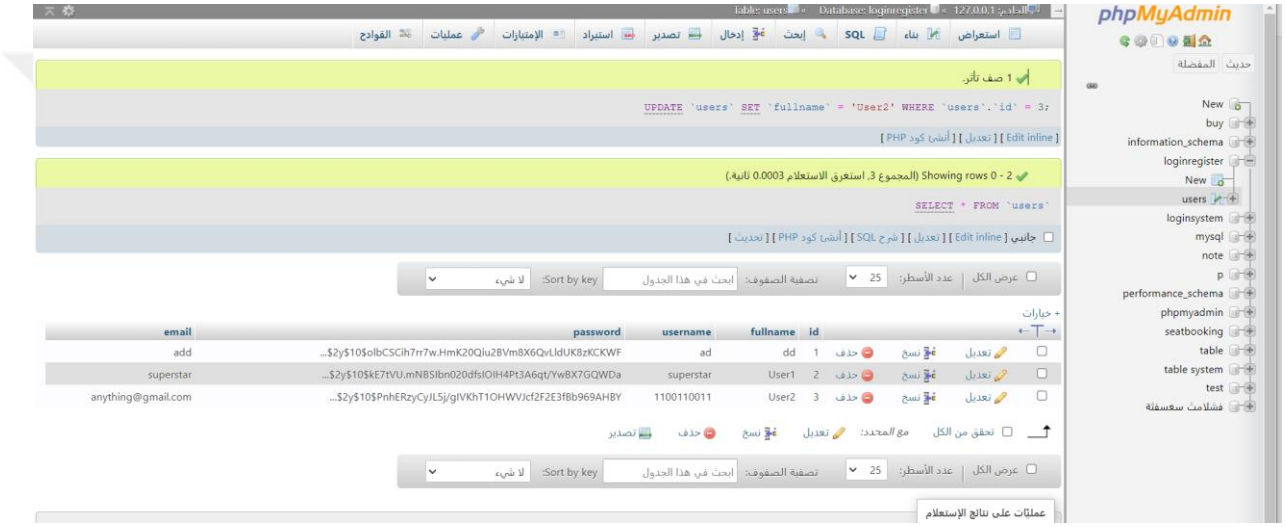

figure 3.3: MySQL server and Apache server

when credentials are submitted with the android application by the user, the android application sends HTTPS POST request to PHP Server to verify user authentication as can be seen in figure 3.4.

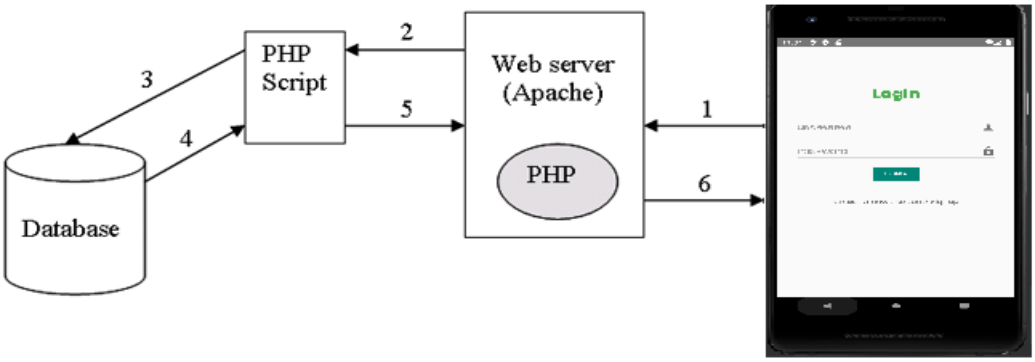

figure 3.4: Activity of Login page

3.2.3 Access control system control page

After the user succeeds in login, new interface opens for the user, in the second-factor authentication interface the user provides the needed biometrics to access control system as seen in figure 3.5. Furthermore, the user clicks open access control system button the application send a signal to complete the process.

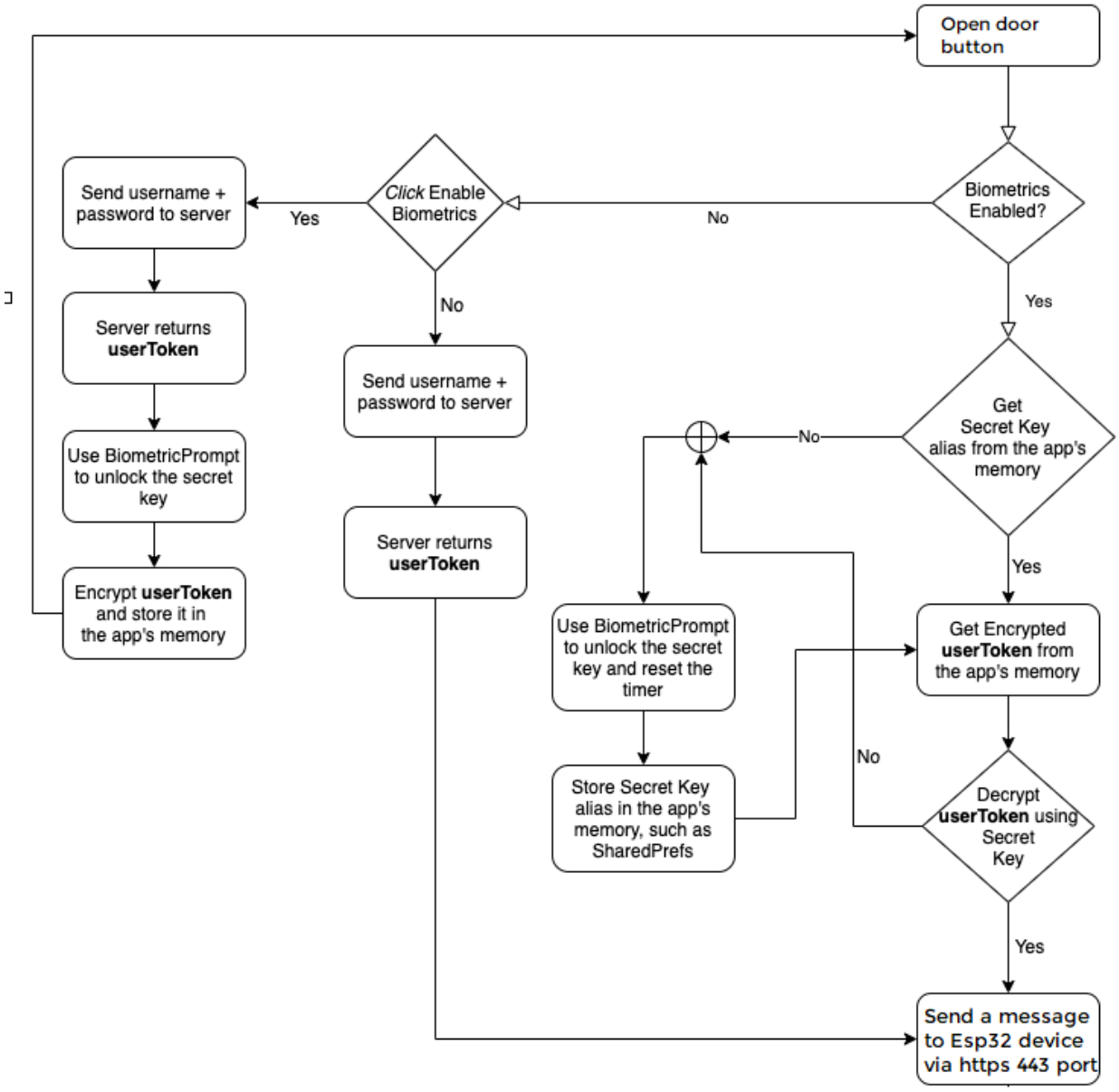

figure 3.5: Access control system open activity

There is the ability to implement authentication using the BiometricPrompt API both with and without encryption. If the developed application needs a robust security system, such as an application for a healthcare provider or an application for a financial institution, also many options could be implemented to connect your encryption keys to biometric authentication in order to verify that the user is really there. If this is not the case, using biometric authentication as a kind of convenience for your consumers may be a good idea. Both scenarios include code snippets that are fairly similar to one another. The main difference between them is that while implementing encryption, CryptoObject should be given but when implementing convenience, must omit the CryptoObject argument.

Figure 3.6 shows how the Android application sends a message via HTTPS protocol to Esp32 for access control system opening. In this process, the android application listens via UDP protocol to get the IP address of the device and sends a message to that IP via UDP protocol to open the access control system.

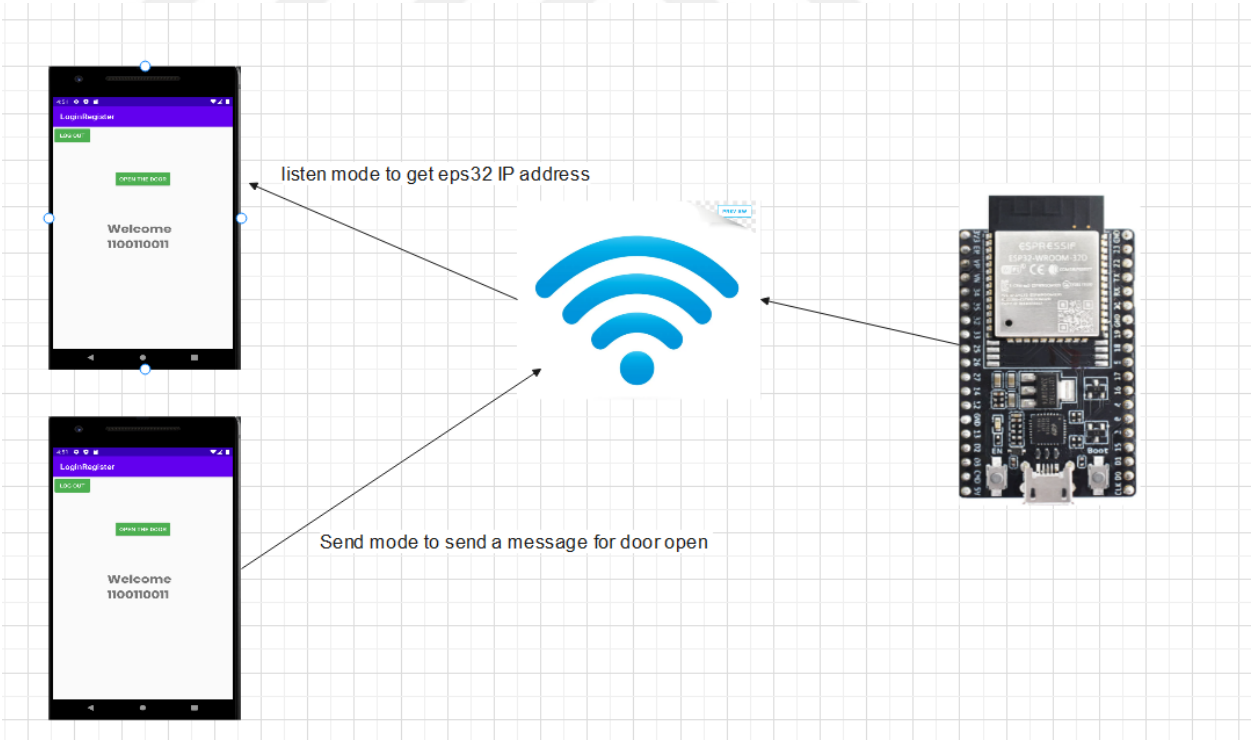

Figure 3.6: show how the Android application sends a message to Esp32 device

3.2.4 Encrypted parts of HTTPS communication

HTTPS means the transmission of HTTP data through SSL [42] or TLS [36] encryption protocols. With SSL, it is not possible to know whether HTTP data is being transmitted. Thus, it is not possible to distinguish SSL connections transmitting HTTP data from other SSL connections. It is therefore not possible to obtain useful data from the SSL protocol for the purpose of measuring HTTP headers. In the following paragraphs, the work deals only with the TLS protocol.

The HTTPS protocol begins by establishing a TLS connection (so-called TLS handshake), which takes place unencrypted. When establishing a connection, the client can use the optional Server Name Indication (SNI) header [65]. This header is used by clients to connect to the web server. According to this header, it is possible to recognize that the encrypted stream contains HTTP data. Any recognized HTTPS flows were recognized based on SNI.

Because the HTTPS protocol data is encrypted, we do not have the ability to determine the nature of the data transmitted from the encrypted parts of the TLS communication. We can only measure unencrypted parts of the communication or try to decrypt at least part of the encrypted content.

3.3 Hardware Features

3.3.1 Arduino ESP32

Arduino is a group of several single-board computers based on microcontrollers. However, it is not a classic IBM PC, but a backup board, to which sensors, modules, servos, and displays are connected rather than control and display peripherals. The project has been distributed as open source since its inception, and the language manual and external libraries are then distributed under a Creative Commons license.

The manufacturer of these boards has created a development environment identical to all Arduino products. This is called the Arduino IDE, is available for free on the manufacturer's website, and supports Wiring [42], which is a modified version of C. The environment also includes a Serial Monitor, which is used for two-way serial communication between the Arduino and the PC.

An alternative could be the Processing environment [64] using the language of the same name, enabling the creation of graphical multiplatform applications. There are several diodes, a reset button, various additional buses, connectors for ICSP (In-Circuit Serial Programming), a power connector, an oscillator, and a circuit mediating USB communication. Arduino supports the connection of expansion cards. These are called Shields for Arduino, they have mostly the same shape as the Arduino board and are connected using long pins [22].

They take up the entire area, but most of them also provide GPIO (General Purpose Input / Output) pins, so they can be stacked. Like Arduino boards, there are a few shields. Of course, the modules or sensors themselves can also be connected to the Arduino, by direct connection to the given pins. However, you need to keep in mind that the Arduino works with 5 V logic, while the RaspberryPi, for example, works with 3.3 V logic [2].

The system on a chip DFRobot FireBeetle, sometimes known as the "brains of the system," is the component of the development board that is considered to be the most crucial. The DFRobot FireBeetle Systems ESP32 is a low-cost and low-power system that has both Wi-Fi and dual-mode Bluetooth capabilities [3]. It was designed by DFRobot Systems. The chip's primary component is a dual-core microprocessor from Tensilica LX6 dual-core processer that operates at a clock frequency of 240 megahertz. The ESP32 is an ultra-low power consumption microcontroller that was developed specifically for use in mobile devices and Internet of Things applications. It accomplishes this feat by incorporating a number of power-saving features and relying on its real-time clock (RTC) and ultra-low power co-processor (ULP). Figure 3.7 presents the whole functional block diagram in its entirety and figure 3.8 show the specification of esp32.

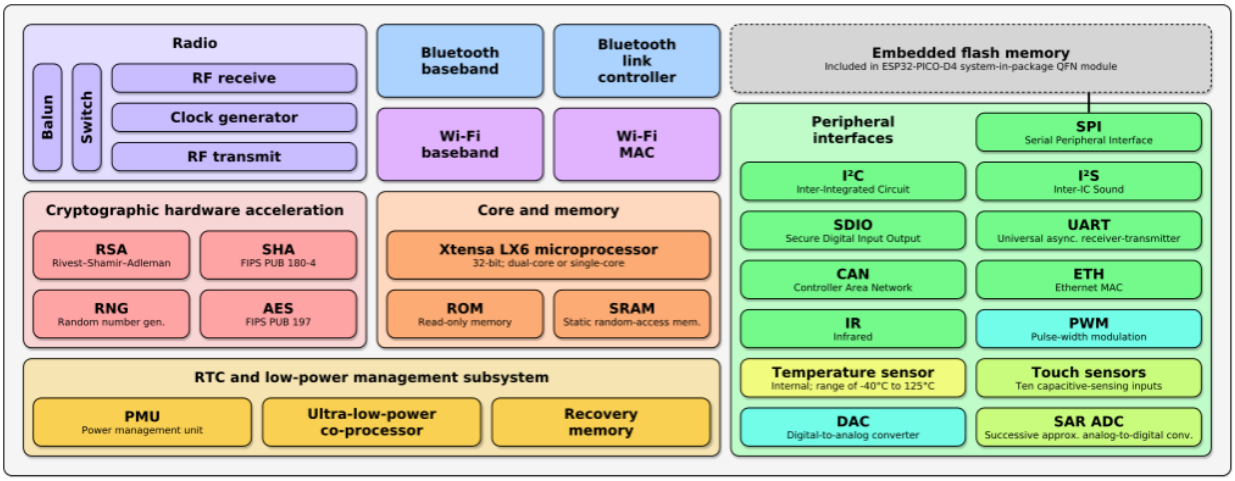

Figure 3.7: presents the whole functional block diagram in its entirety [36].

Name	FireBeetle ESP32
SKU	DFR0478
Microcontroller	ESP32
Power supply interface	USB or 3.7V Lipo
USB Powered or External (V)	3.3 - 5.0
Operating Voltage (V)	3.3V
CPU Frequency (MHz)	240
Flash(M)	16
SRAM(KB)	520
Analog pins	5
Digital pins	10
Wi-Fi protocol	802.11b/g/n
Frequency range	2.4 - 2.5 GHz
UART	1
I2C	1
I2S	1
SPI	1
Compatible IDE	Arduino IDE 1.6+
Download Mode	Micro USB
Arduino UNO Compatible	×
Lipo Charger Support	√
Dimension(mm)	58*29
Weight (g)	24 g
Key Features	Mobile BLE APP Connection Support. Two way H-bridged Motor Driver with 2A maximum current and wireless socket.

figure 3.8: the specification of esp32[65]

3.3.2 Relay model

A relay is an electrically operated switch. Many relays use an electromagnet to mechanically operate a switch, but other operating principles are also used, such as solid. Relays are used where it is necessary to control a circuit by a low-power signal (with complete electrical isolation between control and controlled circuits), or where several circuits must be controlled by one signal [21].

Features:

- 5VDC SPDT Relay
- Rated up to 10A (@125VAC)
- Fully Sealed
- Can be mounted directly into a breadboard - 300mil spacing
- Omron part #: G5Q-0609

3.3.4 Solenoid lock

A solenoid is a coil of insulated or enameled wire wound on a rod-shaped form made of solid iron, solid steel, or powdered iron. Devices of this kind can be used as electromagnets, as inductors in electronic circuits, and miniature wireless receiving antennas. In a solenoid, the core material is ferromagnetic. It concentrates magnetic lines of flux. This increases the inductance of the coil far beyond the inductance obtainable with an air-core coil of the same dimensions and the same number of turns.

When current flows in the coil, most of the resulting magnetic flux exists within the core material. Some flux appears outside the coil near the ends of the core; a small amount of flux also appears outside the coil and off to the side [20].

Features:

- Standard voltage: 10, 12, 20, and 24 volts D.C.
- Ambient operating temperature: 212°F/ 100°C
- Magnet wire: All 100 series are thermal class 200°C
- Encapsulating material: Thermoplastic polyester (PET) (RYNITE 415 HP)
- Lead wires: 18/10 gauge meets sae J1128XLPE, type SXL

3.3.5 IDE

The Arduino integrated development environment (IDE) is cross-platform and works on Windows, Linux, and macOS. Most of the microcontroller systems can be utilized solely on Windows. This IDE is for creating and uploading codes or programs to the board. The Arduino IDE is fully free and straightforward for utilizing. Processing IDE influenced the Arduino IDE, and the language is inspired by Wiring, which is incredibly straightforward to use, even for persons who are utter newbies in programming. Every program built for Arduino is called a sketch. These files end with extension *.ino*. Every sketch contains at least these two functions:

setup() Every reset or power-up of the Arduino board is this function called. For initializing

variables, pin modes, and many more.

loop() Is similar as calling *while(true)*. For controlling the board, all the time. It is called all the time after of one-time calling *setup()*.

```
void setup() {
// put your setup code here, to run once:
}

void loop() {
// put your main code here, to run repeatedly:
}
```

This is what every sketch looks like in the beginning.

Figure 3.9: Arduino integrated development environment (IDE)

3.4 Circuit Diagram

Figure 3.10 shows the circuit diagram for our hardware elements,

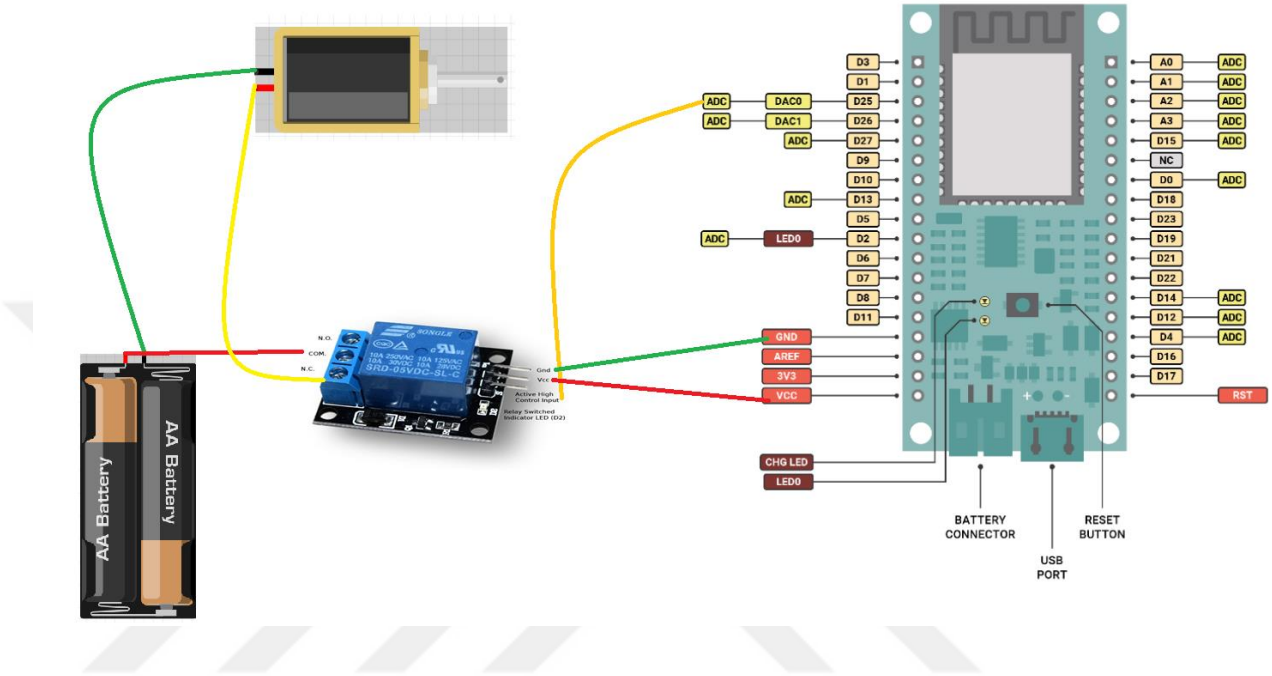

Figure 3.10: The circuit diagram for our hardware elements

Chapter 4

Prototype and Result

4.1 Web Page Prototype

This prototype is responsible for adding and managing authorized people to log in to the system and use it, we used PHP programming language to develop the web portal, figure 4.1 and figure 4.2 a snap for the web pages.

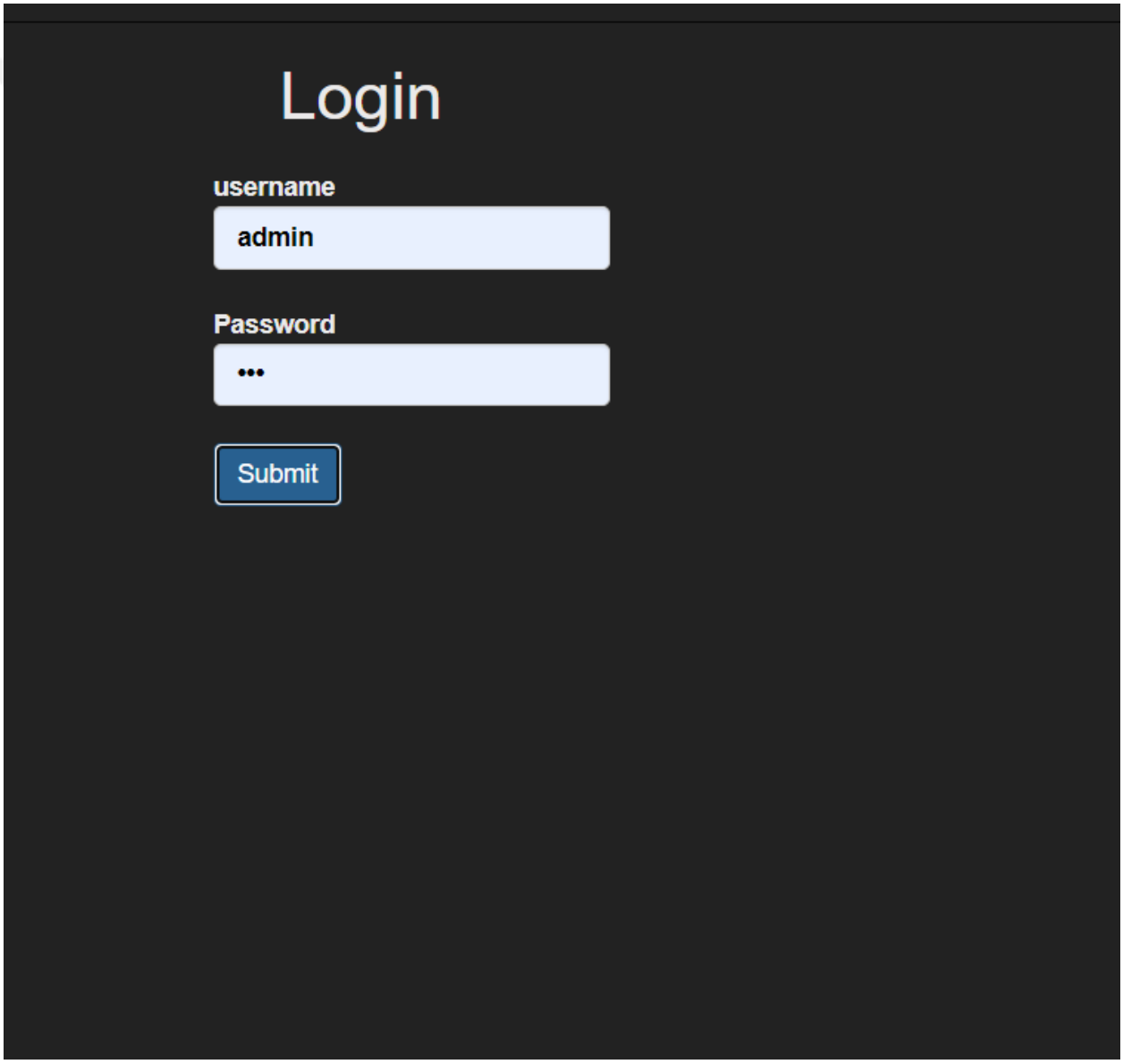

Figure 4.1: login page to web page for user's management

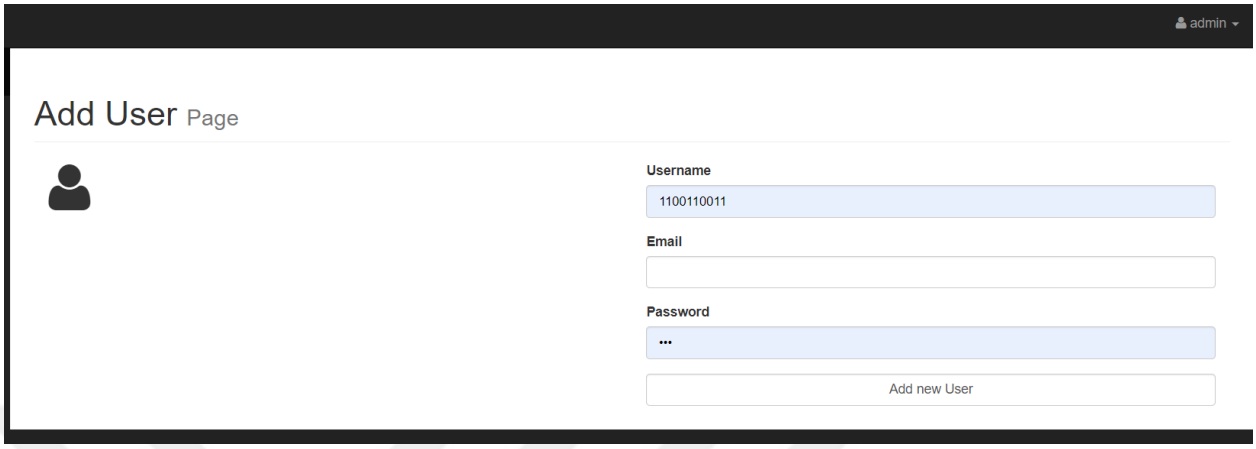

Figure 4.2: add new users

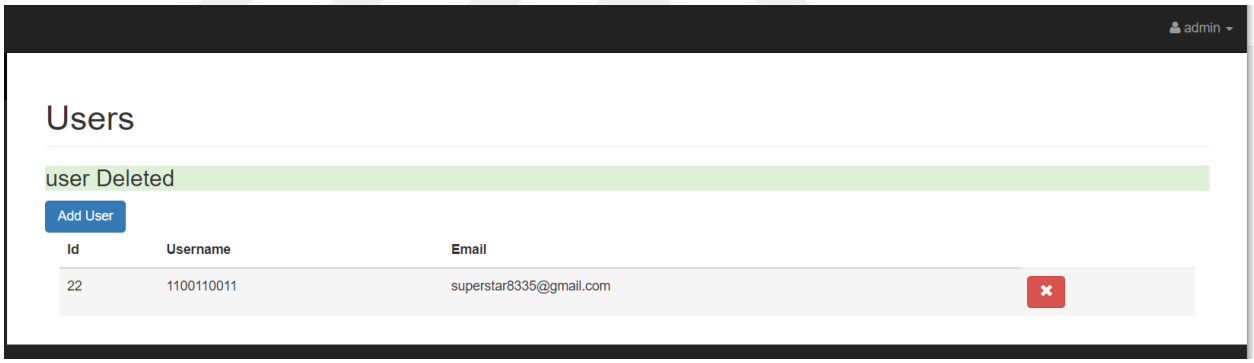

Figure 4.3: User management page

4.2 Mobile Application Prototype

In this section, we develop an android application for access control system controlling as we mentioned in the previous chapter the development details the figures 4.4 and 4.5 show the snap of the mobile pages.

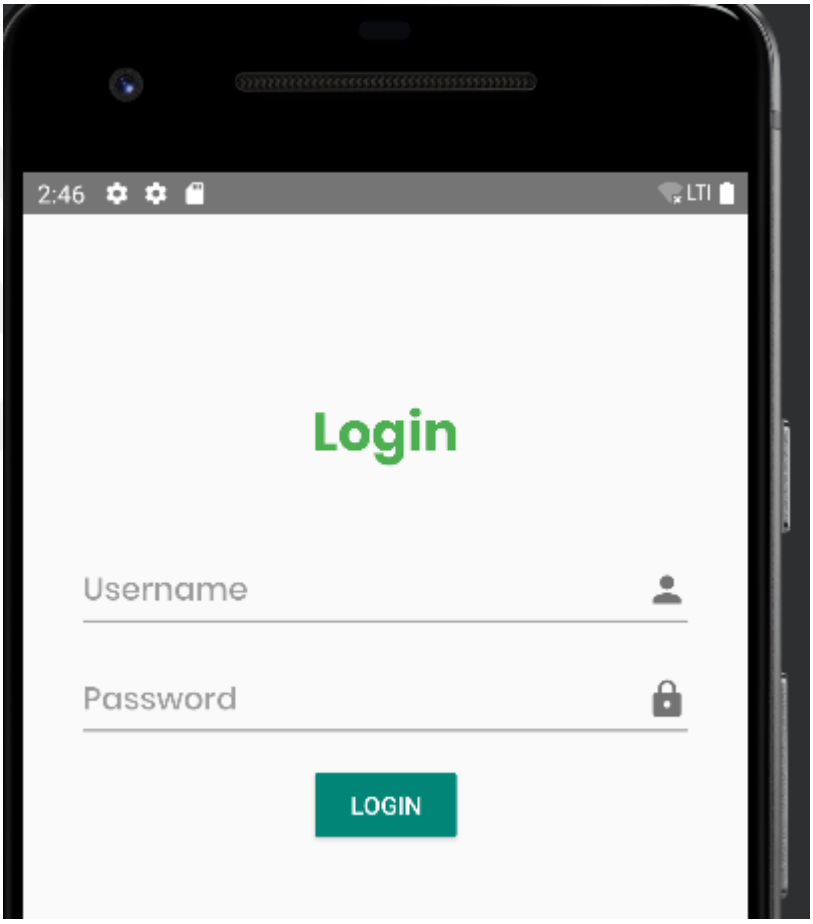

Figure 4.4: login page for mobile app

After the user login, the app checks the data provided using Mysql server, if the user is authorized, he/she will be redirected to access the control system control page as shown in figure 4.5

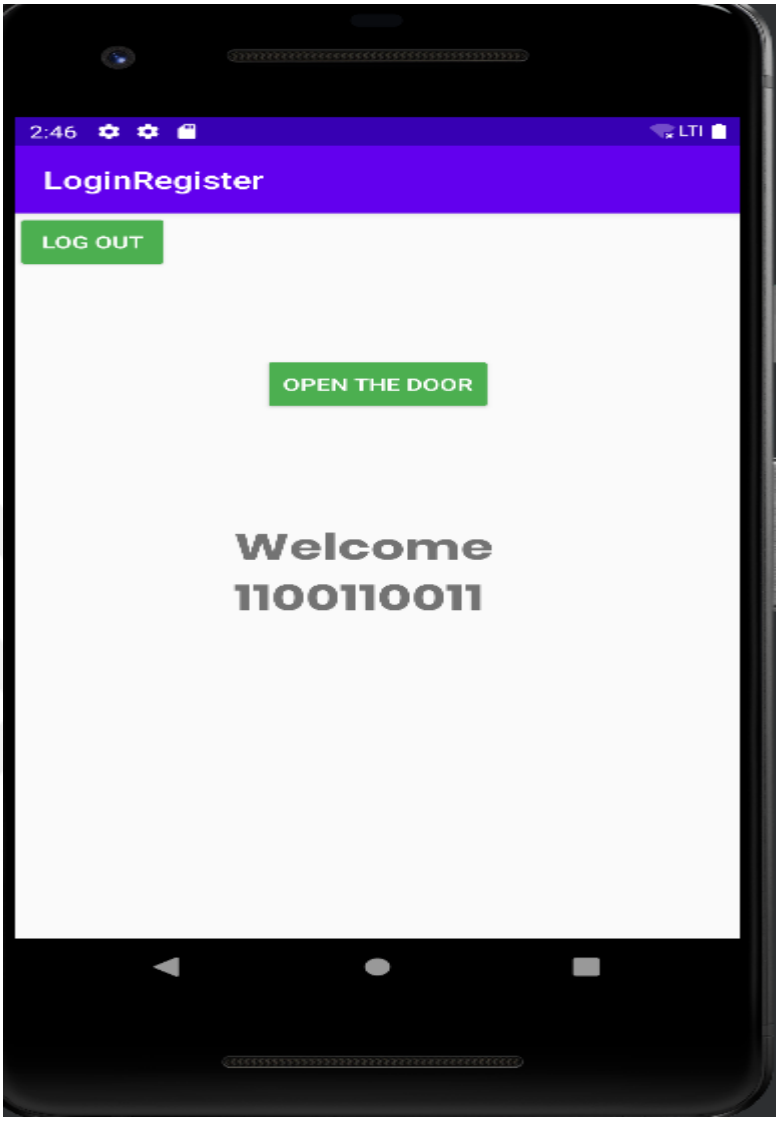

Figure 4.5: Access control system's control page for mobile app

On this page, the user can open the access control system using the button open the access control system with biometric authentication using fingerprints or face recognition as shown in figure 4.6

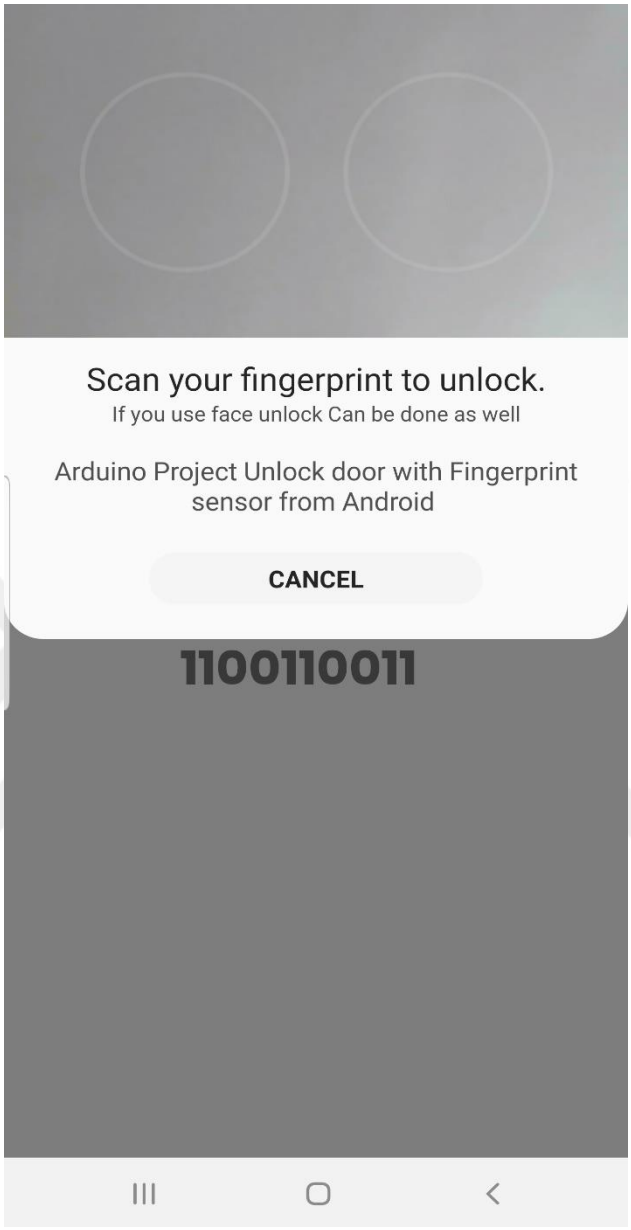

Figure 4.6: biometric authentication using fingerprints or face recognition

4.3 Arduino Prototype

As we describe the circuit diagram for the Arduino hardware the real prototype is shown in figure 4.7.

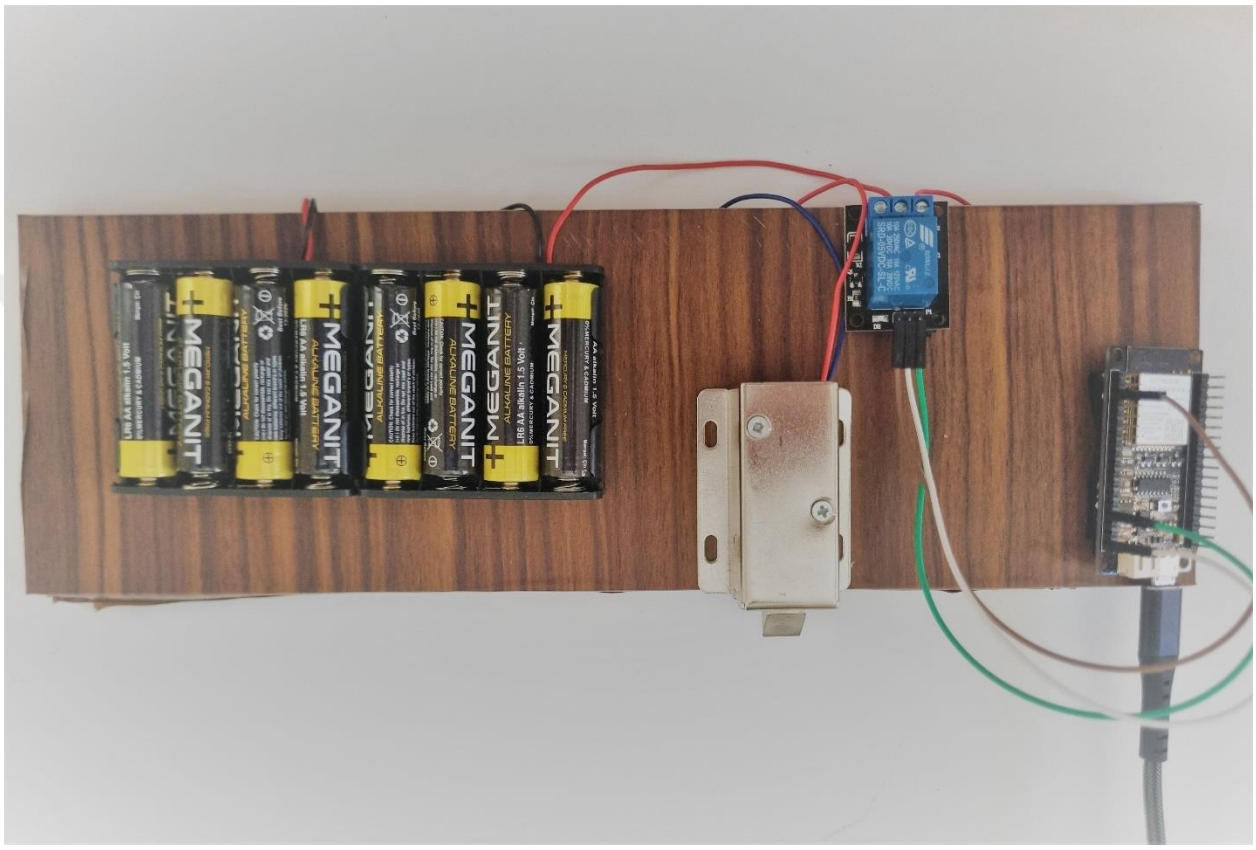

Figure 4.7: Arduino hardware the real prototype

Figure 4.8: Arduino hardware

Chapter 5

Discussion and Comparison

5.1 Discussion

The designed system delivers the required function of secure control access, with multifactor authentication was tested and verified as working system for all mentioned cases as credentials authentication, fingerprint authentication, face recognition authentication.

The system cost was calculated as shown below;

Component	Cost in TL
DFrobot Firebettel	165
Relay	25
Power supply	58
Solenoid lock	65

Implemented component cost

The total cost of the component is 313 TL, which is equal to 18$ total design cost. All software used was free and open source, in case of Realtime installation, a cloud server cost could be added.

Another factor I would like to discuss is the processing delay, since the proposed project is for biometrics authentication inside the user smartphone, the process takes a maximum 1 second to complete the process from the user authentication to the action of allowing access through. One more thing that may affect the delay is the time consumed by the mobile application to detect the access control system coordinates, which is take a maximum of 2 seconds just the first time when user tries to access.

Furthermore, to measure the system's effectiveness in terms of cost, delay, privacy, security, and accuracy a comparison was made with the published literature review.

5.2 Comparison

The design in [60] delivers Software on smartphones that uses a username and password as authentication. Arduino with Bluetooth module, solenoid door lock, and a web server implemented to achieve the required design. The design total delay is 2-5 seconds with a 9m distance. The design total costs 2.000.000 IDR equals to 134$. By comparing with the proposed design. It has the benefits of a secure system delivered with a low budget and user-friendly, on the other hand, the slow process of this system compared with RFID, or fingerprint is considered a Drawback of the system. However, when a comparison was done with our design which is Software on smartphones that uses biometrics-based multifactor authentication. The design implements Arduino with a Wi-Fi server, relay, solenoid door lock, and a web server with a time delay is 1-3 seconds within a 10m distance, and the design cost 313 TL almost 18$. Few things could be noticed here, cost-effective, less delay, and more security by multifactor authentication. Also, the user privacy in this design is considered, and the user biometric data are kept privately in the user's smartphone, and not extracted or kept somewhere that could face cybersecurity threats. if the user is authenticated correctly inside his/her smartphone. A signal will be sent to Arduino to open the access control system. This system is safer and keeps the user's privacy safe. while when comparing to [65] where, its secure access control system using a WIFI bridge device connected to the cloud database server, BLE, and smartphone, and each user is authenticated with their unique ID. It enables multiple levels of permissions and secure control of the lock with no complex hardware or lock firmware delivered. However, the cloud server with the current implementation has a lot of access, and most individuals would be hesitant to trust a third party to unlock their properties and reach to their privacy.

By comparing the proposed design to [8], the design in [8] which is consist of application checks for access control systems nearby every five minutes, the access control system opens when the user is in range. A Raspberry Pi based and MINDS android application was implemented to achieve the required functionality. The system is user-friendly, power effective, and area tracking and indoor accuracy deliver a secure access control system. Except for Automatic opening for the access control system,

consider a drawback since no authentication is required as RFID cards, which we try to eliminate its threats. We notice the proposed multifactor authentication design delivers a more secure access control system. In addition to [8], the same was noticed when looking at [36] which is Arduino, and an Android smartphone that connects with Arduino using Bluetooth module series HC-05 to complete the order of opening or closing the door. The end-user uses 6 pins to authenticate the credentials. Takes 1 sec to complete the command requested. Easy for Android Phone, tab users. This project is based on Android and Arduino platforms both of which are Free Open-Source Software. So, the implementation rate is inexpensive, however lake of authentication security by using One type non -biometrics authentication could be shared with other unauthenticated persons.

The system in [17] delivers a secure smart mobile app for a smart home environment (SSMASHE), which content of three modules mobile applications, IoT devices, and big data platforms are implemented in this project. A username and password are used for authentication.

The delay of this system is in the range of 30 to 72 ms depending on IoT devices connected after the credentials are delivered correctly. In design in [17] is responsible for detecting unauthorized persons and theft recognition. The total delay was compared and calculated as low. However, a continuous background process and message exchange between the 3 modules in smart mobile, so battery maintenance is required. Our proposed method authenticates with multifactor, credentials and biometrics, however, no heavy requests or message exchanges traffic was noticed.

The last comparison is made with [39] A special hatch lock mechanism is made with iron which penetrates a solid bar into the door to lock the door when engaging with the motor’s clockwise rotation. The design work to authenticate using the user's mobile number to restrict unwanted access. The user sends a command with SMS to specific numbers to access. It could be operated from a very long distance even from out of the country from anywhere in the world where GSM network is available, they concluded with this as a benefit, however from my point of view is a threat to access by unauthenticated users. Also, Complex for daily usage depends on GSM systems that

cause cost and delay in operation. The system cost 5405 taka, which is equal to 58$. The Proposed design is easier to install, has fewer components, less cost, and less time to operate a command. Also, the authenticated user could access just when the mobile application is within 10m, which I designed in this way to guarantee security.

Chapter 6

Conclusion

Since the 4.0 industrial revolution, researchers started to increase their researches in cybersecurity, IoT, AI, and Robotics. Since the world is going the most toward smart cities, where everything will be controlled by smartphones. Using Bluetooth low energy (BLE) / WIFI, to produce communication between “things” to be controlled and smartphones as controllers.

Smart access control systems or smart access control systems were one of the most requested IoT technologies, a lot of researches were published regarding this subject, every researcher see the needs and necessities from a different point of view, and all have benefits and drawbacks. Considering the needs and the importance, a secure access control system was developed depending on IoT technology. The delivered design has multifactor authentication, first with username and password, the second using biometrics. No process delay was noticed. No Bluetooth was activated which is considered an advantage since the Bluetooth technology could face a security threat.

A comparison has been made with the published literature, the proposed design delivers more benefits in some areas, first, user privacy since the multifactor authentication with biometrics is not stored in the database which could face a security threat and user biometrics exposure. The authentication is done inside the android OS, if the user authentic correctly a signal will send to the access control system to proceed. Second, low-cost, easy implementation, and has no complex hardware settings since ESP32 is used. Third 100% accuracy as compared with other face detection control systems. Fourth, the system delivers no delay except the GPS detection which may take a maximum 2 seconds, as compared with other systems it still has advantages. Fifth, IoT protocols have security issues of being threatened by MITM attacks since it is having a weak encryption algorithm, but we invested in HTTPS to deliver the data encrypted.

Furthermore, if a comparison was done over RFID cards which is a globally used technology, we notice, that the system eliminates the risk of sharing the RFID card, also multifactor authentication is enable. Furthermore, in case of lost card there is no ability of

unauthenticated access by an unprivileged person since multifactor authentication is enabled.

Chapter 7

Future Work

For our design, we activated the GPS functionality in the mobile application and set the access control system coordination to measure the distance, as future work to keep the system up with multi entrances in the access control systems. We need to implement a GPS detector in the system to measure the distance between the user and the access control system. Furthermore, decrease the delay caused by the current application to detect the coordination of the device itself.

Also, as future work, I propose to add extra privilege control to the users, access through known specific hours.

References

[1] . Baldwin, y. Al., "Round Two SHA-3 Candidates FPGA Implementations," 2nd SHA-3 Candidate Conf., 2010.And E. Homesirikamol, and. CHES2011, LNCS 6917, pp. 491-506, 2011. Al., "Throughput vs. Region Trade-offs in High-Speed Architectures of Five Round 3 SHA-3 Candidates implemented using Xilinx and Altera FPGAs."

[2] . "esp32_datasheet_en.pdf." Accessed: May. 01, 2022. [Online]. Available: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf

[3] ."FireBeetle ESP32 IoT Microcontroller (Supports Wi-Fi & Bluetooth) Accessed: May. 01, 2022. [Online]. Available:"https://www.dfrobot.com/product-1590.html

[4] 8 types of security threats to IoT [online]. Brno: Naveen Joshi, 2019 [visited on May. 01, 2022]. Available from: https://www.allerin. com/blog/8-types-of-security-threats-to-iot.

[5] A. D. Peris, J. M. Hern'ndez, and E. Huedo. "Evaluation of the Broadcast Operation in Kademlia". In: 2012 IEEE 14th International Conference on High Performance Computing and Communication 2012 IEEE 9th International Conference on Embedded Software and Systems. 2012, pp. 756–763.

[6] A. Dorri, S. S. Kanhere, and R. Jurdak. "Towards an Optimized BlockChain for IoT". In: 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI). 2017, pp. 173–178.

[7] AbdessalemAbidi; BelgacemBouallegue; Fatma Kahri Introduction of the Digital Signature Curve (ECDSA) Global Computing & Information Technology Summit (GSCIT) pp. 1-6, 2014.

[8] Adiono, T., Fuada, S., Anindya, S. F., Purwanda, I. G., & Fathany, M. Y. (2019). IoT-enabled door lock system. *International Journal of Advanced Computer Science and Applications*, *10*(5), 445-449.

[9] Advanced Persistent Threats and How Your Organization Can Deter Them [online]. Brno: Susan Hoffman, 2018 [visited on May. 01, 2022]. Available from: https://incyberdefense.com/featured/ advanced-persistent-threats-deter/.

[10] Advanced Persistent Threats and How Your Organization Can Deter Them [online]. Brno: Susan Hoffman [visited on May. 01, 2022]. Available from: https://rweather.github.io/arduinolibs/ classAES128.html#details.

[11] Alavalapati Goutham Reddy, Ashok Kumar Das, Eun-Jun Yoon, Kee-Young Yoo, "Elliptic Curve Cryptography 's Secure Anonymous Authentication Protocol," Volume: 4, IEEE Access 2016, pp: 4394- 4407, 2016.

[12] Alfonso Panarello et al. “Blockchain and IoT Integration: A Systematic Survey”. In: Sensors 18 (2018).

[13] BAKKER, D. M.; MCMICHAEL GILSTER, Diane. Bluetooth end to end. 1st ed. New York, NY: MT Books, 2002. ISBN 0-7645-4887-5.

[14] Baldwin, y. Al., "Round Two SHA-3 Candidates FPGA Implementations," 2nd SHA-3 Candidate Conf., 2010.And E. Homesirikamol, and. CHES2011, LNCS 6917, pp. 491-506, 2011. Al., "Throughput vs. Region Trade-offs in High-Speed Architectures of Five Round 3 SHA-3 Candidates implemented using Xilinx and Altera FPGAs."

[15] Bapat, C., Baleri, G., Inamdar, S., & Nimkar, A. V. (2017, September). Smart-lock security re-engineered using cryptography and steganography. In *International Symposium on Security in Computing and Communication* (pp. 325-336). Springer, Singapore.

[16] BRIAN, Russell.; VAN DUREN, Drew. Practical Internet of Things Security. 1st ed. Packt Publishing, 2016. ISBN 978-1785889639.

[17] Challa, M. L., & Soujanya, K. L. S. (2021). Secured smart mobile app for smart home environment. *Materials Today: Proceedings*, *37*, 2109-2113.

[18] Chistiakov, S. (2017). Secure storage and transfer of data in a smart lock system.

[19] Djupsjo, K., & Almosawi, M. A. S. A. R. (2018). IoT Security Applied on a Smart Door Lock Application. *Unpublished M. Sc Thesis, KTH, tockholm*.

[20] Doh, O., & Ha, I. (2015). A digital door lock system for the internet of things with improved security and usability. *Advanced Science and Technology Letters*, *109*(Security, Reliability and Safety 2015), 33-38.

[21] Dr Gavin Wood. Ethereum: a Secure Decentralised Generalised Transaction Ledger. In: (2014).

[22] Entropy library [online]. Brno: Walter Anderson, 2012 [visited on May. 01, 2022]. Available from: https://sites.google.com/ site/astudyofentropy/project-definition/timer- jitter- entropy-sources/entropy-library.

[23] Eric Harris-Braun, Nicolas Luck, and Arthur Brock. Holochain - scalable agent-centric distributed computing. In: (2018). url: https://holochain.org/whitepaper.

[24] Faisal, F., & Hossain, S. A. (2019, August). Smart security system using face recognition on raspberry pi. In *2019 13th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)* (pp. 1-8). IEEE.

[25] GREENGARD, Samuel. The Internet of Things. 1st ed. New York, NY: The MIT Press Essential Knowledge series, 2015. ISBN 978- 0262527736.

[26] Guy Zyskind, Oz Nathan, and Alex Pentland. "Enigma: Decentralized Computation Platform with Guaranteed Privacy". In: CoRR abs/1506.03471 (2015).

[27] Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016, May). Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security* (pp. 461-472).

[28] Hossein Shafagh et al. "Towards Blockchain-based Auditable Storage and Sharing of IoT Data". In: Proceedings of the 2017 on Cloud Computing Security Workshop. CCSW '17. ACM, 2017, pp. 45–50.

[29] Instructions to set Bluetooth Module HC-05 password using Arduino [online]. Brno: evelta, 2019 [visited on May. 01, 2022]. Available from: https://www.evelta.com/blog/instructions-to-set- bluetooth-module-hc05-password-using-arduino/.

[30] International botnet and security guide 2020 [online]. Brno: CSDE, 2012 [visited on 2019-10-20]. Available from: https : / / www . ustelecom . org / wp - content / uploads / 2019 / 11 / USTelecom _ CSDE-Botnet-Report_2020.pdf.

[31] Internet of Things Security Study: Smartwatches [online]. Brno: Gart- ner, 2015 [visited on May. 01, 2022]. Available from: https://www. ftc.gov/system/files/documents/public_comments/2015/ 10/00050-98093.pdf.

[32] IoT Chain - A high-security lite IoT OS. In: (2018). url:https://iotchain.io/whitepaper/ITCWHITEPAPER.pdf.

[33] IoT: Consumer Commercial vs. Industrial - Main overview. Brno: María Hernández, 2019. Available also from: https://ubidots. com / blog / iot - consumer - vs - commercial - vs - industrial - main-overview/.

[34] JIA, Xiaolin; FENG, Quanyuan; FAN, Taihua; LEI, Quanshui. RFID technology and its applications in Internet of Things (IoT). 2012 2nd International Conference on Consumer Electronics, Com- munications and Networks, CECNet 2012 - Proceedings. 2012. Avail- able from DOI: 10.1109/CECNet.2012.6201508.

[35] Kademlia". In: 2012 IEEE 14th International Conference on High Performance Computing and Communication 2012 IEEE 9th International Conference on Embedded Software and Systems. 2012, pp. 756–763.

[36] Kamelia, L., Noorhassan, A., Sanjaya, M., & Mulyana, W. E. (2014). Door-automation system using bluetooth-based android for mobile phone. *ARPN Journal of Engineering and Applied Sciences*, *9*(10), 1759-1762.

[37] Kazım Rıfat Özyılmaz and Arda Yurdakul. "Integrating low-power IoT devices to a blockchain-based infrastructure: work-in-progress". In: EMSOFT '17. 2017.

[38] Khabarlak, K., & Koriashkina, L. (2021). Mobile Access Control System Based on RFID Tags and rfidFacial Information. *arXiv preprint arXiv:2103.06767*.

[39] Komol, M. M. R., Podder, A. K., Arafat, A., & Nabeed, T. (2019). Remote sensing global ranged door lock security system via mobile communication. *Int. J. Wirel. Microw. Technol*, *5*, 25-37.

[40] Matevž Pustišek and Andrej Kos. "Approaches to Front-End IoT Application Development for the Ethereum Blockchain". In: Procedia Computer Science 129 (Jan. 2018), pp. 410–419.

[41] MITROKOTSA, Aikaterini; RIEBACK, Melanie; TANENBAUM, Andrew. Classification of RFID Attacks. In: 2008, pp. 73–86.

[42] Nagalakshmi, T. J. (2021). Intelligent Door Knocking Security System Using IOT. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(2), 2540-2543.

[43] Oded Goldreich. "Secure multi-party computation". In: (1998).

[44] Palle, S. (2017). *Smart Locks: Exploring Security Breaches and Access Extensions* (Doctoral dissertation, Oklahoma State University).

[45] Petar Maymounkov and David Mazières. "Kademlia: A Peer-to-Peer Information System Based on the XOR Metric". In: Peer-to-Peer Systems. Ed. by Peter Druschel, Frans Kaashoek, and Antony Rowstron. Springer Berlin Heidelberg, 2002, pp. 53–65.

[46] PUŽMANOVÁ, Rita. Bezpečnost bezrátové komunikace: Jak zabez- pečit Wi-Fi, Bluetooth, GPRS či 3G. 1. vyd. Brno: CP Books, 2005. ISBN 80-251-0791-4.

[47] R. Li et al. "Blockchain For Large-Scale Internet of Things Data Storage and Protection". In: IEEE Transactions on Services Computing (2018), pp. 1–1. issn: 1939-1374.

[48] Radix DLT. 2018. url: https://www.radixdlt.com/ (visited on 30/5/2022).

[49] Rameswari, R., Kumar, S. N., Aananth, M. A., & Deepak, C. (2021). Automated access control system using face recognition. *Materials Today: Proceedings*, *45*, 1251-1256.

[50] Ransomware. Brno: Avast, available also from: https : / / www . avast.com/cs-cz/c-ransomware.

[51] Security Tip (ST04-015) Understanding Denial-of-Service Attacks. Brno: Council to Secure the Digital Economy, 2009. Available also from: https : / / www . cloudflare . com / learning / ddos / glossary/mirai-botnet/.

[52] Security Tip (ST04-015) Understanding Denial-of-Service Attacks. Brno: Certified Information Systems Auditor, 2009. Available also from: https://www.us-cert.gov/ncas/tips/ST04-015.

[53] Sikder, A. K., Babun, L., Celik, Z. B., Acar, A., Aksu, H., McDaniel, P., ... & Uluagac, A. S. (2020, July). Kratos: Multi-user multi-device-aware access control system for the smart home. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 1-12).

[54] Sudha Ellison Mathe; Lakshmi Boppana; Ravi Kishore Kodali Implementation of Elliptic Curve Digital Signature Algorithm to an IRIS mote using SHA-512 International Conference on Industrial Instrumentation and Control (ICIC), pp. 445-449, 2015.

[55] Taraxa. 2017. url: http://taraxa.io/ (visited on May. 01, 2022).

[56] The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast [online]. Brno: IDC, 2019 [visited on May. 01, 2022]. Available from: https://www. idc.com/getdoc.jsp?containerId=prUS45213219.

[57] The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Brno: Cisco, Dave Evans, 2011. Available also from: https : / / www . idc . com / getdoc . jsp ? containerId = prUS45213219.

[58] The Making of Arduino [online]. Brno: David Kushner, 2011 [visited on May. 01, 2022]. Available from: https://spectrum.ieee. org/geek-life/hands-on/the-making-of-arduino.

[59] Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing*, *77*(12), 14053-14089.

[60] Trisnani, A., Barry, B. F., Santoso, H., Putra, I. M., & Saputra, F. A. (2017). "SMART DOOR LOCK": Anti-Sabotage Door Security System for Restricted Room. *UI Proceedings on Science and Technology*, *1*.

[61] VENERI, G.; CAPASSO, A. Hands-On Industrial Internet of Things: Create a powerful Industrial IoT infrastructure using Industry 4.0. Packt Publishing, 2018. ISBN 9781789538304. Available also from: https://books.google.cz/books?id=VN18DwAAQBAJ.

[62] What is the LoRaWAN Specification? 2018. url: https://lora-alliance.org/about-lorawan (visited on May. 01, 2022).

[63] What is the Mirai Botnet? Brno: CloudFlare, available also from: https : / / www . cloudflare . com / learning / ddos / glossary / mirai-botnet/.

[64] Yang, J. C., Lai, C. L., Sheu, H. T., & Chen, J. J. (2013). An intelligent automated door control system based on a smart camera. *Sensors*, *13*(5), 5923-5936.

[65] Zhang, A., & Kandubai, R. V. (2020, November). Access Control Schema for Smart Locks using a Wifi Bridge: An exploration of a smart lock access control system based around the SimSim retrofitting smart lock. In *2020 6th International Conference on Robotics and Artificial Intelligence* (pp. 174-178).