International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Multi-factor Authentication for Physical Access

Kaustubh Chude [1], Aditi Karwa[2], Megha Sah[3] ,Tanmay bhavsar[4]

Department of Computer Science and Engineering
Sandip university
Nashik, Maharashtra, India
Guide Name:- Prof. Nisha Patil

Abstract - Digital Multifactor authentication is the best way to implement secure authentication techniques. It covers multiple areas of Internet connected world that includes communications, online payments, access right management, etc. Sometime, Multifactor authentication become little complex as it requires some extra step from users to perform. In two factor authentication, user needs to enter special code received via SMS or a code that user already knows along with the User Id and password.

By creating multiple layers of defense, it will be more difficult for unauthorized users to access the targets such as physical locations, networks, computer equipment or databases. If first or second factor is destroyed or compromised, the attacker still has another barrier to break before successfully gaining access in the target.

Based on all previous researches, it has been deduced that the user authentication design based on Multi-factor Authentication is user-friendly and safe when specifically using factors such as something you know; In this case, users must enter a password that will be used when accessing wireless network facilities; that what you have; in this scenario, users will receive a one-time password. Once token is obtained from sms server, it is used by user to authenticate with first factor. After that user provides something you are factor which includes fingerprints, facial recognition , retina scan etc

***Key Words*:** Multifactor Authentication, Physical Access, Security, Cyber Security, Physical Access

1.INTRODUCTION

Physical access control systems (PACS) are physical security systems designed to allow or restrict access to a certain area. Usually, PACS are used by organizations in order to protect businesses and property from theft, vandalism, and trespassing. They are especially useful in facilities that require higher levels of security and protection. Physical barriers like high walls, fences or strategic landscaping are used to create actual physical barrier and physical access control mechanisms control who, how and when a person can gain entry.
The process of creating restriction of access to a certain secured area which is not usually protected is called Physical access control system(PACS). Traditional secure way to keep unwanted people and thieves out of a space is a locked door, but how can one make sure that the right users have access to secure data? This is where logical access control comes in picture. It controls the systems to restrict, manage, and allow who can enter a space or building using credentials such as key cards, key fobs, or mobile credentials; logical access control takes security a step further by requiring identity authorization and limiting access through processes such as an entry schedules and entry requirements. The problem now is that physical access controls are a decade-old technology that is already in use in most facilities. Also there have been many cases wherein an internal employee managed to gain access to sensitive location by evading single point access control mechanisms as seen in news and certain movies.

Severe devastating effects in the past have been caused by unauthorized access. Harmful malicious activities such as financial frauds, identity theft and attack on system can be used on employees working in a company and its assets. There is for sure need to upgrade already exiting access control mechanisms into multifactor authentication. Physical access to sensitive location these days are controlled by IOT actuators and sensors. Most common application includes a pin-based access control mechanism wherein a subject has to enter 4-digit pin and access is granted to the facility. There are near to none locations implementing multi-factor authentication for physical access.

2. Multi-Factor Authentication

Multifactor authentication (MFA) is a security access control system in which more than one way of authentication is implemented to Confidentiality of transaction. Multi Factor Authentication's goal is to create layered defence which will make it more difficult for an unauthorized, unwanted person to access a network or computer system. It is implemented by combining two or three independent credentials in serial approach which are something user is, something user have, and something user knows. Single-factor authentication (SFA) only requires knowledge the user possesses. Although password-based authentication is a good choice for application or website access, it is not that secure for online financial transactions.

Types of Multi Factor Authentication

Something user knows:
Knowledge-based authentication (KBA) is the first method of authentication in which it involves something the user knows. It can be a PIN, a password, or answer to the security question. Security questions and their corresponding answers are usually set when a user creates his account. They are also often being used as a method for account recovery by verifying the user's identity if the user has forgotten their password.

Something user have:
The next method of authentication is a thing that the user has physically. It could be an object such as a smartcard or a key,

that lets a user access a physical location. However, A one-time password (OTP) is generated by a token for digital accounts. The token authentication which are of three types have their own strength and weaknesses, which are commonly used:

SMS token authentication-
It is when organization sends a unique PIN number via a text message when the user has requested it. When the user has received the PIN as OTP, they can gain access to their account. It is useful for the organizations whose employees frequently needs to access their account from cellphone which can be because they have off-site job or have to travel as a part of their job. However, it not *only* works for employees but also for users who can receive SMS tokens to access accounts. It is very easy to implement but at the same time has its drawback that the user must have to the phone on for it to work. It is also possible for hackers to use cellphone tracking software to man in the middle into a user's phone and see user's mobile activity without user noticing it. This includes the text messages that sent directly to the user.

Email token authentication-
It works similarly to SMS authentication, in this a PIN is sent to the user's email address. It provides slightly more secure layer of protection than SMS token authentication, because in this the user has to be log in their email account to access the OTP. Email token authentication also means that the organizations don't have to rely on employee having their phone on them; users can access the OTP any device that receive emails.

Software token authentication-
It makes the user to verify their identity via an application. When it prompts for the OTP, then the user has to open the app which give them time-based expiring PIN to enter. Most authenticator apps such as google authenticator or Microsoft authenticator generates new PIN every minute which means that it is much harder for the hacker to retrieve the information when compared to an SMS token. The only drawback of this authentication mechanism is that it relies on user having a smart phone and install the app. On the top of it, personal device has very few security measures in place which introduces risk to enterprise account. Solution to tackle this problem is to make sure that the employees only access their accounts via devices offered to them via corporate.

Something user are:
These are physical characteristics possessed by users. It is the secure authentication mechanism because it is difficult for attacker to steal the data associated with biometrics because attacker needs to be highly skilled to steal fingerprints or a scan retina without user getting noticed. For implementing biometric authentication, the user needs to have a computer or smart device that allows biometric scanning. It could be voice, facial recognition or fingerprint scanner. Smart devices that we use today have these biometric related smart features built in. Company needs to be aware of how employee's data is being protected and stored. Some smart devices store the biometric data physically into the device. In case user's personal device is stolen then a hacker could bypass biometric mechanism by guessing the device's credentials and adding their own biometric data. If the organization is issuing corporate devices to mitigate the risk, then you as an administrator should be able to ensure complete security of sensitive data of employees.

3. Objectives

- Finding and understanding various ways of multi factor authentication that can be implemented for physical access.
- Finding relevance and applicability of multifactor authentication for physical access at a particular entry point
- Finding security flaws in implemented actuators/sensors that are using default libraries and fixing default code to make it cyber safe to operate
- Solving the problem of always vulnerable IOT based access control devices by implementing multiple access control measures at one single point. This way there is more security in place and provides better response time window in case attack or bypass of one control is detected

4. PROJECT SCOPE AND LIMITATION

Need of access control mechanism
It is one of the most important assets in a company, access control system holds significant value. Once account credentials have been received and and are checked and once user has been authenticated, then user is granted access to the system. This is called access control. It is important and used to protect the resources from unauthorized access. Also, they put into the place to ensure that the users can only access data using the pre-approved and secure methods. There are mainly three types of access control systems which are listed ahead

- **Discretionary Access Control (DAC):** In this access control mechanism, access rights are explicitly specified by users. The main working behind DAC is that the subjects can determine which users have access to their assets. It uses capability tables and ACL's (Access Control Lists). This table has rows with 'subject' and the columns that contains 'object'. The security kernel which is within the OS does the checking to determine if access is allowed or not. Sometimes a subject or program only has access to read a file when security kernel does the job of making sure that no unauthorized changes occur.

- **Role Based Access Control (RBAC):** It is used when the system administrator has to assign the rights based the organization roles instead of individual user accounts within the organization. It gives opportunity for the organization to address principal of least privilege. It gives the individual the only access needed to do their job.

- **Mandatory Access Control (MAC):** It is most strict among all the levels of access control systems. The implementation and design of mandatory access control is mostly used by the government agencies. It uses hierarchical approach to regulate the access to sensitive resources. In Mac environment, access to resource objects is controlled by settings that are defined by a system administrator. A users cannot change access control of the resource. It makes use of "security labels" that are used to assign resource objects in a system. Two information

connected to this security label are as follows: classification (low, medium, high) and category (specific department). Each user account is explicitly assigned classification and category properties. Though it is most secure access control mechanism, it still requires planning and system management due to updating of objects and account labels.

5. BENEFITS OF MULTI FACTOR AUTHENTICATION

Reduce Fraud & Identity Theft
In earlier days, you can easily carry out password cracking and gain access to privileged information. Now these days are over. When two or more methods of identification are used, then cracking them or bypassing them becomes more difficult. Multi factor authentication provides additional security mechanisms that attacker cannot easily bypass hence it provides additional security.

Increase Customer Trust
When customers know their data is secure, they are relieved and are confident when using a service. They trust business that take precautions to protect data, even though additional verification is annoying.

Achieve Compliance
Compliance measures, such as HIPPA and GDPR are required to be complied to by some industries. Government, finance and health entities demand that businesses follow strict guidelines that governs around protecting consumer's rights and mitigate risk. Make sure that your business considers its unique needs and determine their security requirements.

Reduce Operating Costs
Significant amount of money, cost and time is required by business to notify users of suspicious activity on their account. Staff can focus more on complex service issues when they are relieved their services are secured with multi-factor authentication

Combat Password Fatigue
According to already done research, an average user has to remember between 70-80 passwords. As an average human cannot remember much amount of random strings, users end up using similar password at multiple places or creating simple passwords. Both these methods lead to easy password hacking. Multi-Factor Authentication helps to safeguards against password guessing and brute force techniques that adds an extra security which in turn helps in ensuring that cybercriminals cannot hack passwords.

Simplify the Login Process
MFA has been made much easier by invention of Single sign on. One-time passwords can be sent to a mobile phone via voice or SMS, protecting data, private credentials and web-based services. OTP are excellent tool that help in reduction of risk by sending users a unique time-dependent and random numeric or alphanumeric codes and PINs on their mobile devices via push message, SMS or voice.

6. METHODOLOGY

SYSTEM REQUIREMENTS

- **Software requirements**
  - Windows 10 or any other OS compatible with Arduino IDE
  - CPP Programming Language
  - Arduino IDE for programming

- **Hardware requirements**
  - Arduino
  - RFID Scanner and tags
  - Number Pad for pin input
  - Jumper wires
  - LED
  - Buzzer

SYSTEM ARCHITECTURE
Following image depicts how system will be designed and how it will look like. Imaginary application for it would be as follows:

- User needs to regulate access to a secured area let's say a server room
- To access that room would be a door that a person has to go through
- Door can be fitted with MFA device out of which first factor can be a pin-based input device
- If user properly authenticates pin-based input, then next factor would be unlocked which can be fingerprint or RFID scanner.
- On properly authenticating with RFID, then user will be granted access to the room.
- In all the cases, every successful and failed access is logged.

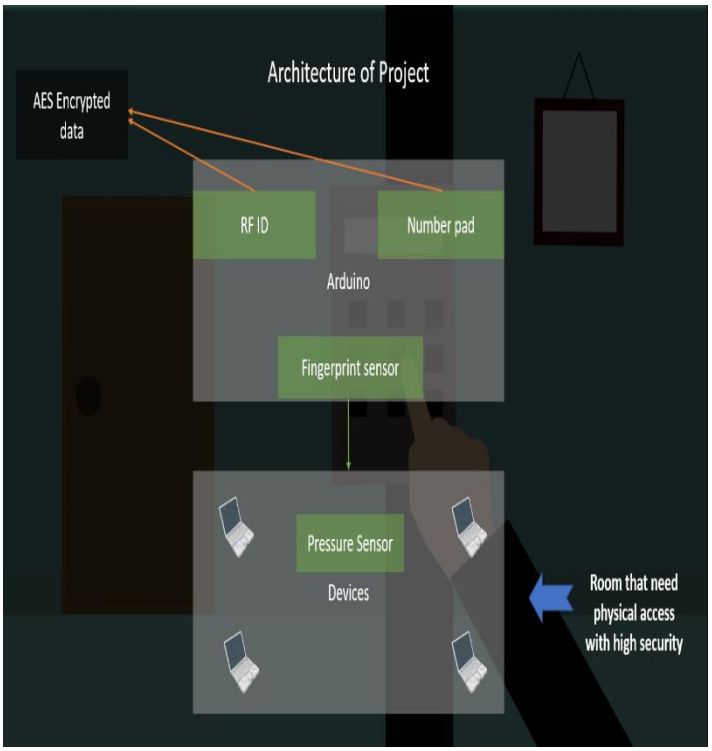


Fig:- System Architecture and Design

7. MODELLING AND ANALYSIS

Serialized implementation is key for working of this model. We have tried to implement its working by Demonstrating its basic working model on Arduino. Following are the steps we took to achieve our goal.

- Finding the appropriate modules and libraries required for implementation
- Implementing multifactor authentication working model using default libraries.
- Modifying default libraries according to project's use case.
- Programming the logic for MFA and later implementing brute force control mechanisms d other security controls.
- In the end, adding alerting mechanisms by which, in case authentication mechanisms fails or are bypassed, then appropriate alert can be generated.

Flow Chart

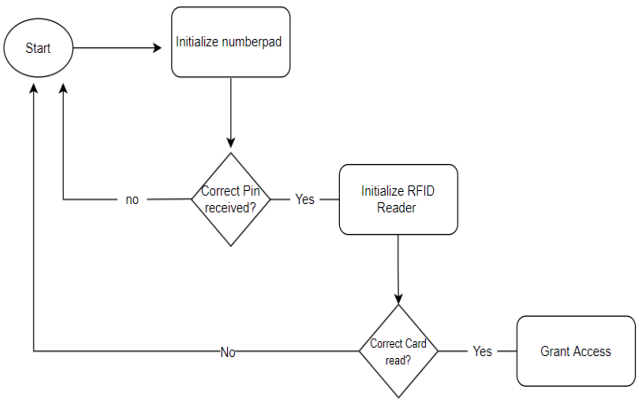


Fig :- Flow chart for Multi-factor Authentication

Bl

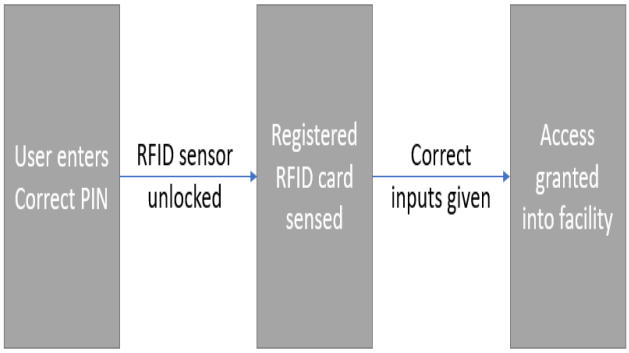
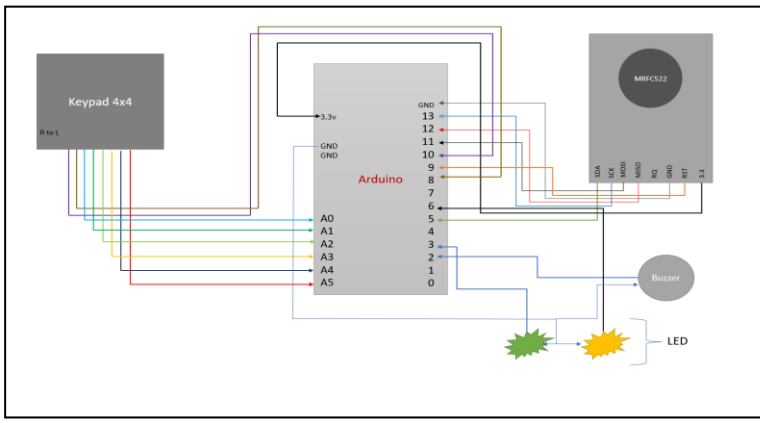


Fig:- Block diagram

Working of Block Diagram and Flow chart

- First implementing multi-factor authentication working model using default libraries
- Modifying default libraries according to projects use case
- Programming the logic for MFA code and later implementing brute force control mechanisms
- In the end, adding alerting mechanisms by which, in case authentication mechanisms are bypassed, then appropriate alert can be generated.

Circuit Diagram



SECURITY IMPLEMENTATION

Let us understand the libraries which are associated with the modules that will be used. To keep things simple, we are going to use RFID and a keypad for our authentication purpose which will give you basic understanding of implement things. If you are interested in making this project then you are free to use and customize the code I am using. Also, this project can be scaled and modified to use different authentication supporting modules as well. Libraries required to build this project are

- Keypad.h
- MRFC522.h (RFID library)
- SPI.h (Serial peripheral interface library for communicating with peripheral devices)
- AES.h (Library used for encryption)

If you are implementing this project, then it is advised to use Arduino IDE and it can be implemented. Libraries mentioned above will not be present by default in Arduino IDE. If so, then you can download them easily by going to Sketch>Include Library > Manage Libraries. Here library manager opens and you can search for libraries given above and install them. First keypad input will be provided, if correct then it unlocks RFID module and then RFID is checked. If correct input is received then access is granted.

CONCLUSION

Multi-factor authentication is an important tool for keeping the Online as well as physical world secure. As the other computing technologies, multi-factor authentication will be as simple or as complex depends on how someone wishes it to be. Whether you desire to protect a blog, a small business, a data center, office building or highly secure location, there are multi-factor authentication options available to cover needs. The technologies are continuing to evolve with more focus on the individual user, authentication security will become more important. Time will come when many wearable and mobile devices will become a core aspect of authentication. A secure solution for multifactor authentication implemented for physical access will be ready to apply directly as per requirements. From learning point of view, this would give a great understanding of ways to modify an already existing code to a more secure version and would be helpful as an experience while applying knowledge and while working for a company.

REFERENCES

[1] Maha M. Althobaiti, Pam Mayhew "Assessing Usable Security of Multifactor Authentication", in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST).
[2] Mohamed El Beqqal, Mostafa Azizi "Review on security issues in RFID systems", Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 6, 194-202(2017)
[3] Ometov, Aleksandr, Tommi, Koucheryavy, Yevgeni "Multi-Factor Authentication: A Survey ".
[4] User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking
[5] Multi-Factor Authentication in Cyber Physical System: A State of Art Survey, 2019 21st International Conference on Advanced Communication Technology (ICACT).
[6] Study to Improve Security for IoT Smart Device Controller: Drawbacks and Countermeasures, Volume 2018 |Article ID 4296934
[7] Two-Factor Authentication Protocol Using Physical Unclonable Function for IoV, 2019 IEEE/CIC International Conference on Communications in China (ICCC).
[8] Aleksandr Ometov, Vitaly Petrov "Challenges of multi factor authentication for securing advanced IOT applications", IEEE Network (Volume: 33, Issue: 2, March/April 2019)
[9] Kerry Ford, Casimer De Cusatis, Michael Otis "Bypassing fingerprint scanners using artificial fingerprints", 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON).
[10] Kumar Sekhar Roy, Hemanta Kumar Kalita "A Survey on Authentication Schemes in IoT, 2017 International Conference on Information Technology (ICIT).