MULTI-FACTOR AUTHENTICATED SECURE DIGITAL LOCKER USING GSM

Anshita Dhoot[1], Kristi Shumka[2], M. Salman Saeed[2], Prof. A.N. Nazarov[1]
[1]Department of Radio Engineering and Computer Technology
Moscow Institute of Physics and Technology, Moscow, Russian Federation

[2]The Department of Intelligent Information Systems and Technologies,
Moscow Institute of Physics and Technology, Moscow, Russian Federation

DOI: 10.36724/2664-066X-2021-7-2-7-12

ABSTRACT

In this time and age, technology is on an ever-developing trend, bringing with it a plethora of new advancements to daily life and common activities, but with these advancements, a whole new set of issues and vulnerabilities become present. This paper aims to discuss and propose a solution to the vulnerability of physical security lockers, a facet of security that many organisations tend to neglect. It aims to provide an elevated level of security for companies who use physical lockers to secure sensitive information or important contents. More specifically, the paper discusses the plausibility and the advantage of utilising multi-factor authentication with dynamic passwords or OTP code for short and facial recognition to access physical lockers. The proposed system will require employees to have accounts in their respective locker by entering their respective ID and passing the facial recognition feature. The system will then provide the employee with an OTP code, allowing the company an extra layer of security from intruders or malicious individuals.

KEYWORDS: *physical locker security, sensitive information, multi-factor authentication, facial recognition, OTP*

I. INTRODUCTION

Security is one of the most concerning and pressing issues at hand for any organisation. Due to the continuous increase in security breaches every year, it becomes more and more necessary to make our systems less vulnerable to any potential future breaches. An individual can attempt to compromise or even steal property which could threaten the integrity of the capital, information or even persons in homes, banks and offices. Securing physical lockers has become one of the more pressing concerns in need of a solution. Nowadays, lockers are prone to various attack types and multiple threats, particularly physical item theft. To reduce this threat, most companies opt for the implementation of dual authentication systems and alarms on their digital lockers. These digital lockers are composed of electronically secured locking systems that work according to the signals received via the corresponding input keyboards. They are unaffected by tampering attempts and offer the user a variety of security options. The utilisation of an electronic keyboard as the entry lock offers several advantages, such as reliability, strength and ease of use. These digital lockers also offer much flexibility in their setup. They can be programmed to automatically enter lockout mode when left idle for longer than a previously specified amount of time. Moreover, they can also temporarily lock the system for a predetermined duration in the cases when a wrong code input has been received multiple times as a result of an intruder attempting to brute force the code.

It is invaluable for any company, business, or even government organisation to implement a secure system that accounts for any possible attacks, discovers vulnerabilities, and ensures ongoing compliance cost-effectively and safely. This is often not easy to achieve, but it can be possible with secure wireless technologies. In the words of Bruce Schneider: “Security is a process, not a product”. This well-known quote is well reflected in the case that while there exist an innumerable amount of security ensuring techniques and best practices nowadays, none of these methods manages to single-handedly achieve all of the security goals for any given organisation, there is always room for more advancements and more secure systems. In this work, the proposed system uses facial recognition as well as a One-Time Password (OTP). As is known, OTP is a dynamically allocated password that is used for a single login session. So, OTP allows the system to overcome several shortcomings present in traditional or static authentication methods such as password-based. This paper proposes a smart locker implementation to ensure secure access and authorisation. This system can implement in a variety of companies, banks, or even for personal use. This is why a mix of facial recognition and OTP is used to subdue unauthorised access attempts. In this proposed system, any registered user can log in by using their identity credentials, and after the face recognition of the valid person as additional authentication, the user sends a request for OTP in order to activate access to their respective locker. The password is then sent to the established individual via Global System for Mobile Communication (GSM) based messaging service, which is currently the most secure cellular telecommunication system. GSM security methods are standardised. It also guarantees end-to-end security by maintaining the confidentiality of messages and the anonymity of the GSM subscriber. The OTP session is set to 15 minutes. OTP offers a primary benefit over static passwords seeing as it is not vulnerable to repeated assaults. OTP has one predefined validity consultation, making it not vulnerable to abuse via hackers or other intruders. Another major benefit of OTP is that it circumvents the vulnerability present when a person uses the same login credentials to access multiple systems seeing as even if passwords are the same, authenticating through OTP will provide an extra layer of security. This paper aims to propose the design and development of a multi-factor authentication based secure digital locker system.

II. LITERATURE SURVEY

Previous research on the topic already exists, with many new and relevant advances made every day. This section discusses some of the mention-worthy papers related to this domain and proves the ever-increasing necessity for more secure systems.

Dey S. et al. [1] presents a home-based web security system that utilises an Arduino microcontroller in conjunction with the Wi-Fi switch. In this case, a simple router is utilised to offer an internet protocol (IP) address to the end-user devices via a corresponding ethernet module.

Shaligram A. et al. [2] introduced a security system for home/office based on GSM technology. The paper proposes different methodologies to utilise for a home security framework. One of these methodologies uses web cameras to alert the owner of a security issue, while another method dispatched a SMS through the usage of GSM and GPS modules. In this case, an atmega644p micro controller became utilised, capturing signals from sensors based totally on making decisions and sending intimation via the use of SMS.

Sharma R. K. et al. [3] proposes an Android based home security system. In this case, an android application used to interpret the message information and in turn provide an answer through SMS, which would light up the light-emitting diode. The signal would then go to mobile as a SMS alert through the use of a GSM modem. Afterwards, the android application would initiate a pop-up alert notifying about the security issue in the house. In this case, as the additional security feature, the authors have also used facial recognition.

MD. Wasi-ur-Rahman et al. [4] describe an approach that uses GSM technology to achieve communication in a remote metering system with devices through the use of SMS. The research demonstrates a method that remotely accesses the electricity meters reading by making use of SMS. Data gathering based on SMS can work very easily and efficiently. Thus, post-paid and pre-paid are both possible to implement utilising this architecture.

Kunal M. et al. [5], the paper discusses the design and the development of a locking system for vehicles. Moreover, it discusses the conception and implementation of an automobile system for theft control and circumvention. The proposed system is made possible through the use of GSM technology in conjunction with an embedded system which is installed onto the vehicle with the cellular-related to the corresponding microcontroller linked to the vehicle engine. If the automobile happens to be stolen, the relevant information is then sent through SMS to the system responsible for central settlement insurance. The microcontroller unit then extracts the SMS information and forwards it to the Global Positioning System (GPS) module, which in turn commands it to be locked or the engine to be switched off. As for the owner of the vehicle, they provided with an account to which they only need to enter the password to access their automobile. Once the valid password has been entered, the microcontroller forwards the SMS to the cell phone number of the account's holder. The individual holding the account can then send the password via a mobile phone with GSM to the relevant microcontroller which in turn compares the passwords received via the mobile phone and entered via the keyboard. If both passwords happen to be correct then the microcontroller will provide the signal required for opening the lock.

Niaz M. et al. [6] presents an IoT based approach to Smart Lockers with the additional use of OTP and facial recognition. First, the user would have to log in and send an (OTP) request code to unlock the locker. After he has received a corresponding feedback e-mail with OTP, he can access the locker's contents. The article also suggests using a facial recognition feature to augment the existing locker security system.

Ajay K. et al. [7] proposes developing a security system for Bank Lockers, which permits the manager to monitor any occurrences and probably catch the applicable frame relying on its benefit. The paper proposes achieving this through properly structuring and organising the application as well as planning of the pages for the site which will then be connected to their corresponding database, capturing pictures through the use of raspberry pi, facial acknowledgment, and facial discovery, thus allowing or denying acces to the clients as neccesary.

Dhoot A. et al. [8] proposes a model for Smart Online Banking Systems (SOBS), which uses biometric authentication and digital signatures to make transactions possible for customers of a bank. The article discusses methods such as machine and data learning, biometric recognition as well as hybridised methods in creating this system, and how they can further help reduce threats and detect intruders.

D.-M. Turner et al. [9] discuss the importance and implications of utilising secure wireless technologies in healthcare and the difficulties faced when implementing them into this particular environment. It uses a case-study approach to investigate these challenges and proposes better practices for secure wireless access for the studied organisations based on the collected data.

Tariq, F. et al. [10] proposes a model for home and industrial automation, which discusses the automation over the GSM-based messaging service. This article discusses multi-factor authentication for home automation, in which the installed system can switch on or off any home appliances via a microcontroller after the verification of the used encrypted key sent via GSM messaging service.

III. AUTHENTICATION TECHNIQUES

In any given system, authentication provides the first line of defence. This is the process in which a system determines if a user or individual is who they claim to be through digital identification so that individuals can have the corresponding level of access or permission necessary to act.

There exist a wide variety of authentication methods, such as fingerprints as well as passwords used to access an individual's identity before allowing them access. It helps add a layer of protection and prevents security issues such as breaches of data. It is worth mentioning that the most secure system reinforcement against possible threats is usually only achieved by combining different authentication methods.

a. Password-based

Passwords are by far the most common authentication method. They can be numbers, a string of letters or special characters, but a secure password generally incorporates all three of these forms. This being the most common form of authentication also makes it the least secure when utilised in a single-factor authentication system as brute force attacks easily bypass it.

b. Biometrics

The term biometrics defines the measuring of any unique personal characteristics like fingerprints, face, voice, retina as well as iris. Nowadays, this term is often used when refering to a method of securing stored data, systems or computers which requires the user to scan the corresponding body part in order to gain authentication. Biometrics are very difficult to fake, but in order to use them, specialised scanning equipment is often necessary, which is often not ideal for projects or industries.

c. Token Authentication

A token refers to a physical device that used in order to access secure devices or systems. Some of the common forms of tokens include an RFID chip, card, or dongle. Tokens make it harder for a malicious individual to gain access to an account since they need to have both the credentials and the physical device itself. Similar to biometrics, tokens are also difficult to fake. The unique digital identification of a token in the form of an RFID chip or key based on more sophisticated security standards attackers cannot easily forge. Nevertheless, tokens themselves are very secure. They can still be easily lost or stolen.

d. Transaction Authentication

The basic idea regarding transaction authentication is its context. This authentication method looks out for reasonable mistakes which can make when one compares the known data regarding an individual with the corresponding information of the current transaction. An example of this would be a user living in one given country, but several purchases made from them logged in from an IP address in a different country. This authentication method is thankfully not dependent on the users, as it is usually outsourced to third-party monitoring teams. However, if a criminal manages to spoof a user successfully, they can fraudulently approve of transactions occurring under false pretences.

e. Multi-Factor Authentication (MFA)

Multiple factor authentication uses a combination of several authentication techniques, all necessary to gain access to the system, thus providing a high-assurance method to verify users. MFA uses factors such as biometric, additional passwords, confirmation based on the device, location, or even behaviour based on information in conjunction with each other to confirm the individuals' identity. This layering of authentication methods allows for increased security as if any of the given methods are bypass. The attacker would still have to deal with the additional authentication methods to gain access to the system.

IV. Proposed Model

This project aims to provide an effective, low cost and more reliable locker security system. The proposed system needs multi-authentication from the user to verify the legitimate access and access only the verified user. After passing the user ID to the locker and after verifying the coordinates of the user's face via the facial recognition method, the microcontroller generates a randomly suitable OTP through the GSM module based on the defined parameters. After passing the OTP code generated via the GSM module, the microcontroller gives the response to the relay and finally opened the locker. The user ID and the OTP code required to open the door must enter into the system via the keypad.

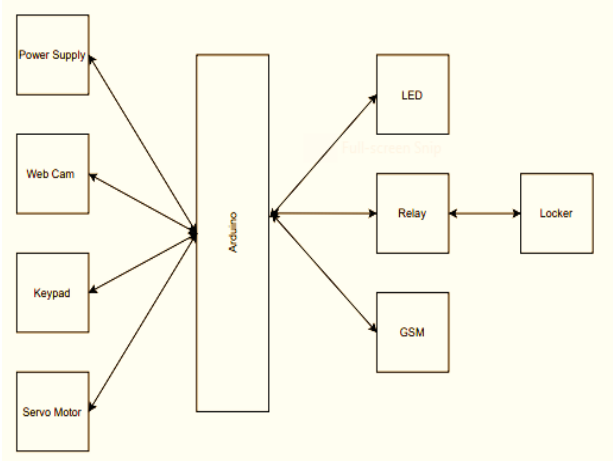

Figure 1: The proposed model

The following Fig. 1 shows the proposed system in the form of a block diagram.

a. Arduino controller

Arduino is simply an Integrated Development Environment (IDE) which runs on a PC and allows users to write C, C++ or any other high-level languages. All programs are installed in the Arduino controller. Arduino is an electronics platform based on easily used and implemented hardware and software while also being open-source. The program is written in Arduino IDE software and burnt onto the Arduino board.

b. Servo Motor

The servo position control method uses a potentiometer. Arduino writes every position value to angular position according to the input change. This method provides not the exact servo position as input, or the user cannot write this Servo position in exact degrees, unless the values entered via the serial keypad. This is an easy way to move the servo motor's position by specifying the degree of the angle as a numerical value. So, we used a servo motor in this paper for better detection of both the face movement and the position of the keypad.

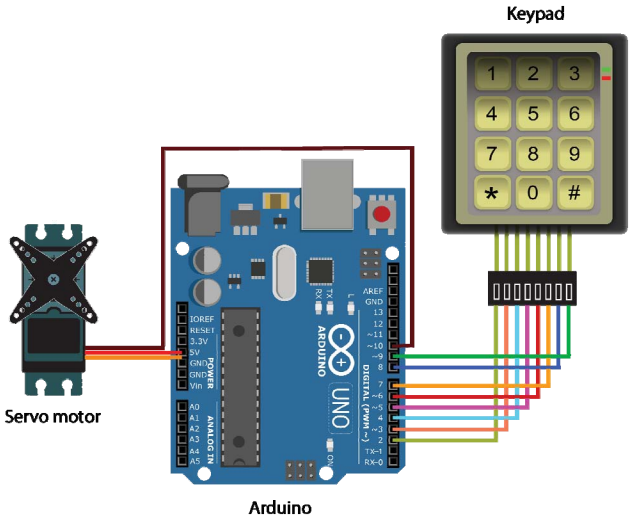

Figure 2: Servo Motor

c. GSM Module

GSM Module is used to provide data transfer to a remote network. After entering the correct user password and detecting the face, the microcontroller generates a random OTP based on the defined length and transmits it via GSM Module to the user's defined cellular network. So, the microcontroller is only switched on the relay after the verification of the respective OTP.

d. Facial Recognition

Facial recognition is a biometric technique used by digital locker systems because it is secure and controls overlocker access. Many algorithms have developed and proposed to achieve facial recognition, including Evolutionary Pursuit (EP), Principal Component Analysis

(PCA), Kernel methods, 3-D face recognition, Independent Component Analysis (ICA), Active Appearance Model (AAM) and Support Vector Machine (SVM).

e. Evolutionary pursuit (EP):

This is an adaptive eigenspace-based approach which appears for the superior set of projection axes to maximise the fitness feature when calculating type accuracy and the system's capability to generalise. Since the dimension corresponding to the solution space for this issue is very large, it is resolved utilising a certain genetic algorithm called Evolutionary Pursuit (EP).

f. Principal Component Analysis (PCA):

It is derived from the Karhunen-Loeve transformation and provided with a s-dimensional vector instance of every face present in the set of training images. PCA tries to determine t-dimensional subspace whose base vectors speak with the full existing variance path in the initial image space.

g. Kernel methods:

Here the facial distributor present in the subspace does not necessarily have to be linear. Kernel methods can be thought of as a generalisation of linear methods and may conceptualise as instance-based learners: instead of learning a fixed set of given parameters relating to the features of their inputs, they rather "remember" the example in training and learn the corresponding weight for it. For studying this nonlinear distribution, direct nonlinear distribution schemes have studied.

h. 3-D face recognition:

The principal innovative element provided with the aid of this approach is its capability in evaluating surfaces independently of any natural deformations taking place on facial expressions. Firstly, the distance image, as well as the face texture, is captured. The image has to delete then preprocessed by removing certain parts that can needlessly overcomplicate the recognition process, such as hair. Lastly, the canonical shape presented by the front surface has calculated. This representation is not sensitive to head orientation or facial expression, which greatly simplifies the process of recognition that occurs on canonical surfaces.

i. Independent component analysis (ICA):

Independent component analysis (ICA) enables the minimisation of the second and higher-order dependencies present within the input information, even when trying to find a basis on which the statistics can be statistically impartial.

j. Active Appearance Model (AAM)

The Active Appearance Model(AAM) provides an integrated model which intertwines the shape replacement version with a shape change model in a form-normalized structure. AAM consists of a statistical version of the appearance and the shape of the interesting object in grayscale that is generalized to almost every possible legitimate instance. Image acquisition includes the acquisition of version parameters which reduce the difference between the images and the synthesized model shown in the picture.

k. Support Vector Machine (SVM):

For a chain of factors that belong to two distinct training, Support Vector Machine (SVM) will discover a hyperplane that shares the maximum capable fraction of points of the equal corresponding class on one side, while also maximising the space between both pieces of training as well as the hyperplane itself. PCA is first utilised inside the extraction of functions from facial images and afterwards during the use of recognition features in-between each pair of pictures found out with the help of the SVM.

The facial recognition algorithm aims to detect and extract the features of the user's face and save them into the database for future matching. After narrowing down the different algorithms for face recognition, we select a PCA based face recognition algorithm. We divided it into phases: the training phase and the recognition phase.

Face recognition is the most important part of this paper because, without accurate recognition, the system would not give access to a given user's locker. The human face is a very complex multi-dimensional structure. So, there is a need to use a more effective technique. We picked the Eigenface technique.

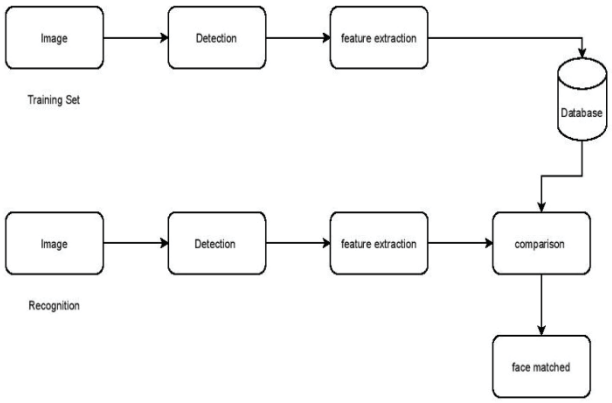

Figure 3: Face recognition steps

V. PROPOSED ALGORITHM

The microcontroller gets inputs from the web to verify the user's verification via facial recognition method and the keypad used to enter the required user ID, giving a suitable output response to LED and GSM. The microcontroller generates a random suitable OTP through the GSM module. After passing the password generated via GSM, the microcontroller passed the relay's response and finally opened the locker.

a. Algorithm 1: Face Recognition Algorithm

Step 1: Facial image **conversion** tested by n*n size into a column vector $v_{i\ n\hat{}2}$

Step 2: Facial image **normalisation** as an input to training images to evaluate its value for distinct matrix x_{input} by reducing the average value to its train images.

Step 3: Compute the weight of trial images by multiplying Eigenval Transpose Matrix $\underset{V}{\rightarrow} t$ to the matrix

$x_{input}\, matrix\ (W_{input})$

$W_{input} = \underset{V}{\rightarrow} t\ x_{input}$

Step 4: Evaluate different image's distance for testing images with the train face image by using Euclidean distance.

$$\varepsilon_i = \sqrt{||W - W_{input}||^2}$$

Where i = 1……N

The result to identify face is the image with the minutest distance with its test image to display by the system.

b.

c. Steps for the System Testing

It determines the system is working, whether it is working properly or not. It is important to the test system is running properly or not to identify the images.

Step 1: Training: In this process, the system is in the training stage. In this, it aims to generate value's weight for each existing training image.

Step 2: Image Recognition: This process occurs after the successful implementation of the training process. In this stage, image recognition carries out to recognise and test all the required images properly. It contains two substages

- The training image is similar to the testing image
- The training image is not similar to the testing image

These training data will assure a 100 per cent identification system. Therefore the proposed system has precise value and provides security from the authentic user. It saves the system from various unknown attacks and protects the user's crucial data.

VI. Conclusion

This work proposes a multi-factor authenticated secure digital locker to enhance the security of valuable assets. The proposed system ensures security by providing an OTP on top of the dual-authentication. In the first step, an individual's identity credentials in conjunction with facial recognition techniques are utilised to authenticate the user. After the dual-authentication of the user, the system generates an OTP for their corresponding personal device and sends it via the GSM module, thus providing an extra layer of security for ensuring the authentication of the valid user. Moreover, the PCA algorithm is utilised for face detection because it is easier for the classifier to extract faces when data is spread out instead of grouping them. The proposed digital locker is more secure than traditional digital lockers because it provides a dynamic key via OTP on top of dual-authentication instead of traditional keys used in unlocking lockers. It provides a highly reliable and secure system alternative to amplify the security of valuable assets.

References

[1] Dey, S., Kundu, T., Mukherjee, S., & Sarkar, M. (2015). Web based Real Time Home Automation and Security System. *Int. J. Elec & Electr. Eng & Telecoms*, *4*, 126–132.

[2] Bangali, Jayashri, & Shaligram. (2013). Design and Implementation of Security Systems for Smart Home based on GSM technology. *International Journal of Smart Home*. https://doi.org/10.14257/ijsh.2013.7.6.19

[3] Sharma, R. K., Mohammad, A., Kalita, H., & Kalita, D. (2014). Android interface based GSM home security system. *International Conference on Issues and Challenges in Intelligent Computing Techniques*, 196–201. https://doi.org/10.1109/ICICICT.2014.6781278

[4] Wasi-ur-Rahman, Md., Tanvir-Rahman, M., Khan, T. H., & LutfulKabir, S. M. (2009). Design of an Intelligent SMS based Remote Metering System. *Proceedings of the IEEE International Conference on Information and Automation*, 1040–1043. https://doi.org/10.1109/ICINFA.2009.5205071

[5] Maurya, K., Singh, M., & Jain, N. (2011). Real Time Vehicle Locking and Tracking System using GSM and GPS Technology-An Anti-theft System. *International Journal of Technology And Engineering System*, *2*(3).

[6] Mostakim, N., Sarkar, R. R., & Hossain, A. (2019). Smart Locker: IOT based Intelligent Locker with Password Protection and Face Detection Approach. *International Journal of Wireless and Microwave Technologies*, *9*(3), 1–10. https://doi.org/10.5815/ijwmt.2019.03.01

[7] Kumar, A., Sood, P., & Gupta, U. (2020). Internet of Things (IoT) for Bank Locker Security System. *6th International Conference on Signal Processing and Communication*. https://doi.org/10.1109/ICSC48311.2020.9182713

[8] Dhoot, A., Nazarov, A. N., & Koupaei, A. N. A. (2020). A Security Risk Model for Online Banking System. *Systems of Signals Generating and Processing in the Field of on Board Communications*, 1–4. https://doi.org/10.1109/IEEECONF48371.2020.9078655

[9] Turner, D.-M., & Hazari, S. (2007). Bringing Secure Wireless Technology to the Bedside: A Case Study of Two Canadian Healthcare Organizations. *Web Mobile-Based Applications for Healthcare Management*. https://doi.org/10.4018/978-1-59140-658-7.ch007

[10] Tariq, F., Rashid, M., & Khan, M. N. (2015). Implementation of Smart Homes and Industrial Automation System with Secure Communication over GSM. *Universal Journal of Electrical and Electronic Engineering*, *3*(4), 125–131. https://doi.org/10.13189/ujeee.2015.030403