International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X;pISSN:2321-2241 Volume: 11; Issue: 4; April -2022

IOT Based Bank Locker Surveillance System Using Knocking Pattern

Ms. Krishnaveni A, M.Tech(CSE),
Assistant Professor, Dept of ISE,
krishnaveni.nhce@gmail.com,
New Horizon College Of Engineering,
Bangalore.

Ms.Akshaha Patil ,M.Tech(CSE),
Assistant Professor, Dept of ISE,
nhce8kshata08@gmail.com,
New Horizon College Of Engineering,
Bangalore.

Ms. Sony M Kuriakose,M.Tech(CSE),
Assistant Professor, Dept of ISE,
sonynhce@gmail.com,
New Horizon College Of Engineering,
Bangalore.

Abstract-**This project will be focused on effective recognizing and controlling system for Bank locker room which is fully self-determining. In cases of robberies, it commonly happens that the banned entrance in locker room area which can be detected by our security system. If the robbery take place the banks are not capable to recognize the robber due to absence of the proof by using the current human security operated system. The system will be designed in effective way by recognizing and controlling the illegal person to access the locker for the safety of bank locker room. In this, we proposed a three-phase conformation of procedure for smart locker using some registered pattern knocks, camera and SMS which check out the user. As we compare to any other previous approaches our system uses the web App which send an OTP to user's mobile which has to be opened using android app which highlights the smart security. The designed system is highly proficient and consistent because of three security stages and not capable to break the combination of this, three stages.**

I. INTRODUCTION

Security systems plays a very important role in today's modernized industrialized era. Throughout our life, the hard-earned assets and valuables things are expected to be safeguarded under certain security. It is basically designed in order to avoid the risk of vulnerabilities to our valuable items. In this technological world, the system includes biometrics along with digital code lock which response in the way for matching or mismatching the code. Any mismatch to the series of authentication during verification is done raises an alert sound. To overcome the security issues faced with the locker system now-a-days, the locker security system is proposed using IoT (Internet of Things), face recognition and OTP (One Time Password).

For this we shall be using Raspberry Pi for capturing image, processing it and then sending it through message and Internet to the user. The Raspberry Pi captures the image of a person who tries to access the bank locker and then process it and sends it to the user's as picture message. This can also be used in places such as personal workplaces, office locations such as records, server, document storage places and any other places where security is the major concern.so in order to a have highly secured locker so we are using this proposed method.
In this proposal, we have raspberry pi camera fit behind the locker if a person tries to access the locker he/she needs to on the camera, knock the door with the registered knock pattern unit activating the complete circuit and it will be sending the OTP to the authenticated user in the encrypted form which has to be opened in the android to see it's decrypted form.

The major issue of present locker systems in today's world is security. Traditional locker system uses key based system and password system. As an individual can lose his key or forget password. To overcome this problem, in this paper proposed a locker system using face recognition, knocking pattern and OTP. Face recognition is a type of biometric method where an individual is identified by comparing live capture of image with the stored record for that person. Face recognition is implemented using Raspberry pi camera. Facial recognition systems are majorly used for security purposes which can be used in different varieties of applications. Proposed method uses SVM for face recognition. In the proposed framework a novel and efficient approach for the system is implemented by face recognition, knocking pattern and One-time password. Knocking pattern is implemented using touch sensors. A one-time password (OTP) is a dynamic password which is valid for only one session.
To overcome pattern analyzer and fingerprint problem, in this paper we proposed a locker system using face recognition, knocking pattern and OTP. An approach for face recognition is implemented by using face recognition algorithms. Proposed method uses SVM. The person who is trying to access the locker will be captured by the camera and then it will be processed in Raspberry Pi and sends it to user's account as picture message in web application unknown to the user, he/she can make the locker to be in closed state. Knocking pattern can be implemented using IOT sensors called touch sensors. An OTP is generated after the two stages of authentication which is a dynamical one time password. The OTP generated by the server will be encrypted and the authenticated user will get this OTP. To view he/she has to useandroid app to see the encrypted OTP and to open the locker. Thus, the bank locker will be highly secured from the unknown user and this three level authentication cannot be easily hacked hence the robberies will become less.

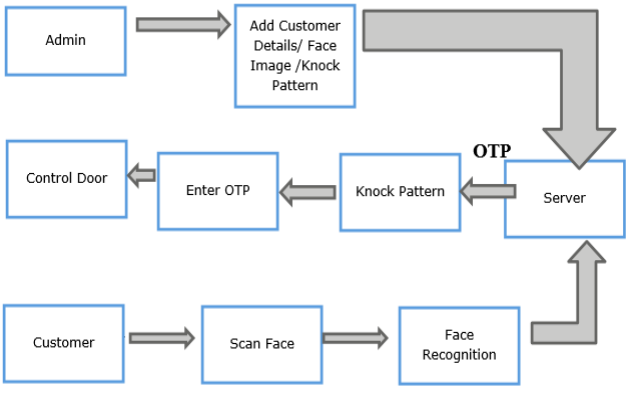
II. RELATED WORK

SVM algorithms are used for face recognition is the first level of authentication. The image input is compared with the database image so that authentic person is being facilitated or allowed to access. Some of the proposed techniques are three dimensional facial recognition which employs a 3-D sensor to obtain precise information about the distinct features of the face (nose, chin and eyes). This method does not depend upon the intensity of light and angle. Another new method is skin texture analysis in this approach the significant lines, patterns and spots visible in person's skin as captured in scanned images are converted into mathematical function. Some facial recognition programs are FACEFIRST compatible for low resolution application in mobile and live-video surveillance.

Second level of authentication is knocking pattern, When the face recognition is done, you will get the display message to knock the locker by using your knocking pattern.

Third level of authentication is otp generation, If the face recognition process and knocking pattern is successful, server generates the OTP using random function and encrypts it using AES encryption.

III. SYSTEM DESIGN



Admin can add the details of the user only then the user can access the locker. As explained in the above we use three stages of authentication as shown in the diagram. Once the admin adds the details of the user he has permission to openthe locker after the three stages.

The first stage is face recognition using raspberry Pi camera, the input image is compared with the database image so that

authentic person is being facilitated or allowed to access.When the face recognition is done, you will get the display message to knock the locker by using your knocking pattern.

If the face recognition process and knocking pattern is successful, server generates the OTP using random function and encrypts it using AES encryption.

IV. DESCRIPTION OF THE PROJECT

1. Registration

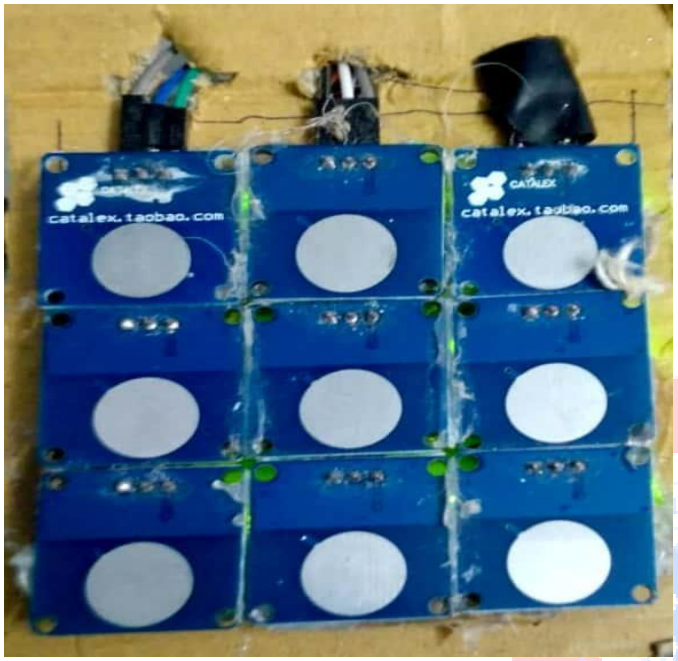
Admin first login into the portal to add the customer details. Admin can add the customers details along with the face image. All these details are saved in the application server. The customer details are sent from web browser to the application server using HTTP protocol. The customer details are saved in the mysql database. The captured customer face images are trained in the server using Linear Support Vector Machine (LSVM) and the trained model will be updated.

2. Face Recognition

When a customer visits the bank to access his/her locker, needs to scan the face for face recognition. The camera connected with raspberry pi is used to capture the image. The captured face image is sent to the server. Once the server receives the image, process it.

we use SVM(support vector machine) algorithms for face recognition. It is a supervised machine learning algorithm which can be used for both classification or regression challenges.

3. Knocking Pattern



When the face recognition is done, you will get the display message to knock the locker by using your knocking pattern. Once Knocking pattern is done, the server will check the details in the database and conforms the user is there or notand then if the user is present he/she will get an OTP to his/herregistered phone number.

4. OTP Generation

If the face recognition process is successful, server generates the OTP using random function and encrypts it using AES encryption. The encrypted OTP is sent to the customer's mobile number as a SMS. Once the customer receives the encrypted OTP, opens the android app, and verifies himself byopening the correct password. If verified, the app decrypt the received OTP and displays on the app.

we use AES(Advanced Encryption Standard) for encryption and decryption of generated OTP. It is a symmetric block cipher chosen for encrypting texts which can be decrypted with the original encryption key.

The popular and widely adopted symmetric encryption algorithm is known as the Advanced Encryption Standard (AES). It is found at least six time faster than the triple DES.

A replacement for a DES was needed as its key size was too small. With the increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

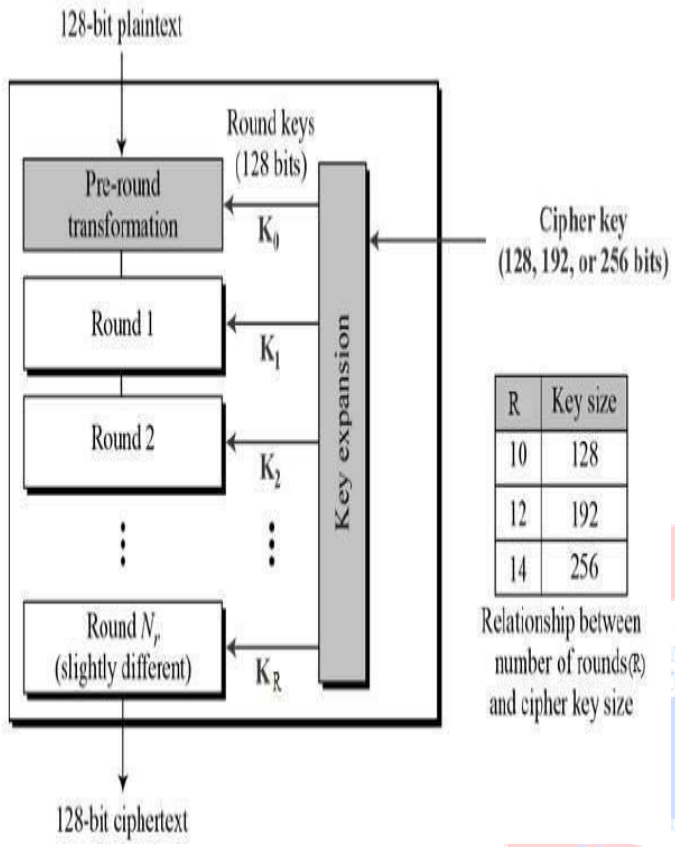
A. Operation of AES

AES is an iterative rather than a Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involves the replacing inputs by specific outputs (substitutions) and others involves the shuffling bits around (permutations).

AES performs all its computations on bytes rather than the bits. Hence, AES treats 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

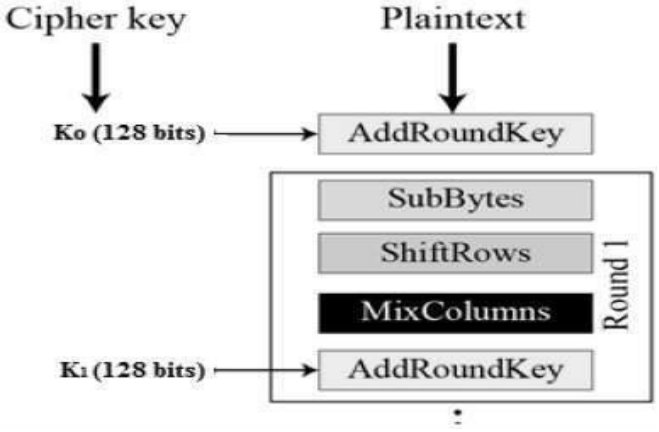
DES, the number of rounds in AES is a variable and depends on the length of the key. AES uses the 10 rounds for 128-bit keys, 12 rounds for the 192-bit keys and 14 rounds for 256- bit keys. Each of these rounds uses different 128-bit round key, which is calculated from the original AES key.

The schematic the of AES structure is given in the following illustration −



B. Encryption Process

Here, we restrict to description of typical round of AES encryption. Each round comprises of four sub-processes. The first round process is depicted below −



1) Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

2) Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

3) MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

4) Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

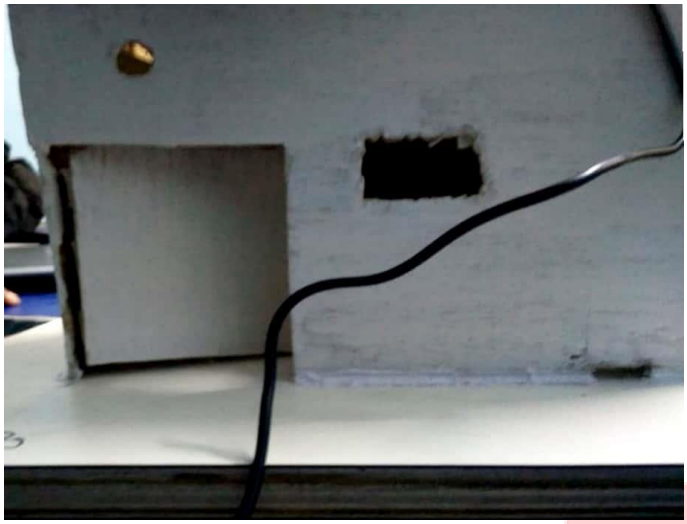
C. Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −

- Add round key
- Mix columns
- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

5. Control Door



To access the locker, the customer now can enter the OTP using the keypad fitted with the locker box. The entered OTP is sent to the server using TCP/ IP protocol from the wifi modules connected with the locker box. Server varies the OTPand the corresponding locker box number and if successful send signal to the locker box. Once locker box receives the signal, opens the door.

CONCLUSION

In this paper a design framework of Locker system is proposed. The locker system is installed with face recognition,knocking patter and OTP service as security purpose. SVM is used to recognize the human face. The technique of face recognition phase is performed accurately. Then OTP is generated and send to the owner by means of SMS. The proposed system is more secured compared to the previous techniques where the user was only able to access the locker either using OTP and knocking pattern. This method can also be used as the home passage security framework with sensors and actuators.

In this proposal, we have raspberry pi camera fit behind the locker if a person tries to access the locker he/she needs to on the camera, knock the door with the registered knock pattern unit activating the complete circuit and it will be sending the SMS to the authenticated user in the encrypted form which has to be opened in the android to see it's decrypted form. Hence the robberies, thefts will be reduced by implementing this. It can be used in homes, offices and also in workstations.

III. REFERENCES

[1] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, ''The FERET evaluation methodology for face-recognition algorithms,'' IEEE Trans. Pattern Anal. Machine Intell., vol. 22, no. 10, pp. 1090---1104, 2000. [2] A. Pentland and T. Choudhury, ''Face recognition for smart environments,'' Computer, vol. 33, no. 2, pp. 50---55, 2000.

[3] J. Goldstein, L. D. Harmon, and A. B. Lesk, "Identification of Human Faces," Proc. IEEE, May 1971, Vol. 59, No. 5, 748-760.

[4] M. A. Turk and A.P. Pentland, Face recognition using eigenfaces, ''Proceedings of the IEEE'', 586-591, 1991.

[5] A. Johnston, H. Hill, and N.Carman, ''Recognizing Faces: Effects of lighting Direction, Inversion and Brightness Reversal,'' Cognition, Vol.40, PP. 1-19, 1992.

[6] Matthew Turk and Alex Paul Pentland,1991. Eigenfaces for Recognition, Journal of Cognitive Neuroscience, vol.3, no.1, pp.7186.

[7] Bhawna chouhan, shailja shukla." Iris Recognition System using canny edge detection for Biometric Identification", International Journal of engineering Sciences and Technology (IJEST), ISSN: 0975-5462 Vol. 3 No. I Jan 2011.

[3] J. Daugman, ''Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters,'' J. Opt. Soc. Amer. A, vol. 2, no. 7, pp. 1160-1169, 1985.

[4] Li Ma; Tieniu Tan; Yunhong Wang; Dexin Zhang, "Personal identification based on iris texture analysis," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol.25, no.12, pp.1519,1533, Dec. 2003 doi: 10.1109/TPAMI.2003.1251145.

[5] Junichi Hashimoto, "Finger Vein Authentication Technology and its Future, "2006 Symposium on VLSI Circuits Digest of Technical Papers, 2006, pp. 5-8. [Jain, 04] Anil K. Jain, Arun Ross and SalilPrabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004, pp. 4-20.

[6] Toshiyuki Tanaka, Naohiko Kubo, "Biometric Authentication by Hand Vein Patterns", SICE Annual Conference, Sapporo, August 46, 2004, pp. 249-253.

[7] Shi Zhao, Yiding Wang and Yunhong Wang, "Extracting Hand Vein Patterns from Low-Quality Images: A New Biometric Technique Using Low-Cost Devices".