Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

Smart Lock with Safe Delegation System

R. Sivakami [1], V.Priyankaselvi [2], S.Chiranjith Raghava[3]

[1]Associate Professor , Department of Computer science and engineering,
Sona College of Technology, Salem, India.Email Id: shivasona07@gmail.com

[2]PG Scholar, Department of Computer science and engineering
Sona College of Technology, Salem, India.Email Id: priyankavellaiswamy@gmail.com

[3]UG Scholar, Department of Computer science and engineering
Sona College of Technology, Salem, India.Email Id: raghavchiranjeet@gmail.com

ABSTRACT

Smart Lock is an electromechanical lock which is planned to perform locking and opening operations on an entryway when it gets such information from an authorized gadget employing a remote convention and a cryptographic key to execute the authorization handle. Biometric as well as passwords are used to secure the locking system. Initially a password given by a user is hashed by using a hashing algorithm, encrypted and it is verified against the one stored in a database. Haar - cascade classifier is used for image identification and biometric authentication. Cryptographic passwords are generated using hashing and symmetric encryption. If the password is same, it unlocks the door or else it raises an alert to the proprietor. Test bed platform for this smart lock system is raspberry pi with Wi-Fi, camera, key cushion framework and a bolt framework. The smart lock proprietor can delegate the One Time Password through SMS if he/she wishes the guest to unlock the door with registered image. To delegate the password and open the smart lock only with delegated password, image recognition system is remotely deactivated by the authorized owner of the locking system as admin and enables the lock to open only with password. All three phases of the proposed system such as biometric authentication, encrypted negative password and safe delegation system are addressed in this paper.

Keywords: Smart lock, Cryptographic password, Haar- cascade classifier, delegation, authentication

1. INTRODUCTION

1.1 IOT BASED SMART LOCK

Anything connected into the internet can be made smart using Internet of Things (IoT). IoT based smart applications are available in every domain like smart home, smart agriculture, smart city, smart environment, smart industry, smart healthcare system, smart car, smart inventory management system and smart governance so on. One of the major applications is smart home which involves automatic controlling of electrical appliances to save the energy consumption and smoke detection system, intrusion detection system for secured home as depicted in Fig 1.

One such vital application is smart lock using IoT for secured home. Many works were done in this area to support smart locking using Arduino and Raspberry Pi boards, some with face recognition system, some with biometric and some with password system. Our smart lock focuses on face recognition with password system –a multimodal smart lock.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

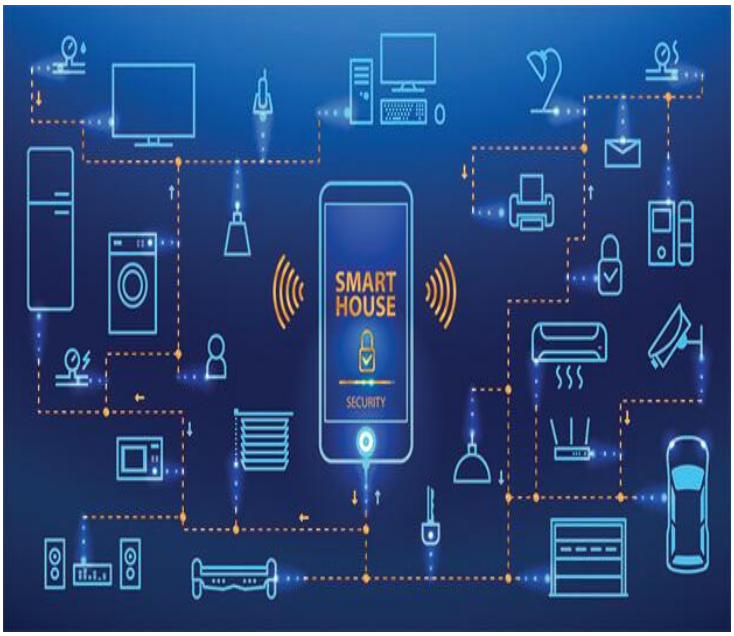

Fig 1. IoT - Smart House

The major problem faced with many of the smart appliances is they are not flexible and are easily hack able as they are connected in the network. One of the most important trade-off when moving from normal appliances to digitalized smart appliances is flexibility. The devices when are secured with passwords are not flexible as they are to be operated by only authorized persons.

To provide flexibility, we need to delegate the authorization occasionally. Passwords are used in almost all online and IoT based applications for authentication purpose. Many applications and devices are breached easily through hacked passwords and hackers. There is a need for delegating the password to authorized persons under certain circumstances. The secured way of delegating passwords can be done with cryptographic techniques such as hashing and encryption. The simple IoT devices like Automated Heating, Ventilation and Air Conditioning (HVAC) can be used to hack the smart lock.

1.2. VULNERABILITIES OF IoT

The layered architecture of IoT with few protocols used at each layer is given in Fig 2. The protocols used at layers 1 and 2 are of less power consumption to support the small and low powered IoT devices. This low power consumption leads to security issues. Security against intentional attackers and safe protection mechanisms are to be carefully planned against accidental failures and threats especially when the developer is laying out the IoT infrastructure. The interface at each layer is vulnerable and as all things are connected into IoT for making them smart, privacy is lost due to huge amount of data collection and lack of proper protection mechanisms.The data being transported is plain rather than encrypted in many network services transport mechanism between device to user interface or from device to cloud, web or mobile interface. IoT transfer data automatically over the net and this high automation leads to increased probability of security breaches and thus careful design of IoT applications to send the IoT data to cloud, data centre or private network.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

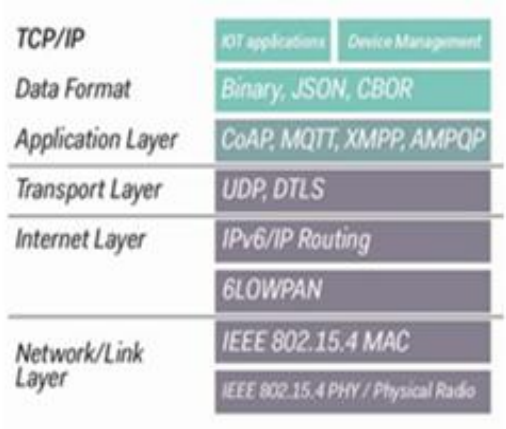

Fig 2. IoT Protocol Stack

The security threats already exist but IoT has increased and further intensifies the threats. As addressed already, threats in the cloud and network are securing data in the cloud especially maintaining data privacy, unauthorized access of the devices in the network. IoT mostly uses wireless transmission and the wireless transmission is prone to errors and malicious attacks. Use of strong passwords and multimode authentication is one of the solutions to provide safe and secure authentication.

Though many steps have taken to strengthen the password by asking the users to include the special characters and specifying the minimum number of characters along with the graph denoting the strength of the password, the hackers can easily guess the password by tracking the previous history of password patterns used by the particular user [1]. Online attackers steal the password as it is transmitted by eavesdropping and also steals it from authenticated server. Joseph Bonneau et al [1] also conclude that having only strong passwords is not sufficient to escape from the hackers. Few works done in analyzing the password security, attacking pattern and user habits reflecting in passwords are given in [5] – [15].

2. EXISTING SMART LOCK SYSTEM

2.1. EMBEDDED CONTROL SYSTEM FOR SMART LOCK

The system proposed by Hasan and Jasim [2] use face recognition system for smart lock and delegate remote authenticate to the owner to open the smart lock using email with the aid of web server. The system uses prominent features of face and binary pattern is established and converted into a vector for matching and classification implemented in OpenCV and the IoT board id Raspberry Pi 2. For remote accessing and delegating authentication to others, their image is captured and if no match is found then it is sent to the owner of the lock. The owner send the security code already loaded into the server using email. If the code matches then the door is unlocked.

2.2. FACE RECOGNITION USING OPEN CV BASED SMART LOCK

The framework given by Deshmuk et al. [3] provides a remote authentication through email. The system uses OpenCV for machine learning to train the system for face recognition. The Harr cascade algorithm is used to extract the features for face detection and Local Binary Pattern Histograms (LBPH) is used for face recognition. The person's picture is captured and binary pattern is computed by comparison with neighbouring cells to generate a histogram. The histogram is matched against those stored in database and for the match found, the door is unlocked otherwise a mail is send to the authorized person along with the captured image of the person who wants to open the lock. If the authorized person wants to open the lock then he sends a mail with the message "allows guest" as authorization delegation. The system uses SMTP and IMAP for mail transmission and raspberry pi 3 and pi camera.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

2.3. DOOR ACCESS CONTROL USING SMARTPHONE

The proposed work in this paper by Tomomi Yamasaki et.al in [16]uses a controller interface framework with Raspberry Pi which is moo taken a toll and expends littler sum of power. When guest movement is identified at Entryway, Camera module interfaced to Raspberry Pi capture pictures, spare it on framework and send it as E-mail caution by means of TCP/IP. The concerned specialist can control the framework and see video stream of camera module through shrewd versatile phone. The framework moreover provides concerned specialist to utilize keen phone to send command for voice alarm when gate crasher is distinguished. The delegation system is shown in Fig 3.

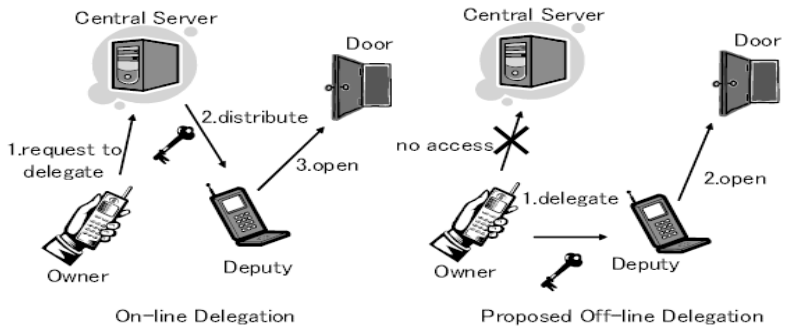

Fig.3 On and Off-line Key Delegation System

Clients can screen visitors and control the entryway bolt on dynamic Secure Shell page designed on android stage and upgraded with JavaScript. This framework finds a wide application in zones where physical presence isn't conceivable all the time.

2.4 THE SHOULDER SURFING RESISTANT GRAPHICAL PASSWORD VERIFICATION

The work presented in [4] is using set of selected images by the user as a mechanism for password verification. The user has to set the Region of Answer (ROA) for the questions displayed in the images he has selected as a secret pass. The work proposed also uses session password from the set the set of images selected as a secret pass and makes the selection to be of an even number.

2.5 SMART CARD – BASED AUTHENTICATION PROTOCOL FOR PASSWORD [17]

Confirmation utilized in watchword is regularly kept up in a expansive framework that overseen the inaccessible get to pc systems. Hence, on list assortment of the assurance and administration issues that happen in old watchword verification conventions, examination has focused on great card-based watchword verification. The work proposed by R.Song in [17] gives out an authentication protocol for smart card remote user authentication.All through this paper, they appear that the progressed recognizable proof verification topic arranged by Xu-Zhu-Feng is inclined to inside and pantomime assaults. The creators arranged relate change of their reply with a substitution conservative vigorous distinguishing proof verification convention, illustrate that the unused convention fulfils the needs of strong distinguishing proof confirmation and are a part of temperate.

3. MULTIMODAL SMART LOCKS WITH SAFE DELEGATION

3.1 NEED FOR SAFE DELEGATION

We propose an IoT based multimodal smart lock system operable with both biometric features and password system to ensure security. The face recognition system with salted encrypted negative password ensures high security to the system with remote user authentication (RUA). Many remote user

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

authentications (RUA) are in practice that uniquely identifies the legitimate user to access the resources or services. Popular RUAs are card based systems. Smart card systems are used for safe RUA. This smart card based remote user authentication allows operating the devices or applications like accessing ATM services without the need for their physical presence. These smart card systems are designed for safe and secure remote user authentication. One time password is also used along with smart cards using a mobile phone or email service which uniquely identifies the user authentication.

We witness numerous pitfalls admitting malignant users to breach the security easily in spite of the all the safety measures. Simple passwords systems alone are also not sufficient as they can be easily hacked. This ended up with biometrics is the only safest technique for remote user authentication but it needs the physical presence of the authenticated user always. So our system uses a combination of biometrics as well as password system for security purposes. The salted encrypted negative password system with negative database is used to overcome the password attacks. The physical presence of the user is not suitable for all the applications. Sometimes there is a necessity to delegate the authentication to others to access the services like unlocking the smart door locks.

3.2 ENCRYPTED NEGATIVE PASSWORD

In this work, security plot called Encrypted Negative Password (ENP) is proposed, which is based on the Negative Database (NDB), cryptographic hash work and symmetric encryption, and a secret word confirmation system based on the ENP is displayed. Encrypted negative password is a secure authentication given by W. Luo et.al in [18]. The NDB is a modern security strategy that's motivated by organic resistant frameworks and contains a wide extend of applications and is modeled by F. Esponda et. al in [19]. Symmetric encryption is as a rule deemed inappropriate for secret word security. Since the mystery key is ordinarily shared by all scrambled passwords and put away alongside the authentication information table, once the verification information table is stolen, the shared key may be stolen at the same time. In this way, these passwords are immediately compromised. But in ENP, the hash value is stored and verification is done along with negative database. Subsequently, the ENP empowers symmetric encryption to be utilized for watchword assurance. The work flow of the system is represented in Fig 4.

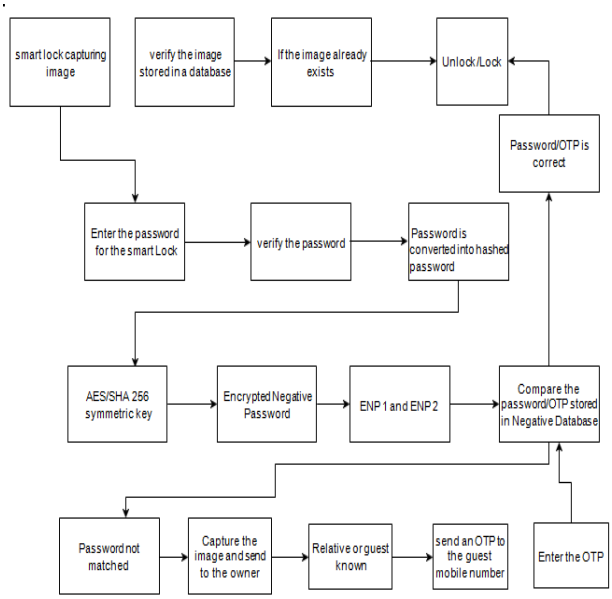

Fig 4. Block Diagram of Safe Delegation Smart Lock System

As an execution of key extending, multi-iteration encryption is presented to encourage progress the quality of ENP. Compared with the salted watchword conspire and key extending, the ENP ensures the differences of passwords by itself without presenting additional components (e.g., salt). In this work a watchword

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

assurance plot called Scrambled Negative Secret word is utilized by twofold encryption such as ENP, ENPI and ENPII. We analyse and compare the assault complexity of hashed watchword, salted watchword, key extending and the ENP assures security against all possible password attacks.

3.3 SAFE DELEGATION

If the verification table password that is encrypted by a password given by an owner in a database table is compared with the password that encrypted by a new user recently type a password is same, then the lock will open, and it is not a same password it sent an alert message to the owner. Thus, these passwords are directly compromised.

We tend to provide a high-level security for the password known as Encrypted Negative Password. Further improve the security double levels encrypted technique such as ENP1 and ENP2 is generated to give best password security verification. Initially the person who is standing in front of the door is captured and it checked in a database whether the image is present in a database or not and if it is not stored in a database it denotes to the owner of the house. Smart lock sends an image with a message that unauthorized person is standing in front of the door. The owner can view the person and if it is a guest owner, a One Time Password is sent to the guest mobile number. After that the guest can unlock the door by typing the One Time Password send by the owner or else owner itself can unlock the door by using the app which is developed in our proposed system.

3.4. ALGORITHMS AND FEATURES

In Encrypted Negative Password, it uses the prefix rule with permutation to get negative passwords that is Negative database. It consists of the Hashing Technique such as Secured Hash Algorithm.

3.4.1. Hashing

SHA-256 is one of the hash functions in SHA-2 crypto graphical hash functions. Secured hash algorithm in a method of unidirectional hash and is generated from any piece of information. However, the data cannot be generated from the hash. In easy words, Secured Hash Algorithm-256 in every cryptographic hash method has a length 256 bits as given in Fig 5. It is Keyless Hash function and it associates with the Magnetic Detection Code. The SHA-256 is an algorithm and it is one kind of SHA-1 format. SHA-256, have the cushiony & splitted into the blocks of 512-bits. According to the size of the variants size of the output, message, rounds, blocks and internal size varies.

Fig 5. Secured Hash Algorithm

3.4.2. AES Features

The features of AES as in Fig 6 have n bit of plain text and it has a pre-round transformation it will go as many rounds according to the number of bits. After that the key is expanded according to the round.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

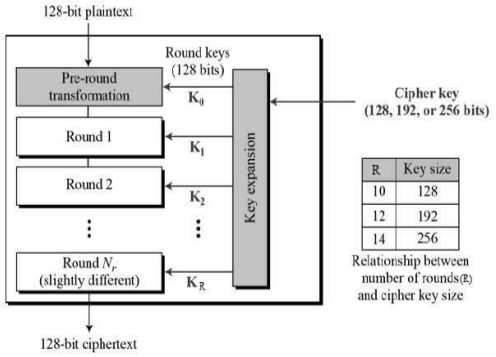

Fig 6. AES Design

3.4.3. AES Transformation

The AES method transforms by shifting a rows and a columns.Then the encrypted key is supported by the number of substitutions based on the size of the key.

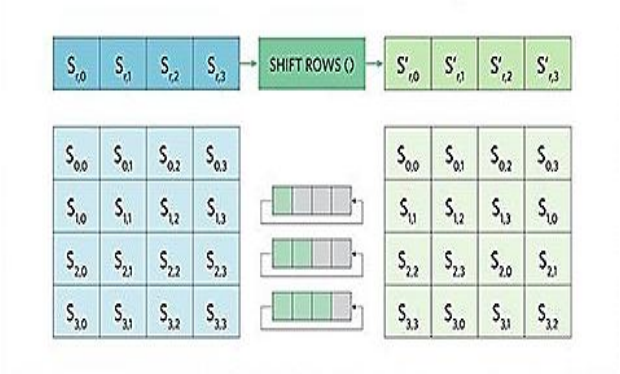

Fig 7. AES Transformation

3.5 WORKING PRINCIPLE OF SMART LOCK

Initially a person is standing in front of the camera is visible to the owner. He/she tried to open the lock by giving a password. If the password is correct it unlocks the door or else it intimates the notification to the owner that someone tries to unlock the door by giving password in a Smart Lock. It requests the house owner whether to unlock the door to the guest or not. If he/she wishes to unlock the door they can unlock the door by using the app developed. Another way to unlock the Smart Lock is sending a one-time Password to the guest from the user authentication. The password is safely delegated using ENP and NDB. If the user enters the OTP it verified in a database whether a given OTP is correct or not. If the OTP is correct it unlocks the door to the guest. This process is represented in the block diagram Fig.4.

3.5.1 Image Capturing Using Raspberry Pi

In a smart lock Face detection is the first step it is detected by using the haar classifier to capture and analyze the image for verificationThe haar classifier is pre-trained within the OpenCv bundle. The haar classifier file location ought to be within the catalog where the most program record is put away. As this will be utilize afterward on for making database catalog containing sub catalogs that has a place to the confront database.In this work making database sub-directories each will comprise of 45 pictures of each individual. The haar classifier extricates confront picture by making utilize of edge include, line highlight and centre-

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

surround highlights. The final errand is to recognize the confront, for this we are utilizing recognizer named Nearby Parallel Design Histograms (LBPH).

The thought to utilize the LBPH is to dodge light impact in case any and it discover the nearby structure of picture by comparing each pixel to the neighboring pixel. Once the picture is nourished to the framework, the recognizer will create histogram of that picture which can be coordinated to the existing histogram. The individual with the outmost coordinating result will be named within the yield window. In case of picture is recognized the electromagnetic bolt will get open through the activity started by raspberry pi.The interface for dc motor, camera and keypad for checking the working of smart lock system is given in Fig. 8.

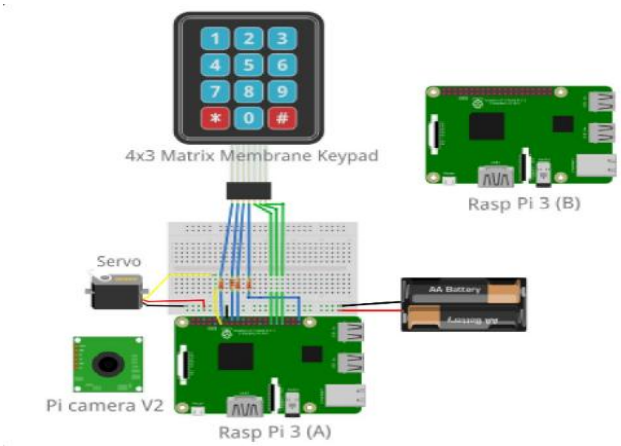

Fig 8. Raspberry Pi interface (Reference:courses.ece.cornell.edu –Face Recognition Door Lock)

In case the picture isn't recognized at that point the captured picture will be sent through raspberry pi utilizing SMPP(Short Messaging Peer To Peer) protocol is used to send message as a intimation to the owner. The reaction of the proprietor within the subject itself will be recovered by raspberry pi inside indicated time. The message sent to the owner will decide to allow them or not.

3.5.2 Secured Password Delegation

The password given by the user is hashed through a hashing algorithm.The hashed algorithm used in the proposed system is SHA 256.SHA is Secured Hash Algorithm.The Secured Hash algorithm has different number of bits such as 224,256,384 and 512.Secured Hash Algorithm is also one of the cryptographic Hash functions.The Symmetric key algorithm used by SHA 256 bits is AES 256 bits. AES is Advanced Encryption Standard.Then the Hashed password is converted into an Encrypted Negative Password.An Encrypted Negative password is again converted into ENP1 and ENP2.It provides a two level security for the Password .By providing a double security it is more secured than other hashing Algorithm.

3.5.3. SMPP Protocol

The SMPP convention is the “true SMS” convention and is created by the broadcast communications industry particularly for transmitting SMS messages. “SMPP” stands for Short Message Peer-to-Peer Protocol. It is the convention utilized at whatever point a content message is sent from a versatile phone to another versatile phone. SMPP has various focal points, in comparison to SMTP, when utilizing it as a strategy for portable device.

3.5.3. Door Lock

The working of door lock in this framework is recreated employing a DC engine to illustrate the locking and unlocking function. This module is a combination of a transfer driver circuit and a DC engine; this framework uses an arrangement 5V 1A 125 Ω (DPDT). Through Gap SubMiniature DIP Relay to control

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

the DC engine. The driver circuit is additionally given with leads for a 9V battery to drive the engine when activated. The driver is activated by the center module through the GPIO pins.

4. RESULTS AND PERFORMANCE ANALYSIS

The techniques such as cryptographic hash function and encoding able to provide a troublesome to break a Password from Encrypted Negative Password. Performance analysis emphasizes on the ultimate comes about of the proposed framework has been arranged to recognize one of the author's confront, and hence a few confront pictures are taken in changing light conditions and are included to the database which is as of now populated with faces from database. The mobile app developed for safe delegation is shown in Fig 9.

The framework accurately recognizes the confront and opens the entryway which is mimicked by DC Engine with an SMS alert. For an unauthorized individual, the calculation reports non-availability of the confront within the database to the centre module, which in turn advances the live depiction to the owner's mail address for manual authentication beside an SMS alert. If the system recognize the individual by physical presence or by delegation then the door unlocking is usually done by answering to the Pi's Short Messaging Service with a secure code as its subject; this code can be changed by the proprietor. Once the Pi gets this code, it approves it and opens the door.

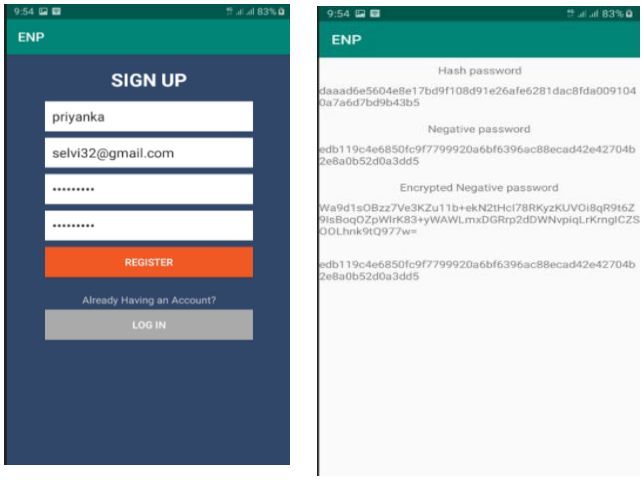

Fig 9. Mobile App for ENP

5. CONCLUSION AND FUTURE ENHANCEMENT

IoT based smart lock system with safe delegation system alone is considered here in this system which is strong enough to defeat the password attacks and also secured even if the hacker access the database by compromising any one of the IoT device because the information about the password is stored as hash value only and the database used for verification is a negative database. If we want fully secured system then all possible attacks in IoT are to be addressed which requires high computational power and trade off between flexibility is security. Gartner and International Data Corporations (IDC) predicts that IoT will be the surface area for cyber attacks and require integrated solutions to secure the IoT devices and applications and demand for this will increase in the upcoming years. The system will be enhanced for an integrated AI based approach to deal with highly potential cyber attackers and hackers.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1647 - 1656
Received 15 April 2021; Accepted 05 May 2021.

REFERENCES

[1] John.Bonneau,C.Herly, P.C.Van oorschot and F.Stajano (2015 July).Paaswords and the evolution of imperfect authentication. Communications of the ACM.58 (7), 78-87.

[2] Hasan Bakeet, Jasim (2018 September).IoT based Embeded Smart Lock Control System.International Journal of Research in Electronics and Computer Engineering.6(3),2028-2032

[3] A.D. Deshmukh, M.G.Nakrani, D.L.Bhuvar, U.B.Shinde (2019 January). Face Recognition Using OpenCv Based on IoT for Smart Door. Proceedings of International Conference sustainable on computing science, Technology and Management.1066-1072

[4] M.A.S.Gokhale and V.S.Waghmare (2016 March). The shoulder surfing resistant graphical password authentication technique. Procedia Computer Science.79,490-498.

[5] J.Ma,W.Yang,M.Luo,and N.Li (2014 May). A Study of probabilistic password models. IEEE Symposium on Security and Privacy.689-704.

[6] A.Adams and M.A.Sasse (1999 December). Users are not the enemy. Communications of the ACM.42 (12), 40-46.

[7] E.H.Spafford(1992)Opus:Preventing Weak Password choices. Computers & Security.11 (3), 273-278.

[8] Y.Li, H.Wang, and K.Sun (2017 October). Personal information in passwords and its security implications. IEEE Transactions on Information Forensics and Security.12 (10).2320-2333.

[9] D.Florencio and C.Herley (2017). A Large Scale study of web password habits. Proceedings of the 16th International Conference on World Wide Web, ACM.657-666.

[10] R.Shay,S.komanduri, A.L.Durity, P.S.Huh, M.L.Mazurek, S.M.Segreti, B.Ur,L.Bauer, N.christin (2016 May). Designing password policies for strength and usability.ACM Transactions on Information and System Security.18 (4).13:1-13:34.

[11] D.wang ,D.He,H.Cheng, and P.Wang (2016 January). FuzzyPSM:A new password strength meter using fuzzy probabilistic context free grammars. Proceedings of 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.595-606.

[12] H.M.Sun,Y.H.Chen, and Y.H.Lin (2012 April). oPass:A user authentication protocol resistant to password stealing and password reuse attacks.IEEE Transactions on Information Forensics and Security.7(2),651-663.

[13] M.Zviran and W.J.Haga (1999). Password Security: An empirical study.Journal of Management Information Systems.15 (4), 161-185.

[14] Andriotis,T.Tryfonas ,and G.Oikonomou (2014). Complexity Metrics and user strength perceptions of the pattern-lock graphical authentication method. Proceedings of Human Aspects of Information Security, Privacy, and Trust, Springer International Publishing.115-126.

[15] D.P.Jablon (1996 October). Strong password only authenticated key exchange. SIGCOMM Computer Communication Review.26(5).5-26.

[16] Tomomi Yamasaki, Toru Nakamura, Kensuke Baba, and Hiroto Yasuura (2007). A Door Access Control System with Mobile Phones. Conference Proceedings.230-240

[17] R.Song (2010). Advanced Smart card based password authentication protocol. Computer Standards and Interfaces.32 (5), 321-325.

[18] W. Luo, Y. Hu, H. Jiang and J. Wang (2019 January). Authentication by Encrypted Negative Password. IEEE Transactions on Information Forensics and Security. 14(1).114-128.

[19] F.Esponda, E.S.Ackley, S.Forrest, and P.Helman (2004). Online negative databases. Proceedings of Artificial Immune Systems, Springer Berlin Heidelberg. 175-188.