International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

DOOR LOCK SYSTEM USING CRYPTOGRAPHIC ALGORITHMS BASED ON IOT

Shruti Jalapur[1], Afsha Maniyar[2]

[1]*Asst professor, Computer Science and Engineering, Secab Institute of Engineering and Technology, Karnataka, India*
[2]*M.Tech student, Computer Network and Engineering, Secab Institute of Engineering and Technology, Karnataka, India*

Abstract – *The Door lock system finds its applications in places such as offices buildings, banks, shopping centers, server rooms, labs and homes. There are also many other applications of a door lock system. In the recent development in technology, Internet of Things (IoT) has gone through many revolutionary changes in the area of industries, smart home application, agriculture, health facilities, smart phone and etc. In the area of networking IoT finds applications related to data confidentiality, control over unauthorized access of confidential data and also remote access of information. The project aims in designing a Door Lock System based on IoT using cryptographic algorithms. The system designed on the basis of IoT achieves applications of confidentiality, security and also remote access of data. Sometimes, the data shared over a network might not be secured. Therefore many researchers are taking interest in developing such a system secured from hackers. The cryptographic algorithms which are used in this door lock system will protect the data being communicated from hackers, because the data is as important as the valuables behind the door.*

Key Words: Door Lock, Security, PIR sensor, Cryptographic algorithms, Crypto System.

1. INTRODUCTION

The door lock systems are designs to protect the valuable things. Door lock system finds there applications in offices buildings, banks, shopping centers, server rooms, labs and homes. There are also many other applications of a door lock system. In the recent development in technology, Internet of Things (IoT) has gone through many revolutionary changes in the area of industries, smart home application, agriculture, health facilities, smart phone and etc. In the area of networking IoT finds applications related to data confidentiality, control over unauthorized access of confidential data and also remote access of information. The project aims in designing a Door Lock System based on IoT using cryptographic algorithms. The system designed on the basis of IoT achieves applications of confidentiality, security and also remote access of data. Sometimes, the data shared over a network might not be secured. Therefore many researchers are taking interest in developing such a system secured from hackers. The cryptographic algorithms which are used in this door lock system will protect the data being communicated from hackers, because the data is as important as the valuables behind the door. There are many existing Door lock systems, which provide security only to the door locks but they do not provide any confidentiality of data, nor is the data being transmitted secured against hackers. The existing door lock systems use passwords, RFID, OTP, biometric, and also camera. But none of the works related to door lock has provided a full security. The security is in term of physical security of door, remote access of the confidential data, and security of confidential data over a network. In the password centered Door lock system, the information is provided to the smartphones. In that case the data being communicated between the lock system and the smartphone is not secured. The hackers can hack the data, which is being communicated over the networks. The data over the network is at risk and can be sniffed by any unauthorized person in case of cyberattacks. Therefore, it is essential to maintain data confidentiality and integrity. In this digital era there is a need of such door lock system which is highly secured. The project presents a door lock system which uses the cryptographic algorithms such as AES-128 (Advanced Encryption Standards) and SHA-512 (Secure Hashing Algorithm) to protect the data over network.

2. LITERATURE REVIEW

[1]"SMART DOOR LOCK SYSTEM" This project aims to put forward a door lock system, that let on the user to operate the door remotely by means of 'face-recognition' through camera fixed on the hardware system. The remote access is done via a smartphone. The system consists of a cloud back-end, hardware unit and mobile application. In case of any damage to the face, then the system will not be able to recognize the authorized user. This is the drawback of this system. Also there is no security provided to the cloud.

[2] "AUTOMATIC DOOR LOCK SYSTEM USING PIN ON ANDROID PHONE" This project uses the generation of PIN on an android smartphone for door locking. The OTP is generated whenever a user attempts to unlock the door and the PIN is sent as the notification on to the authorized user smartphone. There is also the voice command functionality

available in the system. The PIN and voice command is given to the system by connecting with blue-tooth. But the network in which the OTP is shared is not safe. Any unauthorized user can hack the OTP and disturb the confidentiality of data.

[3]" AUTOMATIC DOOR LOCKING SYSTEM" The automated door locking system is a project which uses blue-tooth device and the password is entered into this blue-tooth device. This password based system built using blue-tooth is low cost unlocking system but the technology has gone through development and there are many such devices which have replaced blue-tooth. Therefore using blue-tooth is an out dated technique.

[4] "RFID AND ARDUINO BASEDAUTOMATIC DOOR LOCK SYSTEM" The RFID and Arduino based project is studied which is an automatic door lock system is uses RFID (radio frequency identification) technique. The system is provided with a card which is tagged to the object. The system uses electromagnetic field of radio frequency for the transmission of data. It can be developed with low cost. If the card is nowhere to be found or stolen by any person, then the whole system fails to function and in case the card gets stolen then the system will come at risk.

[5] "ANDROID BASD SMART DOOR LOCKING SYSTEM" This project was published in 2018 in the International of engineering research and technology. Here the system is designed for banking and business organization. The security for door is provided and monitored trough arduino. But only a single user is allowed to operate the door lock. Two modes that are normal mode and multi-mode are provided under which the system is made to operate.

3. OBJECTIVES

- Avoiding the unauthorized access of data by increasing the security.
- To resolve the issue of security of belongings and information security, the system is provided with a cryptographically protected and key based lock system.
- The lock system consists of android smartphone app with cryptographic algorithms, hardware system with buzzer, LED's and LCD.
- The data being transmitted over the network is also protected through the cryptographic algorithms.
- It provides remote access of confidential data, physical security of lock system and security of data against unauthorized access.
- To provide users more secure and also a cost-effective technique of door locking system.

4. PROBLEM FORMULAION

Since many decades lock has been very important part of our lives. The locking of door is one among them. No one will stay in home which does not have door which is properly locked, that is to keep the belongings safe and also the home and lives. In the modern era technology had gone through much advancement that there are so many unique door locks designed digitally. The digital door locks find wide application because they are easy to install and are cheap too. The applications of door lock system are industries, smart home application, agriculture, health facilities, smart phone and etc. There are any existing door lock system which works on password, OTP, RFID, biometric and camera etc. In password based system the password is entered by the user through a touchpad o keypad. In systems built on OTP the user needs to enter the OTP which is been generated on the linked mobile number of an authorized user. In systems built on RFID door locking systems the user has to carry the card with itself. RFID is an efficient door look system because it is low cost system, but meanwhile it will fail its working if the card is lost. In the biometric system the characters such as the thumb impression of the person, voice identification, face identification is been verified by the door lock system. In such system the problem is related to the physical damage of the characters of the person. In that case the whole system fails its working. In the system where the information is not only stick to the door lock system, but also shared with the smart phone or any other device, it is important to secure the information communicating over the network. Because the information related to password and username must be kept safe as they are important as that of the belongings behind the door. Therefore it is important to make the network highly secure, this can be done by using Encryption techniques on the network. So, that there should be no unauthorized access of information.

5. PROPOSED SYSTEM

Once the connection of all the hardware parts is established with smartphone, a unique identification key which contains the user name and the password is assigned by the authenticated user. As soon as the user assigns the identification key to the crypto system it gets connected with the server. The information of the username and password is directed to the server. The server stores the information for the authentication process. The server reads the information from the door which can be opening and closing of door and alarm generation is guided to the server. The system uses thee cryptographic algorithms such as AES-128 and SHA-512 for encryption and hashing to protect the data over network. The crypto system performs hashing on the information of the opening and closing of the door using SHA-512 algorithm. The encryption is performed to upload obtained from the door using AES-128 algorithm. The encryption is performed to upload the 'reliability' and confidential' of data. Whenever, an authorized user logs in to the smartphone app

by giving the information through keypad to the crypto system. If the server finds the login details correct then it performs encryption on the data and communicates with crypto system. The crypto system then performs decryption by comparing with help of hashing.

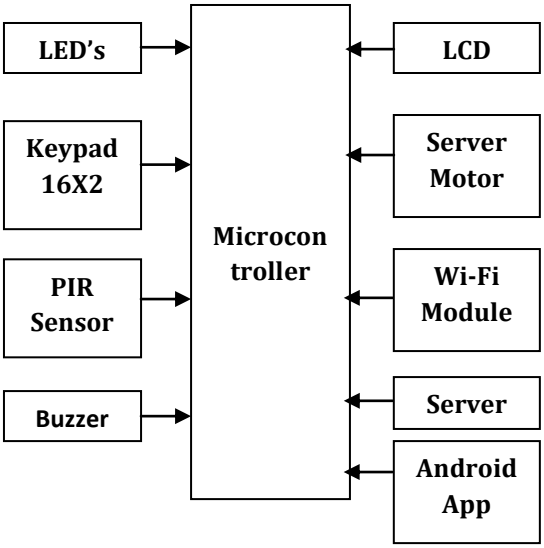

Fig 5.1: Block Diagram of proposed System

Algorithms:

As stated earlier the crypto system consists of two algorithms, applied to provide the integrity and confidentiality of the data. The algorithms used for this security purpose are AES-128 and SHA-512. This algorithm performs encryption and hashing on the user data. AES-128 performs encryption to maintain integrity of data and SHA-512 performs hashing by making the data confidential. Whenever, the user enters the input to the system. SHA-128 performs hashing on the array of input. As soon as hashing is done on the array of input AES-128 encrypts the data. This process is carried out in two steps:

Step 1: The cryptosystem get information about the status of door, PIR evaluation and the user statistics. It takes the statistics in the method of an array of unencrypted text. The SHA-512 performs hashing on the unencrypted text and converts the unencrypted text to the hash-code. To make the hash-code ready for encryption, initially padding is performed on the unencrypted text then 128 bit of earliest data is also computed along with it to make the length multiple of 1024.

Step 2: The fixed length value generated from the hashing is now encrypted using AES-128 algorithm. It performs ten rounds on the hash code. In each round the key size is fixed to 128 bits and 44 sub keys are used in all the ten rounds. The length of sub key is 32 bits. After performing encryption the data is sent to the communication network. This algorithm has resistance against brute force attack, which makes it highly secure among others the AES-128 is symmetric-key encryption method. The data which is encrypted is sent to the server and to the smartphone. The decryption process is applied on the server by means of the symmetric-key. Once decrypting the data, the hash-code is removed from it and plaintext is taken as the information. If the plaintext matches the saved information, then the app updates the information.

6. METHODOLOGY

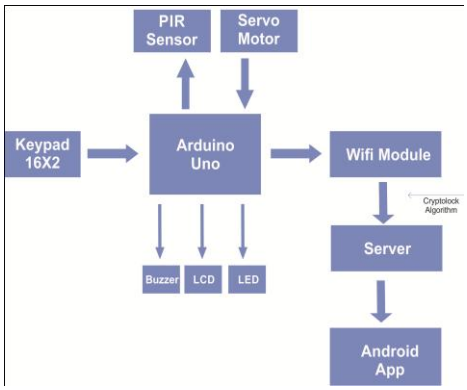

Fig.6.1: Work flow in the System

Designing of a Secure and protected "Door lock system" is the focus of this project. The project is built on IoT, embedded and networking platform. In the modern era all the robots, gadgets and monitoring devices are built on IoT. In this IoT based door lock system the user transmits its confidential data over a network by providing password to protect the belongings behind the door. To answer the problem of security of belongings and also the security of info and password on the network, the project aims to propose a password based "door lock system" designed by applying cryptographic algorithms. It includes a programed hardware along with sensor and servo motor to control unauthorized access and an Android smartphone app to secure communication over a network. The connection between the android smartphone and the hardware parts is established by connecting arduino microcontroller board, which acts as the heart of the system. The user is an authorized person then the information about the door is sent to its smartphone. Cryptographic algorithms are applied on the user info, which makes the data of user secure. In case any unauthorized access is noticed then it will not provide any information about the door lock system. The analysis is done by using both cryptographic algorithms. The cryptographic algorithms are the building blocks of the security system of the door lock system. The not only make the system secure but also flexible to use in

the places where security of the data as well as the valuable belongings of important concern. On testing the system it is also analyzed that the cost to fix the problem is also comparatively low. In general testing is carried out to fix the bugs in software, to overcome the risk of both company and the user, to reduce repairs and development cost of the system and to develop the performance. When any defect is found in the system, the fixing of the problem is just a function of product of life cycle.

7. RESULTS AND ANALYSIS

The Door lock system is built in such a manner that it not only monitors the door and secures the belongings behind the door, but also provides the security to the data being transmitted in the system. The security to the data is provided by applying cryptographic algorithms, which performs encryption/decryption on the text. Once the connection of all the hardware parts is established, the next stage is to provide connectivity between the hardware and android application. This connection is obtained by programming. Whenever user enters the password and username through an application, the authenticity of the user is checked. If the user is an authorized person then the information about the door is sent to its smartphone. Cryptographic algorithms are applied on the user info, which makes the data of user secure. In case any unauthorized access is noticed then it will not provide any information about the door lock system. The analysis is done by using both cryptographic algorithms. The cryptographic algorithms are the building blocks of the security system of the door lock system. The not only make the system secure but also flexible to use in the places where security of the data as well as the valuable belongings of important concern. On testing the system it is also analyzed that the cost to fix the problem is also comparatively low. In general testing is carried out to fix the bugs in software, to overcome the risk of both company and the user, to reduce repairs and development cost of the system and to develop the performance. When any defect is found in the system, the fixing of the problem is just a function of product of life cycle.

7.1 HARDWARE KIT

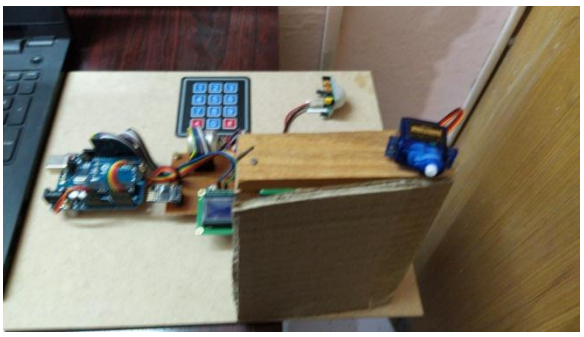

Fig 7.1: Hardware Kit of Door Lock system

8. CONCLUSIONS

In this paper, there is presentation of a secure and protected door lock system. The project not only aims to make the Door Lock system secure, but also secures the info communicated over the network. The security to the network is provided by applying cryptographic algorithms, which areAES-128 (Advanced Encryption Standards) and SHA-512 (Secure Hashing Algorithm). The system also provides the remote access of the information to the authorized user. The algorithms AES-128 and SHA-512 performs encryption and hashing on the user input. The servo motor, which is a motion detector, detects the motion of the human in it range and also from the backdoor. If the sensor detects any entry of unauthorized user then it will send notification to the smartphone app, which is been installed on the smartphone of authorized user. The operations like opening/closing of door are sent to the user. The user can access the information by entering username and password. The security to this password and username is provided through the cryptographic algorithms. The key intention of the project is in designing the door-lock system which is secure and protected; provide remote access of information and to make the data over communication secure. As the future advancement the project can be made more advanced by installing cameras and by monitoring invalid passage using image processing techniques.

ACKNOWLEDGEMENT

The author gratefully thanks to guide Mrs. Shruti Jalapur, for helping and guiding throughout this project. The author extends her thanks for HOD of the Department Dr.Syed Naimatullah Hussain**,** for giving permission to establish this project. The author specially thanks each of the persons who helped me to get information about the environment.

REFERENCES

[1] J. R. Delaney, "The Best Smart Locks for 2019," PCMag, 15 April 2019. [Online]. Available: https://www.pcmag.com/article/344336/the-best-smart-locks. [Accessed 18 April 2019].

[2] “Automatic Door Lock System using pin on android phone” November 2018 [Online]. Available: https://www.academia.edu/37961774/IRJET_Automatic_Door_Lock_System_using_PIN_on_Android_phone

[3] “Automatic Door Locking System” 2016. [Online]. Available: https://www.ijedr.org/papers/IJEDR1601082.pdf

[4] “Rfid and Arduino based Automatic Door Lock System” [Online]. Available: https://www.elprocus.com/automatic-door-lock-system-using-rfid-and-arduino/

[5] https://ijarcce.com/wp-content/uploads/2016/11/IJARCCE-ICRITCSA-26.pdf

[6] "Differences Between Raspberry Pi 3 vsArduino," EDUCBA, [Online]. Available: https://www.educba.com/raspberry-pi-3-vs-arduino/. [Accessed 3 April 2019].

[7] https://web.wpi.edu/Pubs/E-project/Available/E-project-042419-115219/unrestricted/Final_Report_-_Smart_Door_Lock_PDF.pdf

[8] R. Divya and M. Mathew, "Survey on various door lock access control mechanisms,"inCircuit,PowerandComputingTechnologies(ICCPCT), 2017 International Conference on, 2017, pp. 1-3.

[9] P. R. Nehete, J. Chaudhari, S. Pachpande, and K. Rane, "Literature survey on door lock security systems," Int. J. Comput. Appl, vol. 153, pp. 13-18, 2016.

[10] M. K. Shafin, K. L. Kabir, N. Hasan, I. J. Mouri, S. T. Islam, L. Ansari, et al., "Development of an RFID based access control system in the context of Bangladesh," in Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on, 2015, pp. 1-5.

[11] G. K. Verma and P. Tripathi, "A digital security system with door lock system using RFID technology," International Journal of Computer Applications (IJCA)(09758887), vol. 5, pp. 6-8, 2010.

[12] S. Nath, P. Banerjee, R. N. Biswas, S. K. Mitra, and M. K. Naskar, "Arduino based door unlocking system with real time control," in Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on, 2016, pp. 358-362.

[13] T. Kim, H. Park, S. H. Hong, and Y. Chung, "Integrated system of face recognition and sound localization for a smart door phone," IEEE Transactions on consumer Electronics, vol. 59, pp. 598-603, 2013.

[14] M. Madhusudhan, "Implementation of Automated Door Unlocking and Security System," pp. 5-8.

[15] H. Hassan, R. A. Bakar, and A. T. F. Mokhtar, "Face recognition based on auto-switching magnetic door lock system using microcontroller," in System Engineering and Technology (ICSET), 2012 International Conference on, 2012, pp. 1-6.

[16] J. Johnson and C. Dow, "Intelligent door lock system with encryption," ed: Google Patents, 2017.

[17] R. Jagdale, S. Koli, S. Kadam, and S. Gurav, "Review on intelligent locker system based on cryptography wireless & embedded technology," International Journal of Technical Research and Applications, pp. 75-77, 2016