Enhanced Security and Privacy for IoT Based Locker System Operated at Low Frequency Spectrum Using Blockchain

Soumen Santra[1], Sweta Sharma[1], and Arpan Deyasi[2](✉)

[1] Department of Computer Application, Techno International Newtown, Kolkata 700156, India
[2] Department of Electronics and Communication Engineering, RCC Institute of Information Technology, Kolkata 700015, India
deyasi_arpan@yahoo.co.in

Abstract. Conventional locker system faces continuous threat of breaching of data due to phishing scams, which raises high demand of encryption at server's end. Blockchain based security system provides efficient solution so far either by applying personal signature, or by adopting peer-to-peer network. In the present proposal, security is entrusted by generating new encrypted message from the already received binary information from user's end. The code is incremented at each subsequent step which helps to track the number of times the security door is opened with individual time-stamp along with image capture facility. Corresponding circuit is designed at 433 Hz spectrum where relay is connected with electromagnetic door lock through microcontroller. A novel algorithm is proposed to control cloud-based web server for accessing every HTTP request with NodeJS and a MongoDB database. Enhanced security and privacy can therefore be obtained through low-cost hardware system associated with blockchain feature.

Keywords: Blockchain based security system · Digital signature · Internet of Things · HTTP web server · RF communication · Time-stamp image

1 Introduction

The Internet of Things (IoT) has grown in significance in our data-controlled world as a result of technological innovation [1]. The Internet of Things is essentially a technical amalgamation of intelligent devices with embedded chips, sensors, and actuators that gather information about themselves and their surroundings and communicate it via the Internet [2, 3]. The automation of repetitive chores and subsequent real-time monitoring of equipment and tasks are the biggest benefits that IoTs deliver. These gadgets unfortunately typically have inferior processing capacities, security risks, and are more vulnerable to cyberattacks. Additionally, IoTs produce very sensitive personal data about their users, which is then managed by centralized businesses, raising major privacy and data integrity concerns [4]. Because of the technology that could help IoT devices with their issues, blockchain has just lately become popular [5]. Even in the early stages of its

A. A. Sk et al. (Eds.): ISAI 2022, CCIS 1695, pp. 56–63, 2022.
https://doi.org/10.1007/978-3-031-22485-0_6

development, blockchain has attracted experts from all around the world who recognize the many benefits of this technology.

Smartphones and other embedded devices evolve far more slowly than desktop computers [6]. Due to their weak computing capabilities and small data storage, these quiet devices struggle to process transactions utilizing this blockchain-based system. Instead of using IoT devices for mining, some hardware, such as application-specific microcircuit (ASIC) chips, are created specifically for the purpose. Therefore, while considering the integration of blockchain with IoT, new approaches to overcoming these problems are required. Due to the adoption of blockchain technology, one of the main issues is that IoT devices can only be embedded with so many resources [7, 8]. Work has been carried out using CNN based surveillance model [9] where security is adequately taken care of with image recognition and classification technique. As different applications have different requirements, a replacement or a customized implementation of a blockchain system is required [10].

Design of informative interface is the trend of research for the benefit of civilization which is executed either through voice-controlled mode [11], or for ultra-high frequency sensing purpose [12]. Cloud service is integrated with blockchain for providing secured home service [13]. The same, with IoT enabled circuit, are recently implemented for accident prevention under real-time condition [14]. For visually impaired people, blockchain technology can provide assistance when augmented with microcontroller based low-cost circuit [15] and useful for common people. Secured, data immunable transportation system is very recently proposed with the claim of robust security and transparency [16].

However, implementation of blockchain technology in those cases is difficult owing to the complex circuitry requirement. A few works are reported only in the domain financial transactions [17] and multimedia content protection [18]. In this present work, peer-to-peer security system is investigated and analyzed by designing one smart low-cost system at 433 Hz. To provide an additional security layer, binary information for opening the locker is converted into another cryptic message, and time-stamp will be given for each time when the locker will be opened. For accessing every request, simple yet novel algorithm is proposed with MongoDB database. Results are discussed in the next section along with system architecture, data flow and hardware circuit.

2 System Architecture and Dataflow

Architecture for the proposed smart home security system is described in Fig. 1, It has been found that PIR motion sensor is connected to GPIO pins of microcontroller. LCD monitor is interfaced with Raspberry web server along with mounting of loudspeaker. The Raspberry Pi is connected to a relay driver circuit that uses the IC ULN2003 to control an electromagnetic door lock. On an SD card or USB flash drive linked to the Raspberry Pi, the image that was taken can save the date and time.

Figure 2 shows the flow chart of knowledge communication. Each of the subsequent subsections provides an in-depth explanation of how the devices communicate with one another. The Elegoo board transmits an RF signal from its transmitter to the RF receiver found on the Raspberry Pi at first when the reed switch is open. The Raspberry Pi then issues an HTTP POST request to a cloud-based RESTful web server. The top user can then view the door open events by date and time thanks to this web server, which either pushes information or receives GET requests from an Android application. The following sections mention a number of open-source libraries.

When the door is opened, the reed switch is actuated, and the transmitter sends a 433 Hz RF transmission using the Arduino's RC-switch library. Each time a door is opened after that, a code is sent to the Raspberry Pi receiver, which is increased. This enables the Raspberry Pi to keep track of specific door-opening incidents.

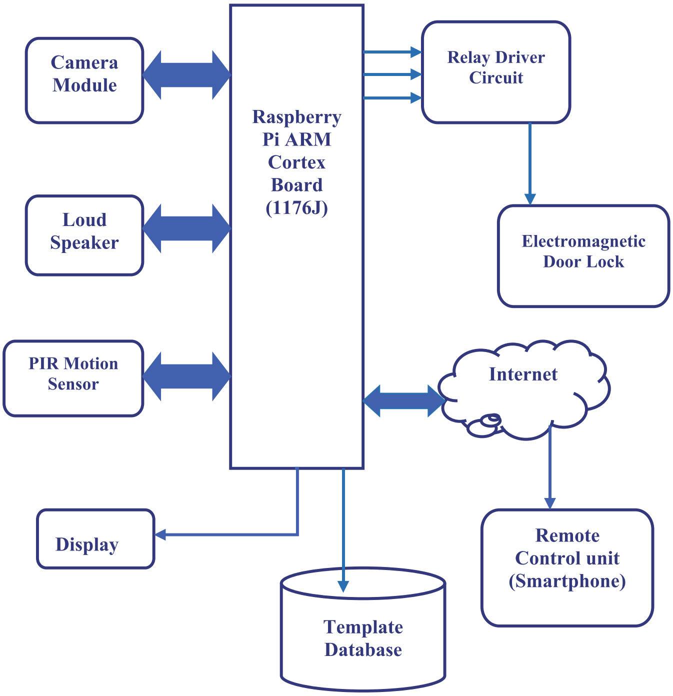
Camera Module
Loud Speaker
PIR Motion Sensor
Raspberry Pi ARM Cortex Board (1176J)
Relay Driver Circuit
Electromagnetic Door Lock
Internet
Display
Template Database
Remote Control unit (Smartphone)

Fig. 1. System architecture for IoT-based smart security

The entire covered area of the home is being monitored by using a simple piece of aluminum (Al) foil as antennas on the receiver and therefore the transmitter when the reed switch is enabled, which sends an uninterrupted stream of binary numbers to the receiver attached to the Raspberry Pi. In order to receive the binary codes, the Raspberry Pi used the 433Utils library and the wiring Pi library. The following stage of the communication process will be carried out by a Python script after it has read the document output containing these codes.

A Python script using the requests library checks the document for brand-new updates every second after the binary codes are received and sent as output to a document. An HTTP web server built with NodeJS and a MongoDB database receives a POST request when replacement code is placed within the page. Door open events will be stored by date and time on this server's RESTful API. The Android application will use GET requests to access the information stored in this database.

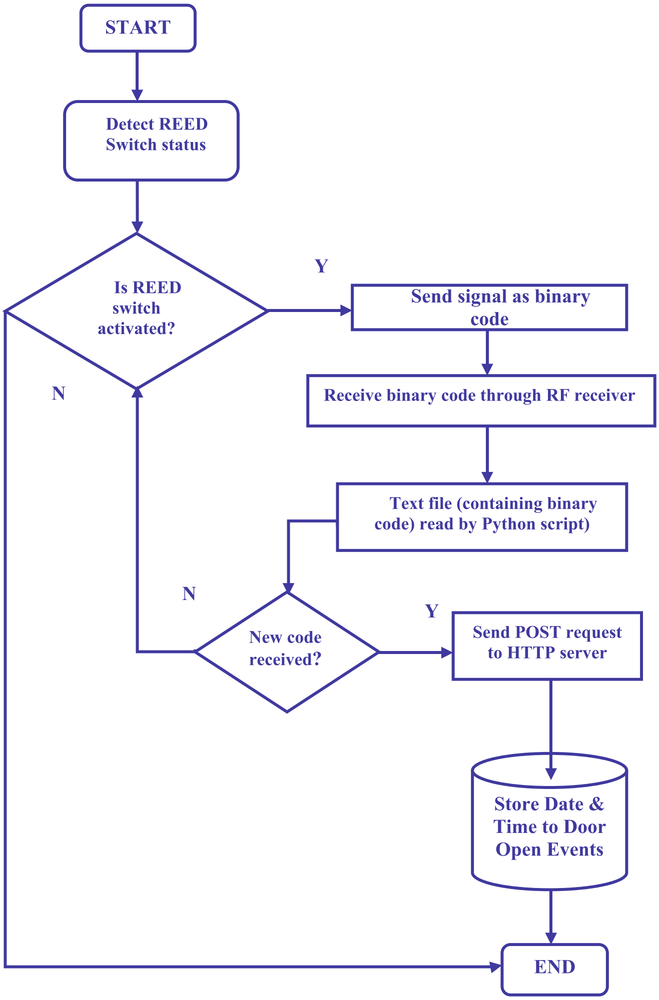
START
Detect REED Switch status
Is REED switch activated?
Y
N
Send signal as binary code
Receive binary code through RF receiver
Text file (containing binary code) read by Python script)
N
New code received?
Y
Send POST request to HTTP server
Store Date & Time to Door Open Events
END

Fig. 2. Flowchart representing data flow through the system

The interaction between internet servers is the last stage of the communication process. But for the purposes of this specific task, the application sends GET requests to the server since it is possible to deliver push notifications whenever a replacement door open event is identified by the online server. The Android application uses a variety of libraries that are accessible through the Android Studio, however the Volley library is the only one that won't process requests.

3 Circuit Design

For the circuit design, Arduino, buzzer, keypad, servo motor, and LCD are considered as major equipments. Arduino is used to control processes like taking a password from the keypad module, comparing passwords, rotating servo motor, driving buzzer, and sending status to the LCD display. The keypad is used for taking passwords. The buzzer is used for indications. The servo motor is used to open the gate while rotating, and the LCD is used for displaying the status or messages on it (Fig. 3).

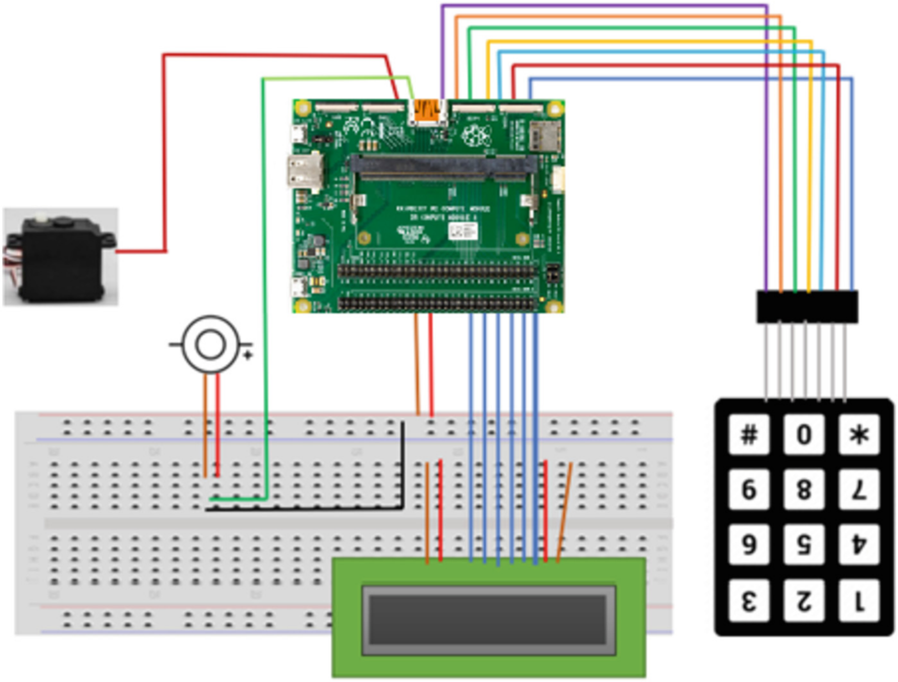

Fig. 3. Proposed system design

4 Proposed Algorithm

The algorithm as proposed is based on the dataflow as mentioned in Fig. 2. In this section, algorithm is described with some arbitrary values, and can be set as per requirement.

```
STEP 1: Start
STEP 2: Initialize variables
STEP 3: Define a function as unlockdoor()
STEP 4: delay(900), setCursor(0,0), print(" "), setCursor(1,0), print("Access Granted")
STEP 5: setCursor(4,1), print("WELCOME!!"), setCursor(15,1), print(" ")
STEP 6: setCursor(16,1), print(" "), setCursor(14,1), print(" "), setCursor(13,1)
STEP 7: Initialise pos=180
STEP 8: Check for condition(pos>=0)
STEP 9: If condition is true then go to STEP 10 otherwise STEP 13
STEP 10: myservo.write(pos) and delay(5)
STEP 11: Decrease pos by 5
STEP 12: Go to STEP 9
STEP 13: End for loop
STEP 14: delay(2000), delay(1000), counterbeep() and delay(1000)
STEP 15: Initialise pos=0
STEP 16: Check for condition (pos <= 180); pos +=5)
STEP 17: If condition is true then go to STEP 18 otherwise STEP 22
STEP 18: myservo.write(pos), delay(15), lcd.clear() and displayscreen()
STEP 19: Set currentposition=0
STEP 20: Increase pos by 5
STEP 21: Go to STEP 17
STEP 22: End for loop
STEP 23: End function unlockdoor()
STEP 24: Stop
```

With the aid of this algorithm, we present a decentralised system that enables quick back-and-forth sharing of device information while storing it on a permission-based, secure chain. The suggested architecture would make it easier for the highest user to connect with the blockchain network; different interfaces are developed by leveraging a variety of online front-end technologies. As representational state transfer application programming interfaces (REST APIs), all of the product-specific services offered by the blockchain network can be accessed by both IoT devices and web clients. Users of the gadgets can manage and recall the surrounding environment without being aware of the physical devices beforehand. The smart contract hosts the ledger functionalities over the network and also provides controlled access to the device meta-data. Participants will only be able to access a predetermined number of approved materials or transactions thanks to an access control policy that has been specified within the platform's design.

5 Conclusion

The Hyperledger Fabric, a permission-based decentralized framework created for developing distributed apps (DApps) or distributed ledger solutions on top of it, is used to implement the current blockchain network. A low-cost smart home security system can be created using the current design as a framework. It was able to create an IoT system that allows users of a household to see when a certain door has been opened by using inexpensive components like microcontrollers. The novel algorithm proposed can be applied to any such type of security system at low frequency range through peer-to-peer network with reliable security.

References

1. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Future General Computer System **82**, 395–411 (2018)
2. Banerjee, M., Lee, J., Choo, K.K.R.: A blockchain future for the internet of things security. Digit. Commun. Netw. **4**(3), 149–160 (2018)
3. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the web of things. IEEE Access **4**, 2292–2303 (2016)
4. Kuzmin, A.: Blockchain-based structures for a secure and operate IoT, internet of things business models, users, and networks, 23–24 Nov 2017, Copenhagen, Denmark
5. Liu, B., Yu, X.L., Chen, S., Xu, X., Zhu, L.: Blockchain-based data integrity service framework for IoT data. In: IEEE International Conference on Web Services, 25–30 Jun 2017, Honolulu, HI, USA
6. Lee, B., Lee, J.-H.: Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. J. Supercomput. **73**(3), 1152–1167 (2016). https://doi.org/10.1007/s11227-016-1870-0
7. Conoscenti, M., Vetro, A., De Martin, J.C.: Peer to peer for privacy and decentralization in the internet of things. In: IEEE/ACM 39th International Conference on Software Engineering Companion, 20–28 May 2017, Buenos Aires, Argentina
8. Liang, X., Zhao, J., Shetty, D.: Towards data assurance and resilience in IoT using Blockchain. In: IEEE Military Communications Conference, 23–25 Oct 2017, Baltimore, MD, USA
9. Ray, S., Ghosh, S., Bhattacharjee, A., Biswas, R., Ghosh, P., Deyasi, A.: Implementation of semi-autonomous UAV for remote surveillance and emergency reconnaissance using convolutional neural network model. In: 2nd International Conference on Microelectronics, Communication System, Machine Learning & Internet of Things (2021)
10. Pinno, O.J.A., Grigio, A.R.A., De Bona, L.C.E.: Control chain: blockchain as a central enabler for access control authorizations in the IoT. In: IEEE Global Communications Conference, 4–8 Dec 2017, Singapore
11. Santra, S., Mukherjee, P., Deyasi, A.: Cost-effective voice-controlled real-time smart informative interface design with google assistance technology. In: Machine Learning Techniques and Analytics for Cloud Security, Chap. 4 (2022)
12. Nath, A., Roy, L., Shruti, S., Santra, S., Deyasi, A.: Efficient detection of bio-weapons for agricultural sector using narrowband transmitter and composite sensing architecture. In: Convergence of Deep Learning in Cyber-IoT Systems and Security (2022)
13. Liao, K.: Design of the Secure Smart Home System Based on the Blockchain and Cloud Service, Wireless Communications and Mobile Computing, vol. 2022, A. id: 4393314 (2022)
14. Sil, S., Daw, S., Deyasi, A.: Smart intelligent system design for accident prevention and theft protection of vehicle. In: Nath, V., Mandal, J.K. (eds.) Nanoelectronics, Circuits and Communication Systems. LNEE, vol. 692, pp. 523–530. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-7486-3_47
15. Santra, S., Deyasi, A.: prototype implementation of innovative braille translator for the visually impaired with hearing deficiency. In: Emerging Trends in IoT and Integration with Data Science, Cloud Computing and Big Data Analytics, pp. 272–290 (2022)
16. Das, D., Banerjee, S., Chatterjee, P., Biswas, M., Biswas, U., Alnumay, W.: Design and development of an intelligent transportation management system using blockchain and smart contracts. Clust. Comput. **25**, 1899–1913 (2022). https://doi.org/10.1007/s10586-022-03536-z

17. Hoksbergen, M., Chan, J., Peko, G., Sundaram, D.: Asymmetric information in high-value low-frequency transactions: mitigation in real estate using blockchain. In: Doss, R., Piramuthu, S., Zhou, W. (eds.) FNSS 2019. CCIS, vol. 1113, pp. 225–239. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34353-8_17
18. Qureshi, A., Jiménez, D.M.: Blockchain-based multimedia content protection: review and open challenges. Appl. Sci. **11**(1), 1–24 (2021)