International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 10, No. 3, November 2021, pp. 176~185
ISSN: 2089-4864, DOI: 10.11591/ijres.v10.i3.pp176-185

ACCESS - IoT enabled smart lock

Harshith Gadupu, Osa Mokharji, Raunak Kankaria, Shrey Kumar, Kayalvizhi Jayavel
Department of Information Technology, SRM Institute of Science and Technology, Kattankulathur, India

Article Info

Article history:

Received Mar 2, 2021
Revised Jun 22, 2021
Accepted Jul 27, 2021

Keywords:

Home automation
Internet of things
Lock system
Mobile application
Raspberry Pi
Smart door lock

ABSTRACT

ACCESS is a centrally controlled extensible security system - a system for enhancing accessibility and security methods. Security is an important matter of concern and everyone wants things easy and fast with the advancement of technology. Many IoT engineers are inclined towards home automation today. An area of recent interest is the automation of lock and key systems of homes and workplaces. This paper comprises mechanisms to view visitors of households, machinery, or any appliance that may be remotely controlled through a mobile application. Owners or supervisors can keep a watch on the guests and choose whom they want to grant entry to. This is conducted by providing the guests with temporary access permission for a validity period of the owner's choice. They can also simultaneously monitor the activities of the guests.

Corresponding Author:

Kayalvizhi Jayavel
Department of Information Technology, SRM Institute of Science and Technology
SRM Nagar, Kattankulathur, Chengalpattu District, Tamil Nadu -603203, India
Email: kayalvij@srmist.edu.in

1. INTRODUCTION

Applying automation to simple manual tasks is challenging and interesting. People access their households and workplaces frequently every day and there are many problems associated with security and accessibility. Sometimes people are away from their homes or workplace when a visitor arrives and they are not present to let them into the house unless they reach home. Elderly people may face difficulty in walking repeatedly to open doors. Also, when there is a security breach like a theft, it becomes difficult to trace the people who visited the property. Hence, people are in control of their property only when they are physically present near it and they lose this control once they are away from it.

In the proposed system "ACCESS", these manual methods are replaced by a mobile application. Users can lock or unlock their doors using this mobile application even when they are not present at home. If we imagine a scenario where a visitor suddenly arrives at the house, normally he would have to contact the owner, and the owner would not be able to help until he reached home. With the proposed solution, the visitor will only have to ring the doorbell and the system will detect the doorbell press and send a notification to the owner along with a photograph of the visitor. Surveillance cameras are used to see who is at the door users can view the visitors and also speak to them through the microphone-speaker provision. The owner can be away from home and still let the visitor in. All lock and unlock operations are logged and users can later check these locks to have a clear idea of who has accessed their property. This is helpful in case of security issues or crimes. On every doorbell press the visitor's photograph is sent to the owner an also stored. This gives a very clear view of all visitors even if they are unknown.

Every lock has a single primary owner and owners can choose to grant this control to any number of users for a time period of their choice and also revoke these access permissions at any time. They are also informed every time another person accesses their locks. It is also ensured that only owners can remotely

access their locks while guests can do it only when in proximity to the locks. The system also provides for accessing the locks manually through offline methods in the absence of an internet connection.

The paper addresses the problem statement of manual control of door locks and aims to replace them by a solution that allows remote control and access. There have been several related works in this field and different solutions are provided but in the research method of this paper there have been drawbacks found in these solutions. The aim of this paper is to provide a completely functioning smart door lock system which can also overcome all the drawbacks which the related works have.

2. RELATED WORKS

Radio-frequency identification (RFID) authentication has been used for access control, where the door is opened by recognizing the RFID tag [1], [2]. The methodology in [3] suggests the use of Zigbee tags, along with motion sensors to detect the presence of people in the vicinity of the door, while method [4] suggests the use of near field communication (NFC) has been attempted to increase accuracy of detection. The major drawback of all these systems is that they need the users to be physically present for operation, hence remote access in not possible. Also, RFID tags, Zigbee tags and NFC cards become additional piece of equipment which can be lost, damaged or forgotten by the user. Furthermore, there is no user interface for registering the devices and every tag, module and microcontroller needs to be hardcoded with access credentials, and this reduces the flexibility of the system. This is also subjected to several false requests because the system will identify the equipment even if it accidentally comes within range of the detector. Several concerns have been raising about NFC sniffing and eavesdropping, because of which NFC cannot be considered completely secure. In the proposed system, all equipment is eliminated and replaced by the mobile phone application. Since almost everyone has a mobile phone today, having a system dependent on phones is more feasible than introducing new equipment to be carried. The problem of not having remote access is also overcome, and the security aspects are all covered (as discussed in later sections).

Biometrics [5] such as fingerprint [6], [7] iris scanning and face recognition [8], [9] have been used to operate door locks. In these systems also remote access cannot be implemented and they need specific equipment that needs heavy maintenance. In methodology [10] we see the use of a Wi-Fi connection. All the house appliances and devices are attached to a Raspberry Pi and when the user's phone and Pi get connected on the same network, the user can control all the connected devices. This is a much more secure method but cannot allow remote access.

The blockchain method has been used for coordinating the interaction between nodes [11]. Blockchain is a method which allows a transaction when all participating entities acknowledge it. All participating devices are called nodes and once the user's phone has connected to one device (assuming a Raspberry Pi), it can communicate with any other connected device provided the transaction has been approved by a chosen number of participating nodes. This is, however, time-consuming and complex to an extent.

Web applications have also been used for lock functions, where the users have had to log into websites to access the control point for their locks [12]. This requires logging into the web application for every operation. There is no solution to a situation where the internet may be temporarily unavailable. Also, in most implementations, lack of organization of user interface may lead to inconvenience of use. ACCESS comprises a mobile application which does not require repeated logging in and makes notifications instant. Offline authentication mechanisms act as a backup for situations of lack of internet.

Some micro-controllers such as the Galileo board [13], Arduino, ESP, ATtiny13, PIC MC [14] have been used for the controlling of locks. However, their functionality is limited as compared to the Raspberry Pi [15]. Our system uses a Pi as a single complete control node which can serve multiple purposes at once. Some systems have used Websockets as the communication protocol to communicate between the user's mobile application and the lock device. Web sockets are connection-oriented and require the application to be connected to the lock persistently for the entire duration of the lock operations. The ACCESS system uses MQTT which is connectionless and connects as soon as the application is opened.

Doorbell detection and motion sensor detection have been used to notify the user when someone is at the door [1], [3]. This system uses microphones for audio reception along with cameras for photo capture of the visitor. It also includes the feature of sending notifications to the home residents through global system for mobile communications (GSM) module [16] or email [17]. The drawback of the system is that the owner may be informed about a visitor but has no means of taking an action to let the visitor in case the owner is not present at the residence. ACCESS contains a speaker in addition to the microphone so that the visitor may speak to the owner, exactly the way it happens when the owner is present in person. Also, the owner has the privilege to unlock the door from wherever he is at the current moment. GSM modules are slow in operational speed and require a separate dedicated SIM card connection with strong connectivity. This makes

them a slightly inconvenient choice for this kind of a system. Comparatively, emails are convenient but require separate paid services to be maintained. This increases the cost of implementation. Also, emails may not be checked regularly by users.

There are some systems which involve mobile application based access to door locks as in [18]. Some of these applications connect to the microcontroller via Bluetooth [19] or local area network (LAN) connections, indicating the inability to function remotely. Bluetooth is a two-way connection protocol which requires a method called pairing [20]. In this, both connecting parties must accept and enter the connection. In contrast to this, Bluetooth low energy (BLE) [21] requires lower power since it happens one way. The ACCESS system uses BLE since there is no pairing required, only a single way broadcast of data is sufficient followed by the receiving of this data from the other end. The mobile application of ACCESS requires an internet connection but this is not an additional requirement since all cellphone users today have internet access. All notifications and server communications take place with the help of the phone's internet connection itself.

3. PROPOSED METHOD

Figure 1 shows the electrical components controlled by a Raspberry Pi [22]. The components are described in the following section.

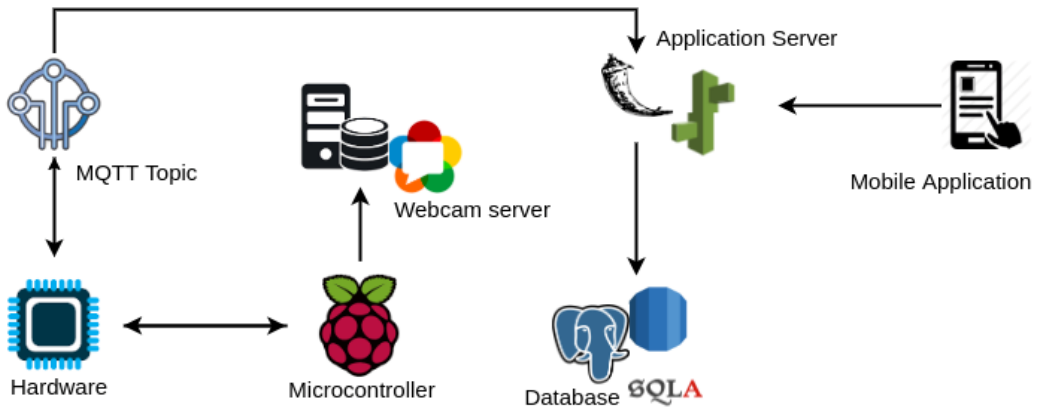


Figure 1. System architecture

3.1. Hardware and microcontroller

- Solenoid lock and relay - The solenoid lock represents household locks. It is controlled by a relay connected to the Pi. When the user gives a lock or unlock command to the Pi, the relay is switched to push up the head of the solenoid lock (to lock) or bring it down (to unlock).
- 4x4 matrix keypad and manual switch - When there is no internet connection, a 4x4 matrix keypad is used to enter a onetime password (OTP) which is generated by the Pi and sent to the owner's mobile application. If someone is inside their home, they can use a switch on the inside of the door to open it, instead of using the app.
- OLED display – This is used for displaying the status of the lock, the entered password or any message to the person standing at the door.
- Doorbell – When this is pressed, the Pi notifies the owners that a visitor has arrived along with a photograph of the visitor.
- Web camera and speaker - The web-camera streams the live video of the visitor to a public URL through the Raspberry Pi as shown in Figure 1. When the user speaks through his mobile application, the audio is streamed back to the Pi and then to the speaker.

3.2. Power supply

The Pi needs a power supply of 12V. This can be supplied through the USB or through the general-purpose input/output (GPIO) pins. The power can be drawn from a power bank, direct plug connection or

lithium-ion batteries. All other components have their power inputs connected to the pins of the Pi and can get their power supply from them. Only the solenoid lock used for demonstration requires a 12V power and cannot draw it from the Pi since the maximum output voltage of the Pi is 5V. For the solenoid lock too, we can use a power bank, direct plug or lithium-ion battery separate from the one used for the Pi. These can be connected to the solenoid lock through its positive and negative terminals.

3.3. Working of lock operations - HTTP and MQTT

Figure 2 explains the system workflow. The user's mobile application (front-end) is developed using a cross platform framework [23] so that it can run on any mobile operating system. The application functions by communicating with the application server (back-end) hosted on the cloud. Two protocols are used in this system - hypertext transfer protocol (HTTP) [24] and message queuing and telemetry (MQTT) [25]. HTTP functions through requests and responses. The user clicks the 'Lock' or 'Unlock' button from his mobile application and an HTTP request is sent to the application server. The server checks with the current lock status from the database to see if the operation is feasible. For example, a 'lock' request on the lock when it is already in 'locked' state will not be executed and the user's mobile application will be notified whether the operation is in progress or already performed.

Following this, MQTT is applied. MQTT involves publishers who send messages to topics and subscribers who await these messages, with a broker to communicate the arrival of these messages. If the requested lock operation can occur, the server publishes the string containing the lock ID and operation to the MQTT topic and the Pi (which is subscribed to the topic) receives this data. Now, the Pi checks if this operation is possible with the state of the lock which it has stored locally. If yes, then the lock is operated on and the lock state is updated. The Pi publishes the entire data to an MQTT topic which triggers a request to the server for updating the data of this operation into the database.

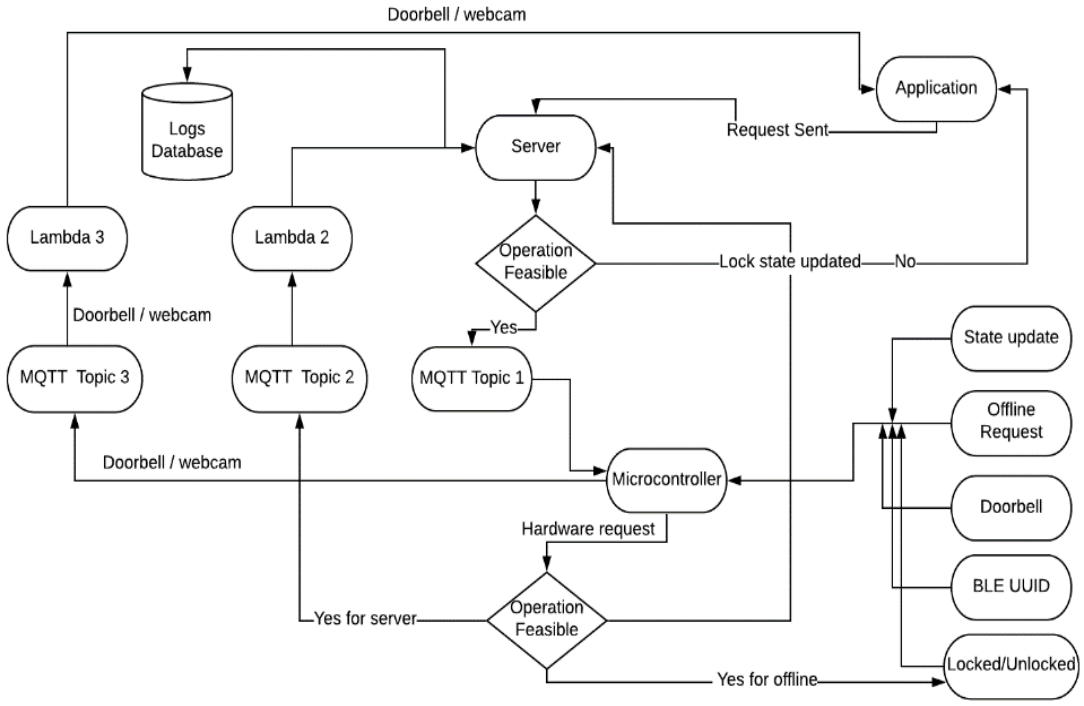


Figure 2. System workflow

3.4. Doorbell detection, web camera and talkback

When a visitor presses the doorbell, the system detects this and triggers a notification to the owner's mobile application. Simultaneously, the system takes snapshots of the visitor and stores them on the cloud for the owner to see. When the owner clicks the notification, he is taken to the screen from where he can switch on the camera to view the visitor live. The web camera captures the video of the visitor and the web camera's inbuilt microphone captures the audio. This web camera feed is streamed onto the local server of the Pi. Reverse secure shell tunneling (or SSH Tunneling) is used to make the webcam server available on a public

URL so that it can be seen on the mobile application. On the other hand, the audio from the owner (coming from the mobile application) is received and amplified by the speaker on the door. The server allows full duplex, two-way communication between the mobile application and the Raspberry Pi. Using this, the owner can see the visitor and talk to them like a video call.

3.5. User privileges

The mobile application is used for many features other than the basic lock operations. There can be three types of users in the system:

- Primary owners – These users have all privileges for a lock. They can perform lock and unlock operations when they are near their locks or even remotely. They can add new locks, edit or delete existing ones. They can also use the webcam and video calling features. They have the privilege to add secondary owners or guests for their locks and set the time for the expiry of the permissions.
- Secondary owners – Their permissions are the same as that of the primary owner but they cannot edit or delete locks. For example, in a family either spouse could be the primary owner while the other spouse and children could be the secondary owners. They can also create other secondary owner or guest users.
- Guests – They only have locking and unlocking permissions which can be performed only when they are in proximity of the locks. Hence, remote access is not allowed for them. They can use their privileges till the expiry time which the primary or secondary owners fix for their guest accounts.

3.5. Bluetooth low energy

Guests are allowed to access their locks only when they are present near the locks. BLE [25] is used to confirm that the user's mobile application is in proximity of the lock. Concepts of Bluetooth and BLE have been widely used for proximity sensing experiments as depicted in [26] through the use of beacons. In the proposed system, the Pi broadcasts a universally unique identifier (BLE UUID) which is scanned by the guest's mobile application when he tries to access the lock. The database is constantly updated with this UUID from the Pi. When the scanned UUID matches that on the database, access is granted. There are many publicly available mobile applications which can scan nearby BLE device UUIDs. Hence it is possible for any guest user to find out the Pi's UUID using such an app and then clone it to pretend to be near the lock when he is actually not. To prevent such spoofing and cloning, the Pi's UUID is changed and regenerated at regular intervals by running cron jobs on the Pi to prevent spoofing and cloning. A normal Bluetooth connection as used in [27] needs both devices to approve of the connection since it involves two-way pairing but in the proposed method BLE is used and it is more efficient for the requirement since the Pi sends out an ID and all nearby devices can capture the ID [28]. The only drawback of BLE is the possibility of cloning which has been solved by the system as well.

3.6. Offline access

There may be situations where the system needs to operate without internet, if the internet connection is lost. This offline system contains a keypad and OLED display to enable manual entry of pass-codes for lock access [29]. The passcode is generated as an OTP which is sent to the user's mobile application [30]. When the OTP is used, the Pi waits to come back online, and then the new OTP is generated and sent to the user for the next use. The Pi also stores a master code locally and this may be used instead of the OTP. The letter keys on the keypad are used for changing the master code, deleting characters or confirming the entered code string. There is also a switch on the inner side of the door which enables residents to access the door lock manually from inside.

3.7. Database

The database instance has been created on cloud and holds data in four tables. It is an Intel AVX, Intel Turbo instance with one single core CPU, 1GB of memory and low to moderate network performance. The tables are as follows:

a) Users - Details of all the users who have registered to the application. Primary owners, secondary owners and guests are all users on the application. The data stored in this table are:
   - Username (primary key), full name and phone number of the user.
   - Mobile application ID - of the user. When an app is installed, it generates a unique ID for itself and this is needed as an endpoint for sending notifications. If a user has signed in from multiple apps, then all the app IDs are stored.
b) Locks – This holds the details of the locks which each owner adds to his account. Each time he adds a new lock from his mobile application, it is added as a row in this table. The data held are:

- Lock ID (primary key), alias (a name given by the owner for easy identification), address (where the lock is located), username (of the owner who created the lock).
- Lock priority – The mobile application allows locks to be marked as a favourite so they can be placed at the top of the list of locks.
- BLE UID and media access control (MAC) address of the Pi.
- Current lock state – This is updated every time a lock operation is completed and helps in avoiding repetition of operations.

c) Access control logs (ACL) - All the secondary and guest users to whom access have been granted. It stores the username, lock ID for which access is given, expiry timestamp of permissions, and user type (guest or secondary).
d) Logs – Regular log details of every action that takes place on every lock in the system. This stores the operated lock's lock ID, operating user's username, timestamp of operation, type of operation (lock or unlock), user type (owner, guest or secondary).

3.9. Logging and filtering data

The mobile application allows the logs (or history of lock operations) to be viewed by owners and secondary owners. Filtering can be based on the operation type (user can choose to view only locks or only unlocks or both), username of the operating user (to view all the operations done by a user or a selected number of users), user type (to view operations done by only secondary owners or only guests), lock ID (to view operations only for a particular lock). They can also specify a start and end time to view the operations only between particular dates or times. These filters give the users an easy way to quickly view past data and is very helpful in case a security issue has to be investigated.

3.10. Authentication and security

The users are authenticated using a cloud authentication service. Each user can only see their own details via the application and hence their details are not accessible by any other user. The database is only accessible by systems on the same network. Hence only the backend server can access it. The database is only accessible by authenticated users and by providing required credentials and passwords. All these measures are taken to secure data and prevent third party access or hacking.

As mentioned in [31], IoT involves a huge amount of data and in every IoT project it is most important to maintain system security. Among security attacks, unauthorized use is very common and the proposed system prevents the possibility of it.

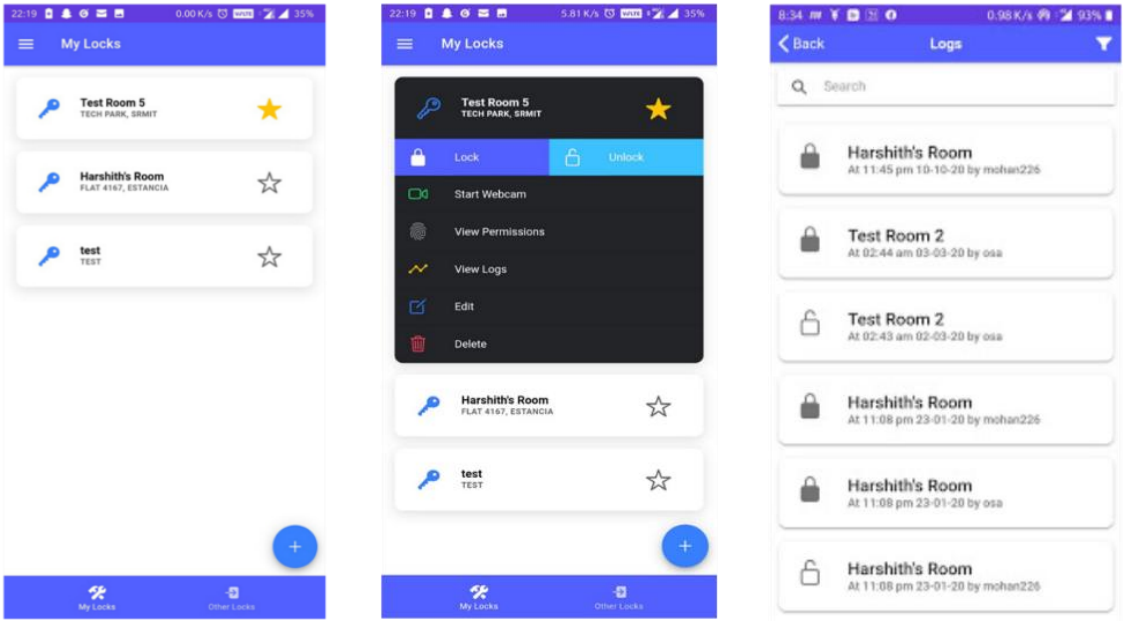
4. RESULTS AND DISCUSSION

Mobile applications are used in many experiments for smart door locks as in [32], [33] and it is very important to have a good user interface. The proposed system's mobile application is developed in a cross-platform framework so that it can run on all mobile operating systems. The mobile application is successfully developed and deployed, and is completely functional. Figure 3 shows the screens of User's locks (a), Lock operations and webcam options (b) and Logs (c).

Response time experiments: For different parts of the system, experiments were carried out to approximate the time taken (in seconds) for the flow of events to occur. 60 experiments were conducted for three scenarios and Table 1 holds an analysis of the studies.

Experimental conditions: The server is hosted on the cloud, with an instance of Intel AVX (Intel Turbo), with 1 GiB memory and single virtual central processing unit. The network performance of the instance is low to moderate and steady internet connection of 70 to100 Mbps was chosen. Table 1 is made by calculating the average values of all the experiments for every scenario.

Experiments show that the operation which takes maximum time is when a guest user performs a lock/unlock and the user's phone BLE UUID is scanned. Table 2 shows an analysis of the possible reasons for failure in the experiments.



(a) (b) (c)

Figure 3. ACCESS mobile application: (a) User's locks, (b) Lock operations and webcam options, (c) Logs

Table 1. Response time analysis

Start	Sequence	Operation	Operation time	Time taken	Total Time
(1) Scenario: Doorbell detection and video communication					
Visitor presses doorbell (0:00 hrs)	1 (a)	Pi detects	0:00.01 hrs	0.01 s	
	1 (b)	Visitor's snapshot taken	0:00.02 hrs	1.01s (from 1a)	
		Snapshot uploaded to cloud	0:01.02 hrs		
	1 (b)	Pi publishes data to MQTT topic	0:01.10 hrs	1.09 s (from 1a)	1.30s
	1 (c)	Request from topic to server	0:01.11 hrs	0.01 s (from 1b)	
	1 (d)	Notification on mobile application	0:01.20 hrs	0.09 s	
	1 (e)	User opens application	0:01.20 hrs	Almost instantly	
	1 (f)	User clicks "Start Webcam" option	0:01.20 hrs	Almost instantly	
	1 (g)	Webcam streaming page opens	0:01.24 hrs	0.04 s	
	1 (g)	Webcam is switched on	0:01.26 hrs	0.02 s	
	1 (h)	Webcam stream is visible on app	0:01.30 hrs	0.06 s	
	1 (i)	User's audio reaches door speaker	0:01.30 hrs	Almost instantly	
(2) Scenario: Lock/ Unlock operations					
User clicks 'Lock'/ 'Unlock' (0:00 hrs)	1 (a)	Server receives request	0:00.04 hrs	0.04 s	
	1 (b)	Server checks lock state from database	0:00.06 hrs	0.02 s	1.25s
	1 (c)	Server publishes data to MQTT topic	0:00.12 hrs	0.06 s	
	1 (d)	Pi receives the data	0:00.14 hrs	0.02 s	
	1 (e)	Pi switches relay	0:00.15 hrs	0.01 s	
	1 (f)	Solenoid lock goes into lock state	0:01.25 hrs	1.10 s	
(3) Scenario: BLE scan – User's phone is present in vicinity of Pi					
Guest user clicks 'Lock'/ 'Unlock' (0:00 hrs)	1 (a)	Server receives request	0:00.02 hrs	0.02 s	
	1 (b)	Server checks lock state from database	0:00.06 hrs	0.04 s	
	1 (c)	Server publishes data to MQTT topic	0:00.09 hrs	0.03 s	
	1 (d)	Pi receives the data	0:00.10 hrs	0.01 s	2.27s
	1 (e)	Pi initiates BLE scan	0:00.11 hrs	0.01 s	
	1 (f)	User's phone's BLE is found in scan	0.01.21 hrs	1.10 s	
	1 (g)	Pi switches relay	0:01.24 hrs	0.03 s	
	1 (h)	Solenoid lock goes into lock state	0:02.27 hrs	1.03 s	
(4) Scenario: BLE scan – User's phone NOT present in vicinity of Pi					
Guest user clicks 'Lock'/ 'Unlock (0:00 hrs)	1 (a)	Server receives request	0:00.01 hrs	0.01 s	
	1 (b)	Server checks lock state from database	0:00.03 hrs	0.02 s	
	1 (c)	Server publishes data to MQTT topic	0:00.05 hrs	0.02 s	1.14s
	1 (d)	Pi receives the data	0:00.08 hrs	0.03 s	
	1 (e)	Pi initiates BLE scan	0:00.10 hrs	0.02 s	
	1 (f)	User's phone's BLE NOT found	0.01.14 hrs	1.04 s	
	1 (g)	Further operations aborted	-	-	

Table 2. Failure scenarios and reasons

Operation	Outcome	Reason
Pi publishes data to MQTT topic	Data not published	Loss of internet connection
Notification on mobile application	Notification not received	Cloud messaging service down
Webcam streaming page opens	Webcam page loads partial data	Poor internet connection
Two-way audio/ video streaming	Lag in audio/video streaming	Slow server processing
Solenoid lock goes into lock state	Lock does not move up	Insufficient power supply to the lock
BLE scan	Pi does not find user's phone BLE UUID	Bluetooth not switched on in user's phone

In the works of [34], the database has been based on NoSQL where data is stored as key value pairs. The proposed system used PostgreSQL which provides SQL relational table structure in which fields can be dictionaries or arrays and hence we cans tore multi-valued data and also key-value pair data. As compared to the results of [34], the proposed system produces faster database results since reading time is optimized due to efficient database structure.

The results show a direct relation between the performance speed and stability of internet connection. On average, every functional module is completed between 1 to 2 seconds. Most reasons of failure are related to internet connectivity which is one dependency of the system to function in online mode. This is also the reason why the offline mechanisms have been included to make sure the system is not dependent on internet for its basic requirement. This also means that the cloud service and tier of service should be chosen very carefully to make sure the server's networking and processing capacities are enough to support smooth functioning. The database also needs to be well chosen because spend of read and write operations depend largely on the database server processing.

Hence, the proposed system is a step towards developing a smart home since IoT is being widely used for smart systems [35], [36]. This project can be improved by the addition of some features. The doorbell detection can be integrated with the doorbell of the house in place of the additional switch. Further, the hardware components can be scaled down to smaller sizes to enhance compactness. A well-designed PCB will make the appearance even better. The application can be made more secure with facial recognition which is the base of the experiment in [37], [38]. There can also be an additional notification process via SMS to ensure the owner is notified even if his internet is not turned on [39]. An interesting addition would be a gesture recognition system for offline access as depicted in [40] through virtual reality methods where lock opening hand gestures can control the locks.

5. CONCLUSION

The project can be deployed in households, educational institutions and workplaces where people are searching for methods to add speed and convenience to their lifestyles. Any region put under lock and key can use this system. IoT has been used for monitoring sensors and smart homes as depicted in works. The vastest application of the proposed system is that of households since the doors are accessed multiple times on a regular basis and the problem of being away from home when visitors arrive is rather common. Apart from this, machinery, storage cupboards and rooms, and appliances can also be controlled by the same. In the case of a door it is a lock, and in the case of computer systems of machinery it is the power supply. Especially for elderly citizens, a more secure way of monitoring entries and exits to and from the house will prove to be beneficial for their safety. As explained in the paper, the proposed system aims at overcoming the drawbacks of existing system and also aims at making improvements by implementing some new approaches suggested by some of the related works.

REFERENCES

[1] Y. T. Park, P. Sthapit and J. Pyun, "Smart digital door lock for the home automation," *TENCON 2009 - 2009 IEEE Region 10 Conference*, 2009, pp. 1-6, doi: 10.1109/TENCON.2009.5396038.

[2] G. K. Verma and P. Tripathi, "A digital security system with door lock system using RFID technology," *International Journal of Computer Applications*, vol. 5, no. 11, pp. 6–8, 2010, doi: 10.5120/957-1334.

[3] K. Gill, S. -H. Yang, F. Yao and X. Lu, "A zigbee-based home automation system," *in IEEE Transactions on Consumer Electronics*, vol. 55, no. 2, pp. 422-430, May 2009, doi: 10.1109/TCE.2009.5174403.

[4] C. Hung, Y. Bai and J. Ren, "Design and implementation of a door lock control based on a near field communication of a smartphone," *2015 IEEE International Conference on Consumer Electronics - Taiwan*, 2015, pp. 45-46, doi: 10.1109/ICCE-TW.2015.7216992.

[5] M. A. Kader, M. Y. Haider, M. R. Karim, M. S. Islam and M. M. Uddin, "Design and implementation of a digital calling bell with door lock security system using fingerprint.," *2016 International Conference on Innovations in Science, Engineering and Technology (ICISET)*, 2016, pp. 1-5, doi: 10.1109/ICISET.2016.7856484.

[6] N. A Anu, and D. Bhatia, "A smart door access system using fingerprint biometric system," *International Journal of Medical Engineering and Informatics*, vol. 6, no. 3, pp. 274-280, 2014, doi: 10.1504/IJMEI.2014.063175.
[7] J. Chaikin and S. Kenter, "Biometric lock", *Legal Patent, United States, US12/339, 176*, 2008.
[8] A. B. Thabet and N. B. Amor, "Enhanced smart doorbell system based on face recognition," *2015 16th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, 2015, pp. 373-377, doi: 10.1109/STA.2015.7505106.
[9] M. Sahani, C. Nanda, A. K. Sahu and B. Pattnaik, "Web-based online embedded door access control and home security system based on face recognition," *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, 2015, pp. 1-6, doi: 10.1109/ICCPCT.2015.7159473.
[10] A. Kassem, S. E. Murr, G. Jamous, E. Saad and M. Geagea, "A smart lock system using Wi-Fi security," *2016 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)*, 2016, pp. 222-225, doi: 10.1109/ACTEA.2016.7560143.
[11] D. Han, H. Kim and J. Jang, "Blockchain based smart door lock system," *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, 2017, pp. 1165-1167, doi: 10.1109/ICTC.2017.8190886.
[12] C. Vongchumyen *et al.*, "Door lock system via web application," *2017 International Electrical Engineering Congress (iEECON)*, 2017, pp. 1-4, doi: 10.1109/IEECON.2017.8075909.
[13] M. Presso, D. Scafati, J. Marone and E. Todorovich, "Design of a smart lock on the Galileo board," *2017 Eight Argentine Symposium and Conference on Embedded Systems (CASE)*, 2017, pp. 1-6, doi: 10.23919/SASE-CASE.2017.8115378.
[14] R. Satoskar and A. Mishra, "Smart door lock and lighting system using internet of things," *International Journal of Computer Science and Information Technology*, vol. 9, no. 5, pp. 132-135, 2018.
[15] V. Vujović and M. Maksimović, "Raspberry Pi as a sensor web node for home automation" *Computers and Electrical Engineering*, vol. 44, pp. 153-171, 2015, doi: 10.1016/j.compeleceng.2015.01.019.
[16] A. Ibrahim, A. Paravath, P. K. Aswin, S. M. Iqbal and S. U. Abdulla, "GSM based digital door lock security system," *2015 International Conference on Power, Instrumentation, Control and Computing (PICC)*, 2015, pp. 1-6, doi: 10.1109/PICC.2015.7455796.
[17] S. Jain, A. Vaibhav and L. Goyal, "Raspberry Pi based interactive home automation system through E-mail," 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), 2014, pp. 277-280, doi: 10.1109/ICROIT.2014.6798330.
[18] A. David O., M. Chinaza and O. Jotham O., "Design and implementation of a door locking system using android app," *International Journal of Scientific & Technology Research*, vol. 6, no. 8, pp. 198-203, 2017.
[19] J. Dabhade, A. Javare, T. Ghayal, A. Shelar, and A. Gupta, "Smart door lock system: improving home security using Bluetooth technology," *International Journal of Computer Applications*, vol. 160, no. 8, pp. 19-22, 2017
[20] L. K. Bhute, G. Singh, A. Singh, and V. Kansary, "Automatic door locking system using Bluetooth module", *International Journal for Research in Applied Science and Engineering Technology*, vol. 5, no. 5, pp. 1128-1132, 2017
[21] M. A. Prada-Delgado, A. Vázquez-Reyes and I. Baturone, "Physical unclonable keys for smart lock systems using Bluetooth Low Energy," *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, 2016, pp. 4808-4813, doi: 10.1109/IECON.2016.7792955.
[22] V. Vujović and M. Maksimović, "Raspberry Pi as a wireless sensor node: Performances and constraints," *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2014, pp. 1013-1018, doi: 10.1109/MIPRO.2014.6859717.
[23] S. Charkaoui, Z. Adraoui and E. H. Benlahmar, "Cross-platform mobile development approaches," *2014 Third IEEE International Colloquium in Information Science and Technology (CIST)*, 2014, pp. 188-191, doi: 10.1109/CIST.2014.7016616.
[24] A. Jestratjew and A. Kwiecien, "Performance of HTTP protocol in networked control systems," in *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 271-276, Feb. 2013, doi: 10.1109/TII.2012.2183138.
[25] U. Hunkeler, H. L. Truong and A. Stanford-Clark, "MQTT-S — A publish/subscribe protocol for wireless sensor networks," *2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08)*, 2008, pp. 791-798, doi: 10.1109/COMSWA.2008.4554519.
[26] B. K. Clark, E. A. Winkler, C. L. Brakenridge, S. G. Trost and G. N. Heal, "Using Bluetooth proximity sensing to determine where office workers spend time at work," *PLOS One*, vol. 13, no. 3, p. e0193971, 2018, doi: 10.1371/journal.pone.0193971.
[27] S. Kavde, R. Kavde, S. Bodare and G. Bhagat, "Smart digital door lock system using Bluetooth technology," *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, 2017, pp. 1-4, doi: 10.1109/ICICES.2017.8070788.
[28] D. C. Aluri, "Smart lock systems: An overview," *International Journal of Computer Applications*, vol. 177, no. 37, pp. 40-43, 2020, doi: 10.5120/ijca2020919882.
[29] H. Alnabhi, Y. Al-Naamani, M. Al-Madhehagi and M. Alhamzi, "Enhanced security methods of door locking based fingerprint," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9, no. 3, pp. 1173-1178, 2020, doi: 10.35940/ijitee.B7855.019320.
[30] V. Pandit, P. Majgaonkar, P. Meher, S. Sapaliga and S. Bojewar, "Intelligent security lock," *2017 International Conference on Trends in Electronics and Informatics (ICEI)*, 2017, pp. 713-716, doi: 10.1109/ICOEI.2017.8300795.

[31] K. Djupsjö and M. Almosawi, "IoT security applied on a smart door lock application," Unpublished M. Sc Thesis, KTH, tockholm, 2018.

[32] K Karimi, M Kabrane, O Hassan, A Badouch and S Krit, "Secure smart door lock system based on Arduino and smartphone app," *Journal of Advanced Research in Dynamical & Control Systems*, vol. 12, no. 1-Special Issue, 2020, doi: 10.5373/JARDCS/V12SP1/20201088.

[33] M. P. Shinde, S. Mehta, I. Shanbhag, V. Lele and A. Bhise, "Android based smart door locking system," *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 1, pp. 329-331, 2020.

[34] K. A. Patil, N. Vittalkar, P. Hiremath and M. A. Murthy, "Smart door locking system using IoT," *International Research Journal of Engineering and Technology (IRJET)*, vol. 7, no. 5, pp. 3090-3094, 2020.

[35] T. S. Gunawan, I. R. H. Yaldi, M. Kartiwi, and H. Mansor, "Performance evaluation of smart home system using internet of things," *International Journal of Electrical and Computer Engineering*, vol. 8, no. 1, pp. 400-411, 2018, doi: 10.11591/ijece.v8i1.pp400-411.

[36] H. H. Qasim, A. E. Hamza, H. H. Ibrahim, H. A. Saeed, and M. I. Hamzah, "Design and implementation home security system and monitoring by using wireless sensor networks WSN/internet of things IoT," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 3, pp.2617-2624, 2020, doi: ijece.v10i3.pp2617-2624.

[37] K. Sri Viraja, K. Bharath Kumar, C. Keerthi, and G. Sandeep, "IoT based smart door system," *International Journal for Research in Applied Science and Engineering Technology*, vol. 6, no. 6, pp. 438-443. 2018, doi: 10.22214/ijraset.2018.4077.

[38] A. D. Dwivedi, H. Gupta, S. Tomar and D. Jaiswal, "Android based flat security system - the digital unlocking and locking system based on android for smart phone," *International Journal of Engineering Applied Sciences and Technology*, vol. 5, no. 5, pp. 192-196, 2020, doi: 10.33564/IJEAST.2020.v05i02.028.

[39] M. Shanthini, G. Vidya and R. Arun, "IoT enhanced smart door locking system," *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2020, pp. 92-96, doi: 10.1109/ICSSIT48917.2020.9214288.

[40] Y. Yu, "A practical digital door lock for smart home," *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, pp. 1-2, doi: 10.1109/ICCE.2018.8326305.