A Dual Authenticated Safety Vault for Cryopreservation Center

Arthi. R[a], Manoj Kumar D[b], C.B.Vasu[c], Aashiq Asan. R[d], and Sohil Pradeep[e]

[a,b,c,d,e] Department of ECE, SRM Institute of Science and Technology, Ramapuram Campus, Chennai.

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: In the most rapidly developing century , one critical issue that has been confronted was in providing security to the houses, offices and vaults. Though the physical surveillance such as CCTV cameras at the areas required has been used , they are only useful for the further investigation of any kinds of burglary and theft. Many security code or combination lock systems are also used are mostly hackable and decodable and hence it always needs to be improved and novel techniques are to be introduced to improve security. This paper therefore proposes a dual authenticated digital code lock system wherein the digital code is of total the 8 digits in which 4 digits of the code are user-defined and the remaining 4 are server generated digits and changes for every individual entry[commonly known as OTP(One Time Password)]. The important and the most reliable part of the proposed digital code lock system is the positions of the user-defined and server generated digits is also user-defined, which makes cracking or hacking the code more complex and also time consuming. The proposed dual authenticated safety vault has its applications in the area of safe guarding cryopreserving centre, medical documents, bank safety locker, residential homes and hotels.

Keywords: Safety Vault, Digital Code, One Time Password, Authentication, Surveillance

1. Introduction

The security code lock systems has been used very commonly at the banks as safety vaults and even in residential places such as houses and hotels to provide safety to the valuables and money and meanwhile most commonly heard news in the cases of robbery was breaking of the security code lock systems. The existing security code lock systems are of both the analog and digital types and has been used in accordance to the comfort and the user convenience . The analog lock systems uses the combination code lock or the lock and the key system. The digital code lock systems are the ones with the digital numbering code lock systems.The analog combination code lock system can be broken by knowing the combinations and the lock and key system can be broken by misusing the key. The digital security lockers can also be broken by hacking or cracking the code.

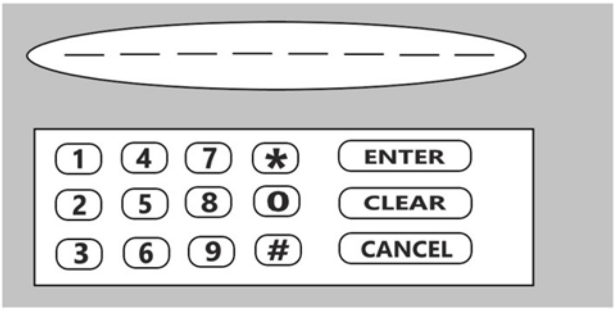


Fig.1. The 8-digit code security system

The proposed work suggests a dual authenticated digital security code lock system with bi-level authentication that will be simple for a user and complex for a robber to crack it. Think of a robber who comes to crack a security lock system and even succeeds in cracking the system of the locker but finds only a 4 digit code of the total 8 digit code . Also the robber finds that the remaining 4 digits are server generated and also succeeds to find the 4 auto-generated digits but still fails in cracking the security locker as the robber doesn't know the positional alignment of the fixed i.e; the user defined digits and the server generated digits.

The introduction to the proposed system is given in this section. The Section 2 explains the related works done achieve the fruitful results of the system. The Section 3 deals with the methodology i.e., it illustrates the techniques,procedure and explains the work flow of dual authentication, algorithm used in the system. The results are shown and has been analysed in the Section 4. The Section 5 concludes the proposed work and the future enhancement of the system has also explained.

2. Related Work

The author has dealt in [1] with the security lockers in which the PIN has been used in the initial stage and the next step would be the facial recognition whose positive results would generate one time password(OTP) which is authenticated and gives access to the respective locker. In [2] RFID and conventional Password method has been suggested and is a dual step process wherein the first step authentication takes place using RFID and the second step authentication has been done using password. In [3] the author has worked on the authentication of the security locker using the voice recognition as every human in this huge universe has a unique vocal. The second level of authentication deals with conventional password again. [4] is a very interesting paper where an electronic security lock system has been proposed in which the password has been used for authentication but the password can be entered from a particular bluetooth enabled smart-phone, this paper also includes capturing the image of the user. In [5], the multi-layer bank security system has been described in which the stages include the biometric and iris authentication that gives access to the locker room and also an RFID has been used to authenticate the authorized person . The most reliable part of this system was that a passive infrared sensor has been placed in the locker room which would inform the security officials in case of any unauthorized motion.

The author has suggested in [6] that it has again a two level authentication where the first level includes the biometric authentication and the second level authentication has a password of two parts i.e, one is of the bank manager and the other would obviously be of the consumer of that bank’s service. The [7] illustrates an anti-theft security system that consists of an LDR based sensor that acts as an electronic eye to detect the attempts of theft or any unauthorized usage. The [8] comprises a simple home automation and security management technique where the unauthorized usages would be informed to the local security and the owners of the particular property. The main feature of [9] was the system would maintain a track of date, time and the number of time the locker has been accessed. This system also has a limit of the number of permissible access per day. Though the references has suggested an insight about bank safety locker system, made us to make an attempt for dual authentication safety vault for Cryopreservation Center.

The author has explained a novel idea [10] in enhancing the bank security system using Visual Cryptography(VC). The most inspiring part is there is no pixel expansion in the reconstructed image and reconstruction is done without any code book. A door locking security system using GSM [11] is a simple security system installed in the door for the authentication. Here the GSM module works as both transmitting and receiving module. This is considered to be an easiest way for authenticating the authorized persons. The smart door lock system using the Internet-of-Things (IoT) [12] uniquely uses Infrared(IR) optical wireless signal(OWS) using IR light emitting diode(LED) of smartphones. Security being a keen issue to be looked in, many multi-layer authentication methods are also introduced one such kind is [13] wherein the RFID and GSM technology is used as a dual level authentication in the bank locker systems. Though it is a dual level security system it felt to be unsafe as both the RFID and GSM technologies are easily breakable. The advancements in the dual level security systems are taking place rapidly and many systems like [14] are introduced where the biometric and GSM technologies are used. Along with advancement of the security systems the cracking techniques also got advanced and the GSM technology is easily hackable and with many clowning techniques the biometric technology is also easily cracked. Eventually many security systems with facial recognition were also introduced.

In [15], the author has introduced an innovative way of generating an invariant private key based on the iris security authentication system. The security system [16] not only with the authentication but also the surveillance system which would help us recognizing the person who tried to break the system. But the surveillance system according to many ought to be unique and separate as hacker would not find the chance to hack it in a one single shot. If the security and the surveillance systems are independent of each other then it would be hard and time consuming for the hacker. A biometric authentication introduces if someone tries to break the system [17] then a security alert will be sent to the owner. Hence this also includes both authentication process and sending the security alerts to incase of any breakage of the system. A similar methodology in [18] wherein facial recognition uses the embedded system to design and the image of the user has been compared with the image in the memory and access is given if it matches. Although it is a tough task to build a security system using embedded system breaching the facial recognition is being so easy these days as previously mentioned. [19] elaborates the Bluetooth based home automation and security system. In this methodology, a communication system has been established between the home appliances and the owner for the easy access and also avoid the unauthorized of his/her house. This is done using the ARM7 and ARM9 boards. [20][22] also explains a 2-level security authentication. It includes the iris authentication and biometric authentication; the iris authentication is a reliable way. The iris authentication being the most reliable way is claimed to be unsafe as the hackers have reached their perks by hacking it too. [21] describes a security system for detection of theft with the help of photosensitivity concept and also using GSM technology. In this system LDR(Light Dependent Resistor) is also used as an electronic eye for detecting theft or its attempt. The GSM technology here is used only for signaling procedure to send the alerts to the respective officials. From all the above works we can conclude that any security system can be breached and so any novel, ingenious security system introduced is appreciated.

3. Methodology

Increasing safety for medical documents, pathological lab, cryopreservation center, households, valuables in the security lockers, banks has been the main motive of the proposed system. The proposed system as shown in Figure 1. has a two-step authentication process that confirms the user as an authorized person by executing the first step authentication process by sending the notification to the registered mobile number of the owner. If the owner approves then the system would be moving on to the next step else the local policemen, security officials and the owner will be informed that unauthorized usage has been taken place by cautioning and alerting everyone.

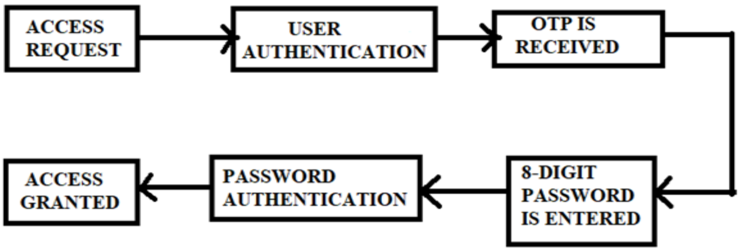


Fig.2. Architecture of the system

In the second step a 4-digit OTP has been sent to the registered mobile number of the owner. The higher-level security to the system has been provided in this respective step because the OTP generated uses the proposed algorithm that makes it difficult for unauthorized users to crack the code. The OTP generated changes for every individual entry has been sent only to the registered owner's mobile and confidentiality has been maintained there by denying the unauthorized user. The user also has to maintain a 4-digit fixed code. Hence the user would have a 4-digit OTP and a 4-digit fixed i.e., user-defined code. The user has also provided with an option to change the positions of the user-defined 4-digit code and the OTP. For instance, the user can fix the positions such that 1,3,5,7 digits of the 8-digit code should possess the user-defined i.e., the fixed code and 2,4,6,8 digits should possess the OTP that is received in the registered owner's mobile.

3.1 Dual Authentication for Safety Vault

The proposed dual authentication's first and the foremost job of the owner would be to setup a 4-digit user-defined code and also to define the positions of the OTP and user defined digits. After this, the 2-step authentication process has to take place whenever access to the system has been requested. From the previous section, the first step of authentication was clear and in the very next step two processes take place simultaneously if the owner approves the user as an authorized one. The user would be asked to enter the 8-digit code combination soon after OTP gets generated. When the user enters the 8-digits combination code according to the positions defined, then the system decodes the given code and compares them individually with the predefined code thereby generating OTP. When the codes match, then access has been given to the user else declined as shown in Figure 3.

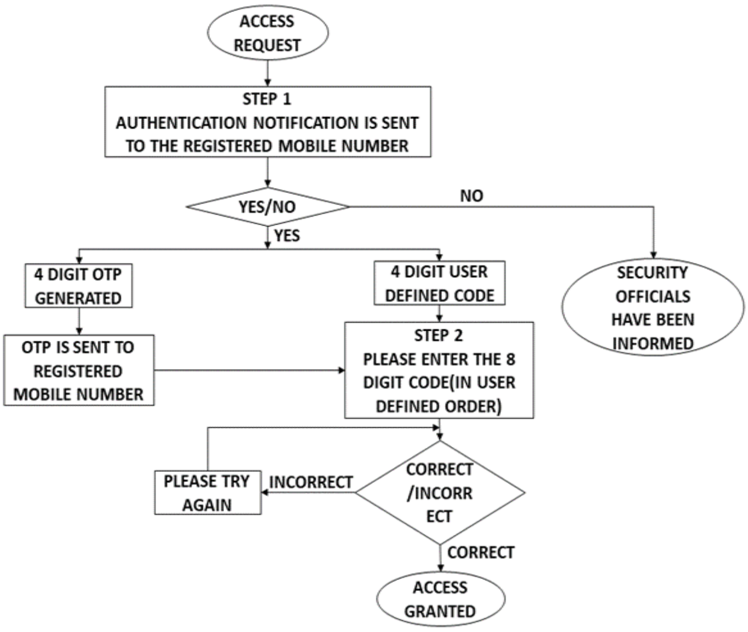

ACCESS REQUEST
STEP 1
AUTHENTICATION NOTIFICATION IS SENT TO THE REGISTERED MOBILE NUMBER
YES/NO
NO
YES
SECURITY OFFICIALS HAVE BEEN INFORMED
4 DIGIT OTP GENERATED
4 DIGIT USER DEFINED CODE
OTP IS SENT TO REGISTERED MOBILE NUMBER
STEP 2
PLEASE ENTER THE 8 DIGIT CODE(IN USER DEFINED ORDER)
PLEASE TRY AGAIN
INCORRECT
CORRECT /INCORR ECT
CORRECT
ACCESS GRANTED

Fig.3. Flow of Dual Authentication

3.2 Dual Authentication Algorithm

The proposed algorithm suggests a pseudo code in two phases such as Authenticity Verification as phase 1 and OTP generation as phase 2.

Phase 1: Pseudo code for Authenticity Verification

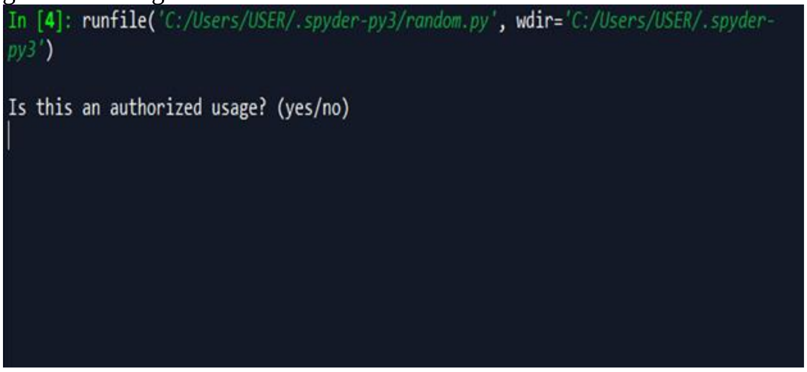
```
1.  Check for authorized usage.
2.  Break if not an authorized usage.
3.  Read the file that contains the user-defined code.
4.  Read the file that contains the positions of the digits of the user-defined code and the OTP.
5.  Initialize an array that contains 8-digits.
6.  Call the OTP function, store it in a variable .
7.  Generate the 8-digit code and store it in the initialized variable.
8.  Get the code from the user.
9.  If the generated code = entered code
            print Access Granted!
      else
            print  Sorry!Please try again.
10. End.
```

Phase 2: Pseudo Code for OTP Generation

```
1.  Read the previous OTP.
2.  Read the secret code.
3.  Set n= previous OTP-secret code.
4.  Set n=n X n.
5.  Left pad "n" with zeroes to get 8 digits.
6.  Set OTP=middle most four digits of "n".
7.  If the next number is less than 1000.
          Next number= next number + 1000
      Else
            Next number= next number
8.  Write the new OTP in the file.
9.  Return new OTP.
10. End.
```

4 Results and Discussion

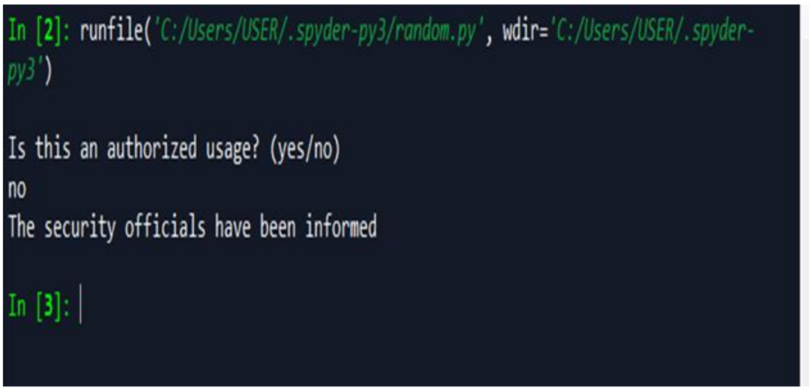
As discussed previously, the initial interface to user would get an individual wish to access the security lock system as shown in the Figure.3, the owner would get a notification in his/her registered mobile number if the usage that is being done is an authorized one or not.



```
In [4]: runfile('C:/Users/USER/.spyder-py3/random.py', wdir='C:/Users/USER/.spyder-
py3')

Is this an authorized usage? (yes/no)
```

Fig.3. Snapshot of initial notification

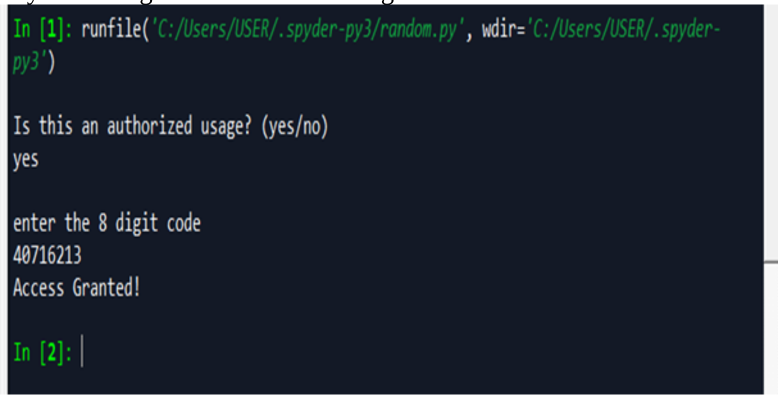
If the owner approves the notification then the system would lead to the next level else the text message would be sent to the local police or security official that someone was trying to crack the security lock system as shown in Figure 4.



```
In [2]: runfile('C:/Users/USER/.spyder-py3/random.py', wdir='C:/Users/USER/.spyder-
py3')

Is this an authorized usage? (yes/no)
no
The security officials have been informed

In [3]: |
```

Fig.4. Snapshot of Notification to Security Official

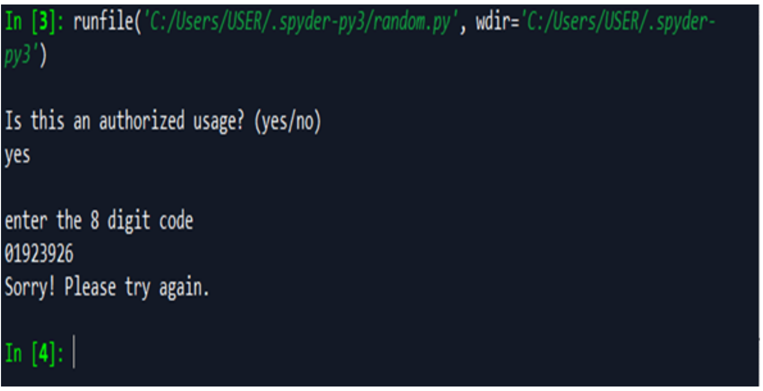
In the next level, the user would be asked to enter the 8-digit code that has a combination of the user defined code and the OTP(one time password) received with the registered mobile number of the owner. If the combination code entered in the 8 positions of the code has been entered accurately then access to the security lock system has granted as shown in Figure 5.



```
In [1]: runfile('C:/Users/USER/.spyder-py3/random.py', wdir='C:/Users/USER/.spyder-
py3')

Is this an authorized usage? (yes/no)
yes

enter the 8 digit code
40716213
Access Granted!

In [2]: |
```

Fig.5. Snapshot of Access Granted after dual authentication

As mentioned previously, higher chances were there to prevent cracking the security lock system at this particular stage. Any malicious user or unauthorized personcomes to know the user-defined password and the OTP, the user would not be able to access the system as he/she would have lack of knowledge regarding the positions of the combination code as the positions of the user-defined code and the OTP was also user-defined. If the user fails to give the correct combination code then he would not be givenaccess to the system as shown in Figure.6.



```
In [3]: runfile('C:/Users/USER/.spyder-py3/random.py', wdir='C:/Users/USER/.spyder-
py3')

Is this an authorized usage? (yes/no)
yes

enter the 8 digit code
01923926
Sorry! Please try again.

In [4]: |
```

Fig.6. Snapshot of Unauthorized user

5 Conclusion and Future Work

The proposed work designs a framework for dual authentication for safety vault with latest technology. While considering the security measures of the assets placed inside the safe against the hacking techniques by unauthorized users can be prevented and protected by this framework. The electronic safe system has a bi-level authentication mechanism. In the existing systems, the security code has either user-defined or server-generated but not its combination. This makes the proposed digital code security system more secure and non-penetrable.

In the near future, a many more number of security levels can be added while the system gets upgraded. Few such considerations can have the ability of providing a strong firewall that cannot be penetrated by malicious operators and users. An end to end encryption for the server generated code, i.e., OTP, that makes the code accessible by the owner alone. Usage of VPN server also cannot be easily used by any unauthorized person. By introducing an independent device, instead of a mobile phone that was only connected to the server so that the code can be cracked or hacked so easily. By introducing the virtual keypad in the same device so that access can also be limited to the owner. Secure system ought to be upgraded with time as they are one of the key security providers in this modern era and also promise to keep up our safety, authenticity, confidentiality and security.

References

1. Anusha, N., A. Darshan Sai, and B. Srikar.: Locker security system using facial recognition and One Time Password (OTP)." In IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 812-815. (2017).
2. Mohammed, Salma, and Abdul Hakim Alkeelani: Locker Security System Using Keypad and RFID. In IEEE International Conference of Computer Science and Renewable Energies (ICCSRE), pp. 1-5. (2019).
3. Avinash, J. L., CS Naveen Kumar, R. Madan Kumar, Korepu Chaitanya, and D. Ashwin Karanth: Voice Based Security System with Electronic Eye. In 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 2434-2437. (2018).
4. Churi, Advait, Anirudh Bhat, Ruchir Mohite, and Prathamesh P. Churi: E-zip: An electronic lock for secured system. In IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), pp. 45-49. (2016).
5. Verma, Amit: A Multilayer Bank Security System. In IEEE International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), pp. 914-917. (2013).
6. Sridharan, Srivatsan: Authenticated Secure Bio-metric based access to the bank safety lockers. In IEEE International Conference on Information Communication and Embedded Systems (ICICES2014), pp. 1-7. (2014).
7. Teja, P. Satya Ravi, V. Kushal, A. Sai Srikar, and K. Srinivasan: Photosensitive security system for theft detection and control using GSM technology. In IEEE International Conference on Signal Processing and Communication Engineering Systems, pp. 122-125. (2015).
8. Nallathambi, Bharathiraja, and M. K. S. Nithyakala: Low cost home energy management with security and automation. In IEEE International Conference on Electronics and Communication Systems (ICECS), pp. 1-5. (2014).
9. Chikara, Arvasu, Pallavi Choudekar, and Divya Asija: Smart Bank Locker Using Fingerprint Scanning and Image Processing. In IEEE 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 725-728. (2020).
10. Tajane K, Patil S, Pitale R, Tajane M. Enhancing Security of Banking Locker System Using Secret Sharing Scheme Based on Random Grids. InEmerging Research in Computing, Information, Communication and Applications 2015 (pp. 175-181). Springer, New Delhi.
11. Ogri UJ, Okwong DE, Etim A. Design and construction of door locking security system using GSM. International Journal Of Engineering And Computer Science. 2013 Jul;2(7):2235-57.
12. Dhondge K, Ayinala K, Choi BY, Song S. Infrared optical wireless communication for smart door locks using smartphones. In2016 12th International conference on mobile ad-hoc and sensor networks (MSN) 2016 Dec 16 (pp. 251-257). IEEE.
13. Ramani R, Selvaraju S, Valarmathy S, Niranjan P. Bank locker security system based on RFID and GSM technology. International journal of computer applications. 2012 Jan 1;57(18).
14. Gayathri M, Selvakumari P, Brindha R. Fingerprint and GSM based security system. International journal of engineering sciences & research technology. 2014 Apr;1(3):4024-7.
15. Raja, S. K. S., & Jebarajan, T. (2012). Reliable and secured data transmission in wireless body area networks (WBAN). European Journal of Scientific Research, 82(2), 173-184.
16. Goyal S, Desai P, Swaminathan V. Multi-level security embedded with surveillance system. IEEE Sensors Journal. 2017 Sep 26;17(22):7497-501.
17. Cortez CD, Badwal JS, Hipolito JR, Astillero DJ, Cruz MS, Inalao JC. Development of microcontroller-based biometric locker system with short message service. Lecture Notes on Software Engineering. 2016 May 1;4(2):103.
18. Zuo F, de With PH. Real-time embedded face recognition for smart home. IEEE transactions on consumer Electronics. 2005 Mar 14;51(1):183-90.

19. Naresh D, Chakradhar B, Krishnaveni S. Bluetooth based home automation and security system using ARM9. International Journal of Engineering Trends and Technology (IJETT)–Volume. 2013 Sep;4:4052.
20. Goud DS, Md I, Saritha PJ. A Secured Approach for Authentication system using fingerprint and iris. Global journal of Advanced Engineering Technology, Vol, Issue3-2012. 2012.
21. Teja PS, Kushal V, Srikar AS, Srinivasan K. Photosensitive security system for theft detection and control using GSM technology. In2015 International Conference on Signal Processing and Communication Engineering Systems 2015 Jan 2 (pp. 122-125). IEEE.
22. Sampathkumar, A., Murugan, S., Rastogi, R., Mishra, M. K., Malathy, S., & Manikandan, R. (2020). Energy Efficient ACPI and JEHDO Mechanism for IoT Device Energy Management in Healthcare. In Internet of Things in Smart Technologies for Sustainable Urban Development (pp. 131-140). Springer, Cham