



e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

Volume 12, Issue 4, April 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.317

9940 572 462

6381 907 438

ijareeie@gmail.com

www.ijareeie.com



LiFi Based Security System –Digital Pen

Dr. J.Kohila^[1], Abhirame. G^[2], Gayathri .M^[3], Juvairiya S.A^[4], Malarvizhi .B^[5]

Associate Professor, Department of EEE, Francis Xavier Engineering College Vannarpettai , Tirunelveli,
TamilNadu, India^[1]

UG Scholar, Department of EEE, Francis Xavier Engineering College, Vannarapettai, Tirunelveli,
Tamil Nadu, India^{[2][3][4][5]}

ABSTRACT: In this digital world every thing is a resemblance of digital technology . Thisproject initialize the digital communication using the visible light and that must be reliable. So it must be secured, less expensive and also ecofriendly . Normally we use card for ATM purpose but there arises over several security issues to overcome such criteria here we introduce out the digital pen which replaces card and also helps in utilizing light communication. It basically uses light sources like LED to transmit data, by blinking the LED. These changes in the intensity of light are detected by a photodetector device which receives the data. Thus, illumination and communication are achieved simultaneously thereby offering a interference secure medium for a transmission.Now-a-days in the banking and financial sector for self-finance ATM plays an important role. With an ATM, a banking user can perform many banking and financial operation such as money withdrawal and money transfer and also uses for some account related information to interact with bank staff.

KEYWORDS : Li-fi Receiver, GSM module, Arduino , Digital pen , Electronic lock , LCD display.

I. INTRODUCTION

An ATM is an electronic banking machine that allows customers to withdraw money with an ATM card and perform other banking transactions without the aid of banking staff. ATM cards are linked to our bank account details. ATM cards are used to make payments in online and offline transactions. There are number of reported incidents nowadays about fraud involving ATM cards. The ATM card may be misused if the secret pin of our ATM card is accessed by others. The hackers through various unscrupulous activities can get access to the account and transfer money.Latest technology has proven that it is possible to clone a card and gain access to confidential information through which another individual or entity can make purchases on your card. In Mohamed Amine Arfaoui^[1] covers almost all aspects of PLS for VLC, including different channel models, input distributions, network configurations, precoding/signaling strategies, and secrecy capacity and information rates. Furthermore, we propose a number of timely and open research directions for PLS-VLC systems, including the application of measurement-based indoor and outdoor channel models, incorporating user mobility and device orientation into the channel model, and combining VLC and RF systems to realize the potential of such technologies. On considering the above problems faced by the users ,we have designed a new device called digital pen which is used instead of cards. It can store several bank accounts in a single pen and it cannot be revealed by the hackers.So therefore the main objective of designing this system is to enhance the security with the help of digital pen. This system uses visible light as the medium of communication by blinking of LED. The data transmission in this technology can be done using light because the light intensity changes quicker than the human eye for capturing. It provides interference free data transmission. This setup is more efficient since the LED consumes less amount of energy. In R. Gowri Shankaran^[2],this system is more secure because light waves cannot penetrate through walls and cannot be intercept by anyone outside the illumination of LED. It can be implemented in indoor infrastructure while it cannot be used in outdoor.

General credit cardarealso known as traditional credit cardsare the most common type.They are issued by a bank or credit card company and can be used in most establishments and online stores.General credit cards can be either secured or unsecured.Normally ATM card plays a vital role in our day to day life which is the basic source for all kind of net banking but even still there arises some kind of security issues . In the existing system ATM cards are used to withdraw money from ATM machine. ATM card enables a customer to access their financial accounts. It uses a 4-digit PIN or unique Personal Identification Number which is linked to the bank account. In this system the verification is performed by means of an RFID reader, which detects the number on the card. Authorization is considered



successful if this number matches the number in the system. This system possesses a major potential for robbery. In Sivakumar T^[15], Fraud occurs when a criminal gains access to your pin number to make unauthorized purchases or withdraw cash from your account.

Credit card fraud can happen if someone physically steals your card or virtually hacks your account, and it can be a serious headache to resolve. If you're a victim of fraud, you may incur unauthorized charges that can result in steep bills. And if your credit card balance increases drastically, you may risk damage to your credit score. Credit card fraud occurs when an unauthorized person gains access to your information and uses it to make purchases. Here are some ways fraudsters get your information:

1. Lost or stolen credit cards.
2. Skimming your credit card, such as at a gas station pump.
3. Hacking your computer.
4. Calling about fake prizes or wire transfers.

II. PROPOSED METHOD

The proposed system is being developed for the transaction process and security purpose. Security is necessary to hide the details of user credentials so that no one can hack it. For security, the existing card is replaced by a cardless system. The proposed method aims at encryption of user credentials through the Advanced Encryption Standard Algorithm (AES). The encrypted credential will be sent through LED (Li-Fi technology), and at the receiver side, will detect the light and send the signal to the Arduino board. In Arduino, user credentials will be programmed already.

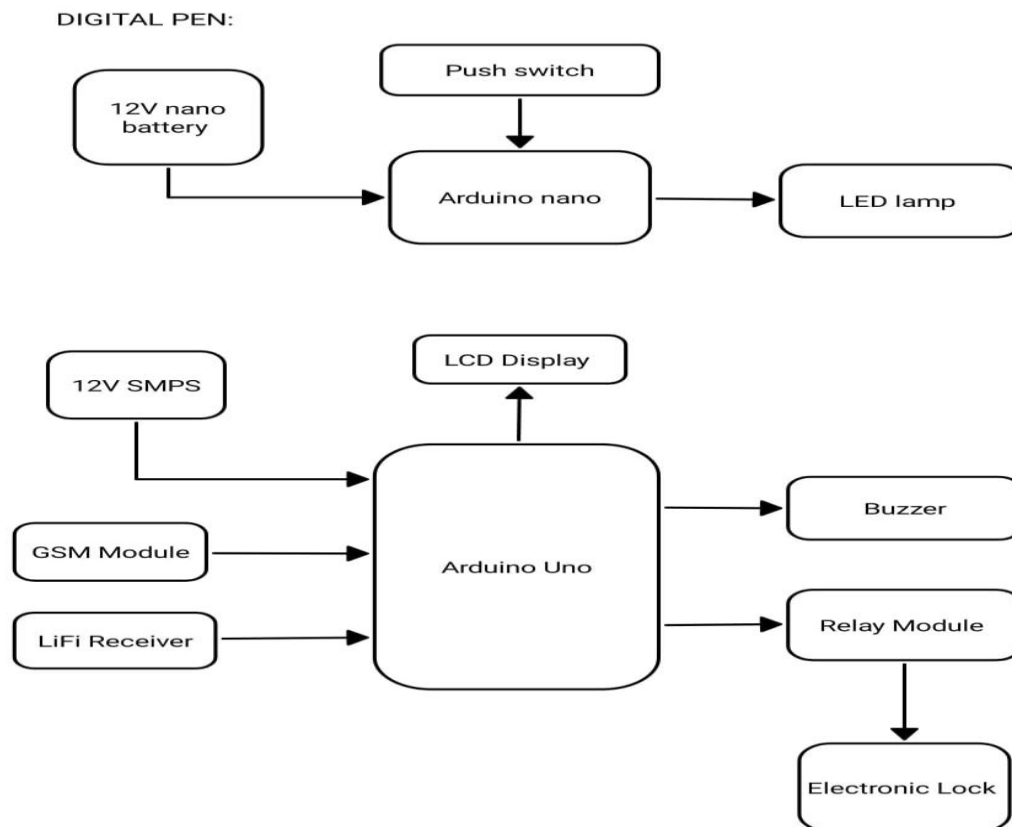


FIGURE 1 BLOCK DIAGRAM OF LIFI BASED SECURITY SYSTEM



When the light containing the data falls on the Li-fi receiver, the data is sent to Arduino which compares the existing data with the input data. If the data entered is correct, the bank transaction will be processed. To overcome all such security relevant issues digital pens are implemented which paves a high security. It uses Light communication in security system for safeguarding the pin code from the hackers. Digital pen can also store all the bank account details within a pen. This pen can store more than one bank accounts so there is no need of carrying ATM cards. This project uses Li-Fi technology in security system for safeguarding the pin code from the hackers by using a digital pen which stores all the bank account details within a pen. This pen can store more than one bank account so there is no need for carrying ATM cards. Simple and faster mode of communication using visible light spectrum. In Anwesh Chakraborty^[4], More secure. More efficient since LED consumes less energy. In Payas Goswami^[5], Lower latency with reduced delay time. Providing an interference free wireless communication. Protects sensitive information from potential hackers. In A. Vinnarasi.S.T.Aarthy^[3], it is reliable. It is safe, unlike infrared, there is no danger to the health from visible light in illumination condition. In Anurag Sarkar^[6], Li-fi is considered better than Wifi because of better availability, security, capacity and high speed of data transfer with less interference.

DIGITAL PEN



FIGURE 2 DIGITAL PEN

Digital pen is a compact portable device. The pen contains a Li-Fi module that enables it to send and receive data through light waves, allowing for secure and efficient communication. The interior design of digital pen consists of Arduino nano, 12V nano battery, push switch, LED lamp. The tip of the digital pen consists of an LED which transmits visible light. The light ray from the LED is captured by the Li-fi receiver. The supply to the Arduino nano is provided by a 12V nano battery. Push switch is used to turn on and off the LED.

DIGITAL PEN:

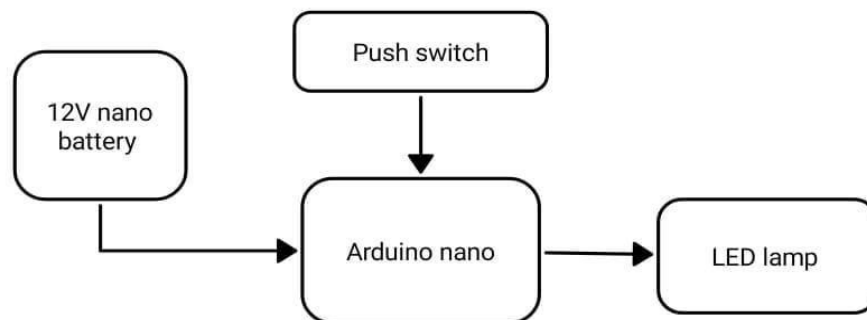


FIGURE 3 BLOCK DIAGRAM OF DIGITAL PEN



||Volume 12, Issue 4, April 2023||

|DOI:10.15662/IJAREEIE.2022.1204029 |

III. RESULT AND DISCUSSION

The prototype model was successfully implemented and tested. The digital pen was designed to send data with high security. The system was also able to send and receive data and also alert the prior bank and the user immediately if any unusual actions takes place. The system also enhances the security. The system's response time was evaluated, and it was found to be significantly faster than traditional methods. This is due to the implementation of light communication. This project uses Li Fi technology in security system for safeguarding the pin code from the hackers by using a digital pen which stores all the bank account details within a pen. This pen can store more than one bank account so there is no need for carrying ATM cards. It basically uses light sources like LED to transmit data, by blinking the LED. These changes in the intensity of light are detected by a photodetector device which receives the data. Thus, illumination and communication are achieved simultaneously thereby offering a interference secure medium for a transmission. It provides high amount of security as data communication is line of sight (LOS). Moreover, light signal covers low region does not pass through the walls. This will avoid unwanted access of light signal by unauthorized persons. The light devices consume low power for operation. The security LiFi provides is most likely its selling benefit. Light is unable to transcend opaque objects - LiFi is limited to its respected space because light cannot permeate walls, making it unable to go out of those bounds. In other words, the network can not be reached by other users in rooms surrounding it. Li-Fi (Light Fidelity) is a wireless communication technology that uses visible light to transmit data. It has several advantages over traditional Wi-Fi, including higher data speeds, greater security, and reduced electromagnetic interference. Li-Fi based security systems can provide increased security for sensitive information and data, particularly in areas where radio frequency communication is restricted or not permitted. Li-Fi signals cannot penetrate walls, which makes it more difficult for attackers to intercept data. Additionally, because Li-Fi uses light waves, it is not susceptible to electromagnetic interference or jamming, making it a more secure option. However, Li-Fi also has some limitations. For instance, it requires direct line of sight between the transmitter and receiver, which can limit its range and effectiveness in certain scenarios. It also requires a clear and stable light source, which can be challenging to maintain in certain environments. Overall, Li-Fi technology shows promise for enhancing security in certain applications, particularly in situations where traditional wireless communication methods are not suitable or secure enough. However, further research and development is needed to overcome some of its limitations and make it a more practical and widely adopted technology. Li-Fi technology can be put into the practical in future. It provides faster, simple, and efficient wireless digital communication. This technology makes us proceed with the safer, cleaner, and brighter future. We find the new in the future, data for smartphones, tablets, and laptops can be transmitted through light in a room by using Li-Fi. Data security is the important concern in the banking sector for secure and esoteric data transaction. In this paper, we use digital pen for transaction. Specifically here we discuss the communication procedure between the user and the ATM machine. In this mechanism, we transfer encrypted data using the Li-Fi Device.

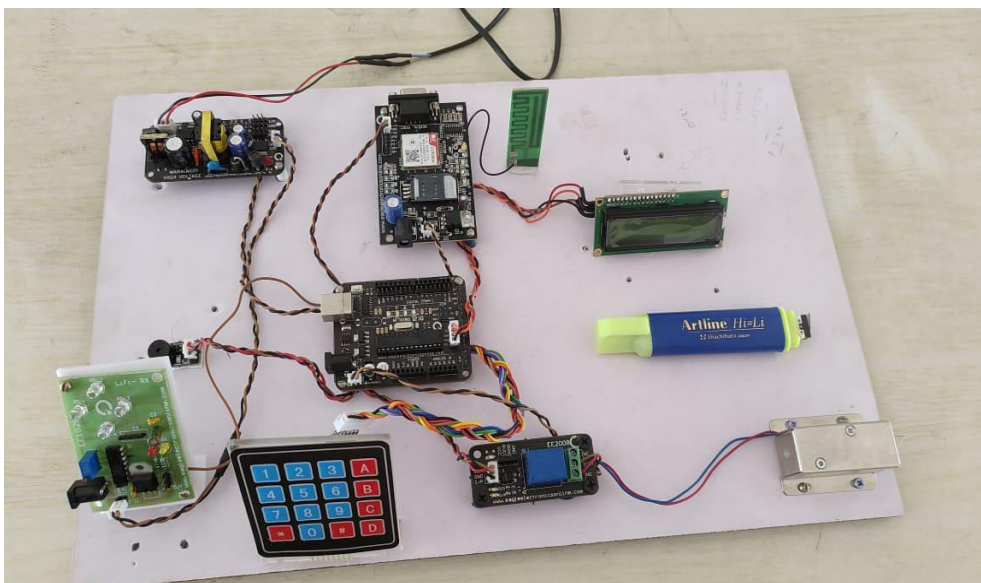


FIGURE 4 HARDWARE OUTPUT



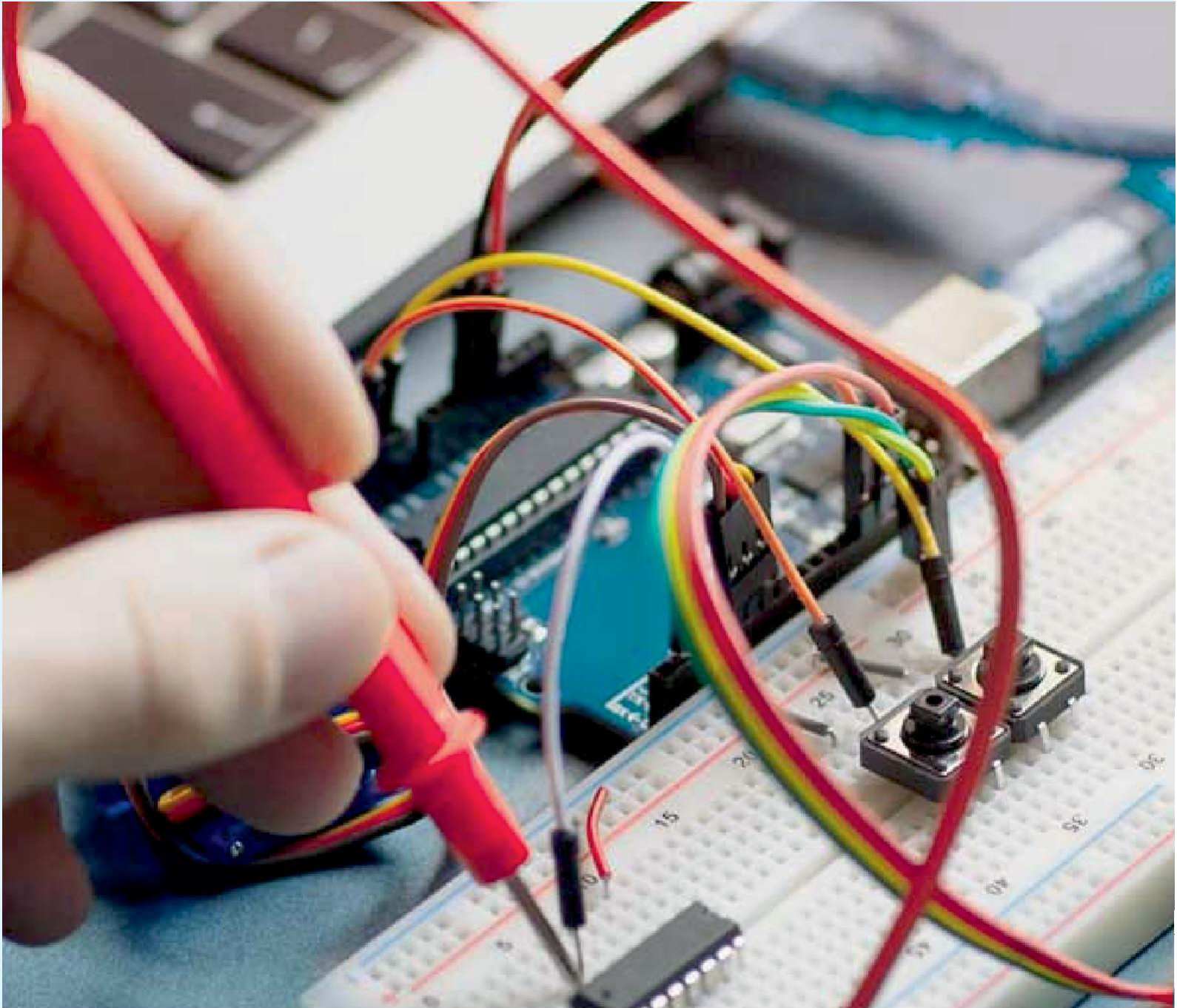
IV. CONCLUSION

Li-Fi based security system using digital pen is a promising technology that has the potential to enhance security and accuracy in various applications. This system uses light waves to transmit data, which provides a more secure and faster means of communication compared to traditional wireless technologies. The digital pen is a key component of this system, as it allows for accurate and efficient data capture and transmission. The pen contains a Li-Fi module that enables it to send and receive data through light waves, allowing for secure and efficient communication.

At present, the concept of Li-Fi technology is attracting a lot of wireless internet users due to its genuine features. The purpose of Li-Fi technology is to provide a high-speed data communication using visible light spectrum. Although Li-Fi has a good performance in the transfer rate, Li-Fi is not good enough when deployed in an outdoor in sunlight or other condition. Li-Fi will probably not completely replace Wi-Fi, these two technologies can be used together to achieve more efficient and secure network. Li-Fi's benefits may change the nature and dynamic of wireless communication technology with its users. Its light limitations make a secure network that can provide effective monitoring and location-based accessibility. Overall, Li-Fi based security system using digital pen has the potential to revolutionize the way we approach security and data communication. With its fast, secure, and accurate data transmission capabilities, this technology could be a game changer in various fields, including healthcare, finance, and education, among others. However, further research and development is needed to fully explore its potential and address any potential limitations or challenges.

REFERENCES

- [1] Mohamed Amine Arfaoui, Mohammad Dehghani Soltani, Iman Tavakkolnia, Ali Ghayeb, Majid Safari, Chadi M Assi, Harald Haas, "Physical Layer Security for Visible Light Communication Systems: A Survey" ,27 May 2019 ,Volume: 22 Issue: 3.
- [2] R. Gowri Shankaran, Dr. J. Selvakumar, "Visible Light Communication Using Li-Fi". International Journal for Research in Applied Science & Engineering Technology, Volume No 6, Issue VI, (2018),2321-9653.
- [3] A. Vinnarasi.S.T.Aarthy, "Transmission of Data, Audio Signal and Text Using Li-Fi", International Journal of Pure and Applied Mathematics, Volume 117 No.17. Special Issue, (2017),179-186.
- [4] Anwesha Chakraborty. Trina Dutta, Sushmita, Mondal, Dr. Asoke Nath. "Latest Advancement in Light Fidelity (Li-Fi) Technology" International Journal of Advance Research in Computer Science and Management Studies Volume No 5, Issue 11, (2017),47-53.
- [5] Payas Goswami, Manoj Shukla, "Design of Li-Fi Transceiver", Wireless Engineering and Technology Volume No 3, Issue 8, (2017),71-86.
- [6] Anurag Sarkar Shalabh Agarwal Dr. Asoke Nath. "Li-Fi Technology: Data Transmission through Visible Light", International Journal of Advance Research in Computer Science and Management Studies, Volume No 3, Issue 6, (2015), 1-12
- [7] Arunapriya V. Praveenkumar S. Kalimuthu K, "Li-Fi for Medical Care Using Visible Light Communication", International Journal of Applied Engineering Research Volume No 13, Number 11, (2018), 9273-9276.
- [8] P.M Benson Mansingh.M.Nithya.M.Krithika, "Li-Fi Based A New Home Automation System", International Journal for Research in Applied Science and Engineering Technology, Volume No 4, Issue 2, (2016), 321-325.
- [9] A. Bhati, M. Hansen, and C. M. Chan, Energy conservation through smart homes in a smart city: A lesson for Singapore households, Energy Policy, vol. 104, no. February, pp. 230-239, 2017.
- [10] I. Meena and D. Kumar, A Review Paper on Li-Fi, in National Conference on Innovations in Micro-electronics, Signal Processing and Communication Technologies, 2016, no. February, pp. 9-11.
- [11] Aneesa Tankasali, Vani.P.Datar, Divyashree Payannavar, Kadambari Chavan, Kaiyum Yelegar, "Smart Door Lock and Lighting System using Internet of Things", International Advanced Research Journal in Science, Engineering and Technology Vol. 8, Issue 8, August 2021.
- [12] P. Mishra, J. Poddar, and S. Priya, A Review On Li-Fi: The Green Wi-Fi, Int. Res. J. Eng. Technol., vol. 3, no. 3, pp. 99-103, 2016.
- [13] A. Jovicic, J. Li, and T. Richardson, Visible light communication: opportunities, challenges and the path to market, IEEE Commun. Mag., vol. 51, no. 12, pp. 26-32, Dec. 2013.
- [14] S. Wu, H. Wang, and C. Youn, "Visible Light Communications for 5G Wireless Networking Systems: From Fixed to Mobile Communications", IEEE Netw., vol. 28, no. 6, pp. 41-45, 2014.
- [15] Sivakumar T, Gajjala Askok K, Sai Venupratha, "Design and Implementation of Security Based ATM theft Monitoring system" International Journal of Engineering Inventions Volume 3, Issue 1 (August 2013).



INNO  SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.317



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

 9940 572 462  6381 907 438  ijareeie@gmail.com



www.ijareeie.com

Scan to save the contact details