International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Reconstructed Optimization Logic for the Secure Vaults with Arduino for the IoT Environment

Prasida Sunanda[1], K.A. Janardhananm[2], Rajesh Gupta[3], Shrishailappa Patil[4] Santosh Mitkari [5], Dr. Usha C. Pawar [6]

Submitted: 14/08/2022 **Accepted**: 20/11/2022

Abstract: Internet of Things (IoT) provides the transparent and seamless services to the deployed application. However, the IoT environment subjected to the challenge of the data security for the deployed environment. The presence of the IoT devices in the network comprises of the evolution, advancement and huge data for the frequent attackers in the network. The hackers of the IoT network uses the large number of data attacker to identify and collects the personal information and identity of the data. To make the IoT devices more manageable and secure for the different environment it is necessary to develop a appropriate security scheme. This paper proposed a Reconstructed Network Logic optimization (RNLO) model for the data security in IoT. The proposed RNLO model uses the reconstructed network logic features for the estimation of the features. Through the reconstructed algorithm the logic is characterized with the optimization model. The implementation of the optimization model uses the estimation of the node is attacker or not with the scoring value in the optimized values. To enhance the security the Arduino Duo based secure vaults is implemented in the proposed RNLO for the security improvement. The experimental analysis expressed that proposed RNLO model increases the attack prevention rate with the improved accuracy value of 99% which is ~5% higher than the existing attack detection techniques.

Keywords: *Internet of Things (IoT), Arduino Duo, Reconstructed Logic, Optimization Model, Security, Vaults*

1. Intoduction

The major challenge in using IoT is to provide transparent and maximum seamless service without security. The IoT devices evolution, advancement, and huge amount of data make the target of hacker's frequent attacks [1]. The report of internet security threats says that the attackers require just 2 minutes of time to hack IoT devices. The attackers will collect the data and utilise the IoT devices as a botnet to generate a larger number of attacks. The physical objects will identify and share personal information about the user's daily life frequently [2]. So, it is required to check the security and privacy of applications based on IoT. The impact of the attacks on IoT devices will result in loss of life or disaster. The utilisation of IoT devices on unmanaged and managed environmental conditions increases the rate of complexity in terms of computing and communication systems [3]. Further, it increases the vulnerability of IoT devices, and the wireless data transmission makes the application of IoT meet the requirements of security in the internet and network of devices along with the security measures to check reliable and safe operations [4]. In the perspectives of privacy and security, the introduction of sensors and devices in intimate spaces like wearable devices, cars, and houses inject more security and privacy threats in the environment of IoT.

[1] Research Scholor, Management Studies, NICHE, Noorul Islam Centre for Higher Education, Thucklay, prasidasunandas@gmail.com
2 Professor, Management Studies, NICHE, Noorul Islam Centre for Higher Education, Thucklay, kajanardhanan@yahoo.com
3 Pro Chancellor, Department of Management,Sanskriti University, Mathura, Uttar Pradesh, India, prochancellor@sanskriti.edu.in
4 Professor, Computer Vishwakarma Institute of Technology, Pune patil.st@vit.edu
5 Assistant Professor, Mathematics, Bharati Vidyapeeth's College of Engineering for Women, Pune, Santosh.Mitkari@bharatividyapeeth.edu
6 Assistant professor, Datta Meghe College of Engineering, Airoli, Navi Mumbai, Maharashtra, Mechanical Engineering, Datta Meghe College Of Engineering, Airoli, Navi Mumbai

Various cutting-edge technologies were developed, such as software-defined networking, big data analysis, cloud computing, and intelligent sensors to use every power of IoT [5]. But, these technologies for IoT are in the initial stage and need to be improved from the technical perspective. So, the new technologies include challenges in providing security and privacy issue [6]. The heterogeneous behaviour of IoT devices increases the security problems on the present internet. Most of the information used in IoT is personal data which needs to be protected for providing security. The perimeter defences are limited in the IoT environment. It will interpret and analyse the huge 26 structured and unstructured information in IoT devices to develop the instincts of security to provide an effective response for the defence to threats [7]. The conventional mechanism for providing security is not suitable in the environment of IoT because of its unique characters.

As specified before, brilliant urban areas end up noticeably more quick witted due to the advance idea of computerized innovation, in which shrewd city is prepared with various electronic gear used by the different application [8], In this heterogeneous condition in term of articles highlights, donors, inspirations, security rules, and so forth unique inquiries emerges from a city domain, which need to respond . These are [9]: How to handle vulnerability prompted because of the ongoing and disconnected elements and guarantee the nature of data? How to make existing items more astute? Then again, how to outline new questions more intelligent in light of the client decision? How to empower items to respond as needs be as for setting? How to limit the cost of information gathering that is being created by a few gadgets? How to get an understanding into the information if information is gathered and going to preparing stage in a continuous? In view of the inquiries specified over, the keen city idea uses ICT in a way that could help the subjects in an extremely day life inside constrained assets. In addition, different association plan to build up a framework that utilizations propelled innovation by giving the productive administrations to their residents [10]. The larger part of these current innovations

comprises of cutting edge detecting abilities, stockpiling capacity for the remarkable volume of information, lastly, to get an understanding into the voluminous information. The common outline of the Internet of Things consolidates other than various passing on devices a cloud-based server plan, which is required to relate and perform remote data organization and tallies. Sensors, actuators, devices and furthermore individuals and programming administrators relate and grant data to execute specific endeavors or more refined business or particular structures [12]. The Internet of Things maps and arranges certifiable articles into the virtual world, and extends the relationship with adaptability systems, composed exertion candidly strong systems, additionally, structures and organizations for enormous data and cloud conditions. As the security is major concern this paper developed a secure vaults for the IoT environment to increase data security in the IoT network. The proposed model uses the reconstructed logic based optimization model for the secure data communication in the network.

2. Related Works

In [13] proposed a thought that in industry, there is, have to secure all the pertinent data, insights and information identified with the distinctive modern procedures, engines, machines and gadgets utilized in industry premises. This goes for controlled access, better efficiency and top notch consequences of mechanical items being made. For this reason, modern natural parameters checking and controlling is required. Web of Things (IoT) is quickly expanding innovation. IoT is the arrangement of physical things or things embedded with equipment, programming, sensors, and framework organize, which engages these articles to assemble and exchange data. In this article, they are developing a structure which will screen and control the cutting edge parameters using thought of IoT with remote devices, Android, and sensors. It is the best and by and large invaluable. So it has awesome social prospects.

In [14] proposed a moved response for checking the surroundings conditions at a particular location and make the records discernible everywhere in the international. The development at the back of that is net of factors (IoT), that is an advanced and succesful response for associate the matters to the internet and to interface the whole universe of things in a framework. proper here matters might be a few element like virtual devices, sensors and car digital equipment. The device oversees searching and controlling the commonplace conditions like temperature, relative moistness, slight strength and CO degree with sensors and sends the information to the internet site internet page and a quick time later plot the sensor records as graphical bits of expertise. The information revived from the realized gadget can be open within the net from anywhere on the earth.

In [15] arranged a framework and plan of street of a nation plays extremely essential or fundamental parts being developed and development in different field like financial, social, social and so on. So for better and fast development for any nation we should concentrate on street condition, plan of street, offices for client and terrible street organize overview in light of the fact that there are numerous issue faces by buildup individuals in their every day routine life. Some advanced creative system and strategy are already acquaint with make or develop street more astute and resolve all issue likes automobile overloads, mischances, wounds and deferral because of terrible street condition and so on. In this paper we are dealing with those strategies and systems that already present yet not get such a large amount of supportive as we acknowledged. So there is need of act of spontaneity in already strategies and techniques and acquaint some more methods with escape all issues however much as could be expected.

In [16] developed a medicinal services benefits in light of Internet of Things (IOT) to vanquish the thoughtlessness of the present human administrations information system. The key innovations and improvement of savvy medicinal services administrations is displayed in perspective of appreciation of the suggestion and designing of shrewd social insurance. Commonly, as a result of distractedness of social insurance staff or of relatives it may happen that pharmaceutical isn't observed appropriately and it might prompt the reason of heart assault or other dangerous conditions.

3. Estimation of Node with the Gate Interface System

The deployed sensor nodes are evaluated based on the consideration of the substantial amount of node optimization in IoT environment. The developed model Reconstructed Network Logic optimization (RNLO) uses the substantial load in the systems. To reduce the overall load in the system the proposed RNLC uses the optimized system for the network maintenance. The proposed model uses the Arduino sensor are Dust Concentration Sensor (MQ135), Humidity Sensor (DHT11), Air Quality Index Sensor (MQ 135) and Voltage Level Sensor (ZMPT101B) are utilized. The data for processing is collected from the three sequential data with the interfaced MCU ESP8266 with the 600 different records and readings in the sensor unit. The proposed RNLO algorithm uses the hashing and merging process with the 512-big segments. Additionally, the four different buffers are utilized with the 32 bit size.

The proposed model perform the 4 iteration with the utilization of the sub-blocks, buffer and fixed array number value of T[1] -> T[64]. The gated array blocks are denoted as the M[0] -> M[15] with the buffer value of B,C and D with the non-linear process. The four step iteration process are presented as follows:

Iteration Count 1: (a AND b) OR ((NOT b) AND (c))
Iteration 2: (b AND c) OR (d AND (NOT c))
Iteration 3: b XOR c XOR d
Iteration 4: c XOR (b OR (NOT d))

The proposed RNLO process with the selection of the header in the sequences are presented as the follows:

Algorithm I: Reconstructed Network Logic Optimization

Compute the present state of node
  Construct a cluster with the header formation
Perform the secure cluster Head selection
Compute the node position $N_i = \{n_1, n_2, \ldots\ldots, n_n\}$ with the estimation of the neighbours $P_i = \{p_1, p_2, \ldots\ldots, p_n\}$
If
  Size of the neighbor > volume of cluster
  Modify the neighbor list based on volume cluster
Arrange the list of neighbour as P_i
Compute the every node “i" within the neighbour values
If
  Neighbour value <=2/3
then
  node is considered as mistrust nodes
Compute the P_i with the value of ct<0
Categorize the every node either as normal or malicious based on probability
else if
  Neighbour > 2
Considered the node is normal
Else if
  Distance > size
Enrol in the intruder list in the node
Cluster head with the peak value of V

The overall process architecture of the proposed RNLO is presented in figure 1 as follows:

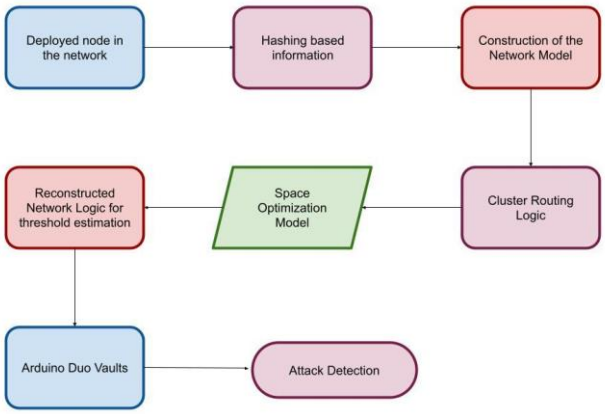

Figure 1: Overall Flow of RNLO

The information about the sensor node are estimated based on the information data *e (n).* Based on the consideration of the array data dissimilarity data d (j). The features in the data were processed and evaluated using the equation (1) – (3)is

$$e_1(i) = e(i+1) - d(i), i = 1,2, \ldots \ldots, n-1 \quad (1)$$

$$e_2(i) = e1(j+1) - d1(i), i = 1,2, \ldots \ldots, n-2 \quad (2)$$

$$e(j) = [e^2(j)]^2 \quad (3)$$

In the above equation the information data is represented as e (n) for the total n points in the sensor data those are squared with the dissimilarity value of d(j). The sensor data dissimilarity feature values for the peak overhead is estimated based on the threshold value of 3% maximal values. The proposed RNLO model comprises of the interval value time of ±75 ms. The every designed comprises of the ±75 ms windows.

3.1 Arduino Uno Processor

The RNLO model aimed to increases the security in the IoT environment with the use of the Arduino processor. The analysis is based on the consideration of the ATmega328 based microcontroller board with the 14 digit input and output pins. In this the 16 pins are uses as the analog input and frequency operation of 16MHz with the USB connection. The connected USB-to-serial converter with the Arduino 1.0 were presented in the table 1.

Table 1: Configuration of the Arduino

Name of Microcontroller	ATmega328
Voltage utilized for operation	5V
Input Voltage Range	7-12V & 6-20V
I/O Pins	14
Input Pins (analog form)	6
I/O Pin for DC current	40 mA
DC Current pin	50 mA
Flash Memory	32 KB
SRAM	2 KB
EEPROM	1 KB
Clock Speed	16 MHz

The selected Uno Arudino model comprises of the reference version of the processors in the forward direction based in the Arduino series. The power supply of the USB connector is provided with the external source supply.

4. Analysis with the Arduino Vault for security

The proposed RNLO model comprises of the database to evaluate the vector values collected from the different sensor nodes. The process of data collected from the sensor nodes were evaluated with the 500Hz for the 20sec. In table 2 the data set features for the collected data form the sensor for the bits 14 are presented.

Table 2: Estimation of bits in Arduino

DCT, Q bits=14, Samples=43200, Time = 2 mins												
Data	UPRD=0.5			UPRD=1			UPRD=2			UPRD=3		
	BPRD	QPRD	CR	BPRD	QPRD	CR	BPRD	QPRD	CR	BPRD	QPRD	CR
120	0.42	0.49	15.67	1.04	1.45	34.74	1.99	1.94	48.56	1.98	3.04	48.76
130	0.48	0.43	11.83	1.03	1.35	30.56	1.98	1.98	43.64	1.87	3.16	36.54
150	0.53	0.48	12.67	1.07	1.55	19.57	1.98	1.96	19.56	2.78	3.25	23.67
200	0.51	0.46	12.87	1.84	1.78	17.56	1.99	1.99	20.97	2.57	2.97	26.45
230	0.53	0.47	11.63	1.45	1.35	19.68	1.99	1.96	23.45	2.79	2.86	22.45
250	0.53	0.46	11.46	1.78	1.80	21.35	1.98	2.06	20.86	2.45	2.65	25.95
260	0.54	0.49	12.45	1.63	1.45	18.56	1.99	2.07	19.74	2.86	3.36	23.46
270	0.53	0.53	11.73	1.43	1.34	13.63	1.99	2.06	23.46	2.58	3.07	28.46
280	0.52	0.54	11.93	1.39	1.87	14.56	1.98	2.18	22.78	2.59	3.14	22.78
290	0.51	0.56	11.96	1.04	1.34	19.56	1.99	2.08	26.54	2.86	3.67	28.56

The evaluation is based on the consideration of the quantization bits denoted as Q bits; User defined PRD as UPR, PRD before the quantization is represented as BPRD and PRD value after the quantization process is denoted as QPRD and Compression Ratio is stated as CR. With the secure vaults in the Arduino the proposed RNLO model features are evaluated for the duration of 2 minutes with the data sample of 43200 with the quantization threshold value of 14-bits.

Initially, with the Arduino vaults for the secure communication in the IoT environment accuracy is computed as in equation (4)

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

The figure 3 provides the graphical representation of the measured accuracy for the different secure vaults with the proposed Arduino vaults with the RNLO model.

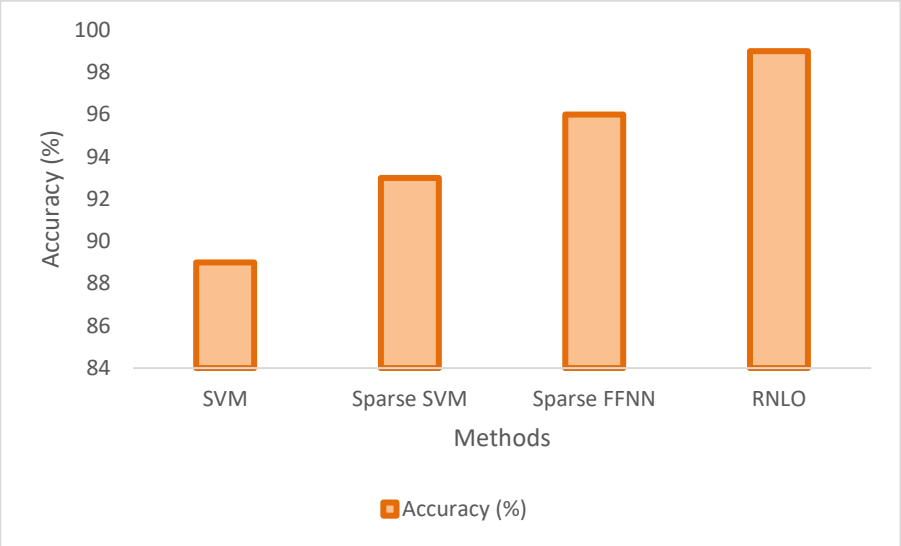

Figure 2: Comparison of Accuracy

The experimental analysis of the accuracy demonstrated that proposed RNLO secure vaults scheme for the Arudino provides the accuracy value of 99% which is significantly higher than the SVM, Sparse SVM and Sparse FFNN.

Sensitivity is the parameter involved in the positive prediction of the variables with the estimation of the features with the identification of the points in the system. The sensitivity of the model is computed using the equation (5)

$$Sensitivity = \frac{TP}{TP+FN} \quad (5)$$

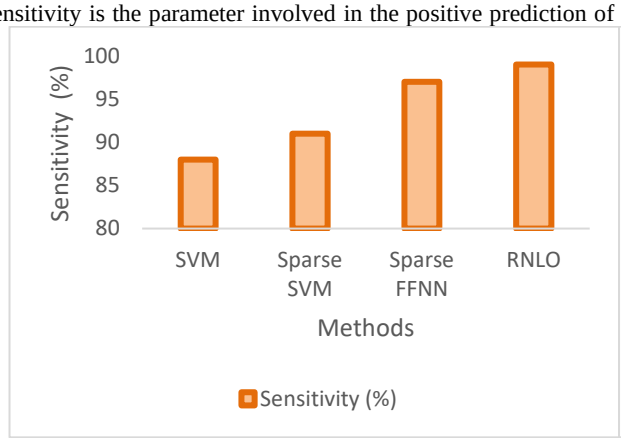

Figure 3: Comparison of Sensitivity

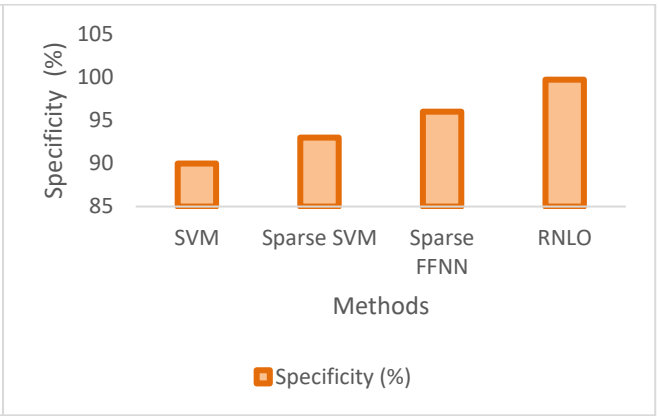

Figure 4: Comparison of Specificity

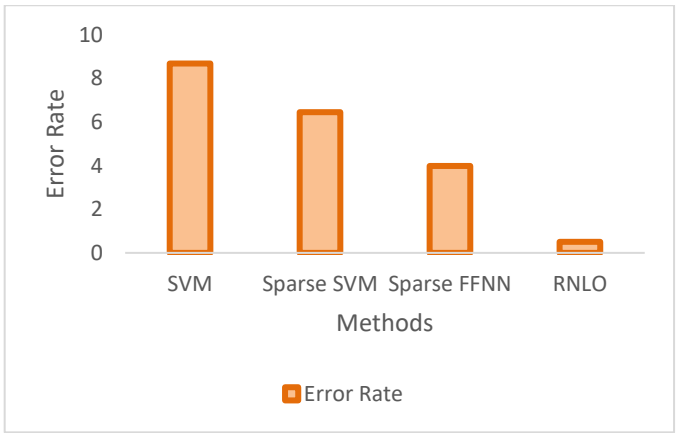

Figure 5: Comparison of Error Rate

The comparative examination of the sensitivity and specificity expressed that the proposed RNLO secure vault model with the Arudino exhibits the higher security value than the conventional techniques. The sensitivity of the proposed RNLO model is achieved as the 99% and the specificity value of the model is achieved as the 99.6% which is significantly higher than the existing techniques. Similarly in figure 5 the estimated error rate for the proposed RNLO model is presented. The comparative examination expressed that the error rate for the proposed RNLO model is significantly minimal than the existing techniques. Through the analysis it is concluded that the proposed RNLO model with the Arudino secure vault exhibits significant security for the IoT applications.

5. Conclusion

IoT is emerging field for the different application scenario for the effective functionality and the performance. However, the conventional IoT system subjected to the challenges associated with the security. To withstand the security challenges associated with the IoT system this paper uses the Arduino vaults secure model for the IoT applications. The developed model RNLO estimates the position of the nodes with the reconstructed optimization model. The security in the proposed model is improved with the Arduino Duo processor. The experimental analysis expressed that proposed RNLO model with Arduino achieves the higher accuracy value of 99% compared with the existing security technique. The performance of the proposed RNLO model is ~5% higher than the existing SVM, Sparse and FFNN model.

References

[1] Mabrouki, J., Azrour, M., Dhiba, D., Farhaoui, Y., & El Hajjaji, S. (2021). IoT-based data logger for weather monitoring using arduino-based wireless sensor networks with remote graphical application and alerts. *Big Data Mining and Analytics*, *4*(1), 25-32.

[2] Kanade, P., & JP, P. (2021). Arduino based machine learning and IOT Smart Irrigation System. *International Journal of Soft Computing and Engineering (IJSCE)*, *10*(4), 1-5.

[3] Arunachalam, A., & Andreasson, H. (2022). RaspberryPi-Arduino (RPA) powered smart mirrored and reconfigurable IoT facility for plant science research. *Internet Technology Letters*, *5*(1), e272.

[4] Ahmed, A. S., Marzog, H. A., & Abdul-Rahaim, L. A. (2021). Design and implement of robotic arm and control of moving via IoT with Arduino ESP32. *International Journal of Electrical & Computer Engineering (2088-8708)*, *11*(5).

[5] Mankotia, A., & Shukla, A. K. (2022). IOT based manhole detection and monitoring system using Arduino. *Materials Today: Proceedings*, *57*, 2195-2198.

[6] Banerjee, P. S., Karmakar, A., Dhara, M., Ganguly, K., & Sarkar, S. (2021). A novel method for predicting bradycardia and atrial fibrillation using fuzzy logic and arduino supported Iot sensors. *Medicine in Novel Technology and Devices*, *10*, 100058.

[7] Ahmed, E. Q., Aljazaery, I. A., Al-zubidi, A. F., & ALRikabi, H. T. S. (2021). Design and implementation control system for a self-balancing robot based on internet of things by using Arduino microcontroller. *Periodicals of Engineering and Natural Sciences (PEN)*, *9*(3), 409-417.

[8] Janeera, D. A., Poovizhi, H., Haseena, S. S., & Nivetha, S. (2021, March). Smart embedded framework using arduino and IoT for real-time noise and air pollution monitoring and alert system. In *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)* (pp. 1416-1420). IEEE.

[9] Ga, S., Cha, H. J., & Kim, C. J. (2021). Adapting Internet of Things to Arduino-based devices for low-cost remote sensing in school science learning environments.

[10] Kumar, N., Dey, B., Chetri, C., Agarwal, A., & Debnath, A. (2022). Development of an IoT-Based Smart Greenhouse Using Arduino. In *Advances in Communication, Devices and Networking* (pp. 455-465). Springer, Singapore.

[11] Singh, K., & Bura, D. (2021). Internet-of-Things (IoT): Distinct Algorithms for Sensor Connectivity with Comparative Study between Node MCU and Arduino UNO. *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, 4313-4324.

[12] Gnanavel, S., Sreekrishna, M., DuraiMurugan, N., Jaeyalakshmi, M., & Loksharan, S. (2022, January). The smart iot based automated irrigation system using arduino uno and soil moisture sensor. In *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 188-191). IEEE.

[13] Ganguly, K., Karmakar, A., & Banerjee, P. S. (2021, January). ValveCare: a fuzzy based intelligent model for predicting heart diseases using arduino based IoT infrastructure. In *International conference on computational intelligence in communications and business analytics* (pp. 229-242). Springer, Cham.

[14] Prakash, A., Kumar, R., Singh, P. K., Singh, A., Ahmed, S., & Jain, A. (2021). A Review on IOT Based Water Irrigation And Farm Protection using Arduino.

[15] Reddy, N. V. K., Varma, G. M., & Visalakshi, P. (2021). Design of IoT Based Coal Mine Safety System Using Arduino UNO. *Annals of the Romanian Society for Cell Biology*, 5663-5670.

[16] James, A., Seth, A., & Mukhopadhyay, S. C. (2022). Programming Arduino for IoT System. In *IoT System Design* (pp. 81-104). Springer, Cham.