[1]Faizan Ahamad*

Faisal Anwer[2]

Salman Ali[3]

Secured IoT Model for Monitoring Smart Field Data Through Real-Time Cloud Integration Utilizing Lightweight Cryptography

Journal of Electrical Systems

Abstract: - Implementing an Internet of Things (IoT)-powered system in agriculture, supported by sensors for real-time data collection, is crucial. Nowadays, there has been a surge in the adoption of sensor-based IoT devices in agriculture, which is a cutting-edge communication technology embraced by agricultural entrepreneurs and farmers. Agricultural entrepreneurs and farmers utilize this technology to execute various agricultural tasks with the aim of enhancing productivity, improving monitoring capabilities, and reducing labor costs. In the proposed method, the sensor detects the change in temperature and humidity and transmits sensor data to the cloud server after every 2 sec. The user can request this data from the cloud. There is a significant security and privacy threat during data transmission. Because of the diverse and dynamic nature of the IoT network, traditional cryptographic algorithms are not suitable for it. The approach employs two levels of encryption, namely the Substitution-Caesar cipher and the Advanced Encryption Standard (AES), to ensure the secure transmission of sensor data. Genetic algorithm (GA) is employed for key generation in order to improve system security. Mobile applications, like RaspController, that are easily accessible can be utilized to monitor the temperature and humidity of the field. The obtained average avalanche effect of the proposed method is about 55%, which shows the strength of the algorithm. The resulting encryption and decryption times are 0.390 ms and 0.110 ms, respectively. Furthermore, the suggested hybrid approach exhibits better performance on specific parameters when compared to cutting-edge cryptographic algorithms like DES, 3DES, RSA, Blowfish, and ECC.

Keywords: IoT, Data confidentiality, Raspberry Pi, RaspController app, DHT22, Genetic Algorithm, Advanced Encryption Standard.

I. INTRODUCTION

A wide range of agricultural applications are anticipated to be brought about by the rapidly expanding Internet of Things (IoT) technology [1]. The adoption of IoT by the agriculture sector has happened extremely swiftly [2], [3]. By integrating IoT features into farming devices, the industry has improved production and quality of service, which has greatly benefited farmers and entrepreneurs with secure management [4]. Cloud-based services can be used to give regular and emergency services to farmers who are situated in remote areas. Through cloud utilization, wireless communication systems such as 5G have enabled users to get data from sensor-based Internet of Things devices[5]. IoT sensors have the capabilityto process large amounts of field data continuously. Applications for farming based on IoT can be employed to collect essential field data in real-time, at regular intervals. Agriculture sectors acknowledge that the Internet of Things is going to be the most significant technology in the future [6][7]. The advent of IoT in the agriculture sector has inspired researchers worldwide to develop intelligent applications. High-tech monitoring tools can be utilised to gather data from the agricultural field about many parameters, such as temperature, moisture content, humidity, and air quality [4]. Sensor-based Internet of Things (IoT) devices provide continuous data monitoring and transmission to smartphones via cloud servers [8].Figure 1 shows anIoT-based smart agriculture system with temperature and weather sensors.

[1*]Department of Computer Science, Aligarh Muslim University, Aligarh-202002, ahamadfaizan.amu@gmail.com

[2]Department of Computer Science, Aligarh Muslim University, Aligarh-202002, India, faisalanwer.cs@myamu.ac.in

[3]Department of Computer Science, Aligarh Muslim University, Aligarh-202002, India, salmanali.amu@gmail.com

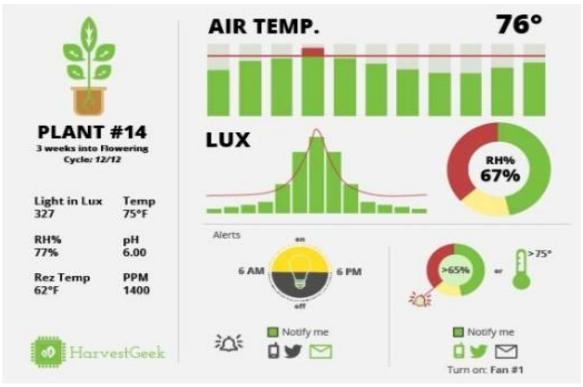

Fig. 1. Agriculture Field with weather and temprature sensor

Numerous security and privacy concerns have been noted in the vast volume of agricultural data generated by the quick growth of IoT in this field. However, any advantages of the Internet of Things may be outweighed by assaults and malfunctions if strong security is not in place [9],[10]. The main obstacle to cloud-based systems for agriculture is the security risks, which include the manipulation of private cloud data, breaches of data privacy, and unapproved use of the data. Consequently, a variety of security requirements for cloud-based farm systems and IoT must be met. Therefore, high security intelligence is supported by all IoT devices for the encryption and decryption of sensitive data[11].

IoT devices' range of use and power are constrained. Thus, depending on the key size, encryption techniques for Internet of Things devices should be less complex and operate with lower memory utilization[12]. Elliptical curve cryptography (ECC), being an option for Internet of Things devices, can statistically offer more security using a smaller key size than traditional systems[13]. Because the outcome of the decryption process will be unclear in the absence of a valid authentication key, elliptical cryptography is strong.

The IoT-based smart monitoring system for agriculture presented in this research uses IoT technology to facilitate communication among farmers and field nodes[1]. An IoT device with processing capability collects data from sensors and sends it to a cloud server. On request, farmers can access this data from the cloud[14]. As shown in Figure 2, data can be retrieved using a smartphone, tablet, orLCD that is connected to the device.

Fig. 2. Sensors data flow

Ensuring confidentiality of data is a significant challenge in maintaining security and privacy. It enables the protection ofinformation from unauthorized users. Conventional encryption algorithms present numerous difficulties for this task. To provide confidentiality in IoT, solutions must address the challenges of high scalability requirements, heterogeneity of the building blocks involved, as well as the limited resources of embedded devices, such as energy and processing limits [15],[16].

This approach uses a lightweight hybrid security framework that uses Substitution Caeser Cipher and AES for data confidentiality during transferred or stored data. Within this framework, encryption key is created using GA, and AES is employed for encryption of sensor data[17],[18], shown in Figure 3.With this two-pronged strategy, data confidentiality will be reinforced and resource usage will be optimized to meet the unique requirements of agricultural IoT.

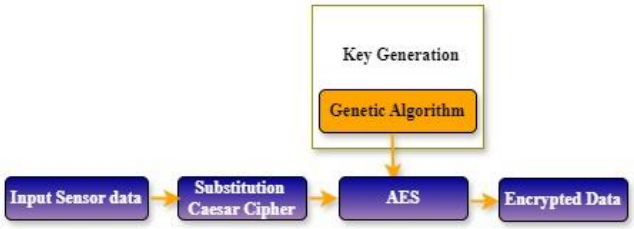

Fig. 3. Lightweight hybrid GA – AES framework

The rest portions of this paper conform to a specific framework. Part II discusses works that can be compared to the research, Part III provides the background of the paper, and Part IV presents a comprehensive analysis of the proposed study. Section V analyzes the outcomes of theimplementation and Section VI concludes the paper.

I. RELATED WORKS

In this section, we reviewed the cutting-edge contributions of other researchers in this domain. Most of the research has concentrated on cloud based monitoring of agricultural condition. We explore a few of these noteworthy contributions below.

Thakuret. al. [19], outlined a network of wireless sensors with application for agriculture in articlefor crop field monitoring. These systems are completely furnished with two types of sensor nodes for temperature and humidity measurements, as well as an image sensing node for information comparison through crop picture capture.

Rehmanet. al. [20], provides a study to make an informed decision quickly and produce a healthy crop, parameters are crucial. The three parameters are pictures, humidity, and temperature. By using these techniques, one can obtain great sensor stability at minimal power consumption. For an extended duration, the agricultural field area is being monitored.

Subahiet. al. [21], outlined a greenhouse monitoring system based on cloud-based agriculture IoT was proposed in paper. Employing sensor devices like light, relative humidity, temperature, and soil moisture sensors, greenhouse management may efficiently monitor various environmental factors. The sensors are gathering data on the agricultural field area every thirty seconds, which is then documented and saved online via cloud computing as well as the Internet of Things.

Raoet. al. [22], describe an irrigation automation and crop-field monitoring system based on Internet of Things. In their work, a system for monitoring crop fields is constructed with sensors, plus the irrigation system runs automatically based on a server's decision made using the detected data. Data that has been sensed is transmitted wirelessly to a website server database. If the irrigation system is automated, it will stop working if the temperature and moisture levels drop below the acceptable range. An application that gives the user a web interface allows them to control and monitor the system remotely.

Anushreeet. al. [23], proposed a smart drip irrigation system. In order to minimize human intervention, an Android smartphone application is utilized to remotely regulate and monitor the agricultural area. A drip irrigation system can cut down on water waste since it uses data from water level sensors. The ambient conditions are monitored by a few more distinct sensors.

Garcíaet. al. [24], describes IoT-based smart irrigation solutions are suggested. It takes a few wireless sensors to determine the soil's water content and humidity. Through a network, these sensed data are transmitted to a smart gateway, which is referred to as the Generic IoT Border Router Wireless Br 1000. The data is subsequently sent over a network from the gateway to a web service.

Sinhaet. al[25], provides a survey to carry out a range of agricultural tasks, including spraying, weeding, moisture detection, and scaring birds and animals, to gain a better understanding of the Internet of Things-based advancement in agriculture using cloud computing.

II. BACKGROUD

This section provides an overview of the network's architecture and briefly explains the key concepts and techniques used in the methodology, such as Genetic Algorithm (GA), Substitution Caesar cipher, and Advanced Encryption Standard (AES).

A. Four layers IoT-Agriculture architecture

Analysing the literature review leads to the proposal of a conceptual model for smart agriculture. Tell us about the general IOT structure first. In actuality, IOT is composed of numerous physical devices and essentially includes three layers[26]. The integrated application layer, which is the initial layer, is used for agriculture-related applications since it is regarded as the user interface layer. In order to monitor the agricultural region, it is free to use and incorporates personal gadgets and cell phones belonging to farmers. With the help of this layer, farmers are able to make decisions that will safeguard their crops and improve the yield of food produced.

Figure 4 illustrates the four-layer Internet of Things architecture.The second layer, known as the information management layer, has a key role in creating, maintaining, and making decisions as well as for the formation and classification of data. The third layer, called the network management layer, encompasses various communication technologies like UMTS, Gateway, Bluetooth Low Energy, WiFi, Zigbee, and 3G. The fourth layer, referred to as the information collection layer, comprises a range of sensor technologies. They are utilized for gathering crop data to enable more convenient and effective field monitoring in agricultural areas[27].

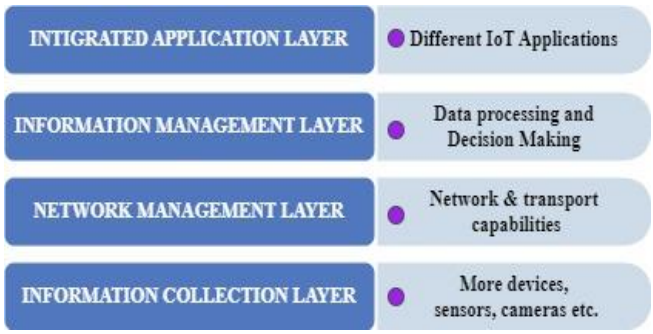

Fig. 4.IoT architecture layers

B. Genetic Algorithm

The generative algorithm, or GA, is a popular method for resolving optimization issues with or without restrictions. Mathematical sciences, computer sciences, and biological sciences all heavily utilize GA. GA is implemented in computer science to solve rh security and optimization problems that are both limited and unrestricted. Since GA can tackle NP-hard problems, it minimizes the enormous computational cost by addressing optimization problems quickly. GA is a bio-inspired computational method that continuously alters each unique solution for the chosen population. The fundamental processes of GA are population generation, crossover, and mutation [28]. Because GA's structure differs from that of traditional security techniques, it offers the greatest security while generating a guaranteed high avalanche effect [29]. This is because GA uses independent attributes, such as crossover and mutation, which lead to a more complex and challenging mapping between the input and output. Chromosomes can be utilized as the population in GA and may be expressed as binary or hexadecimal data. A new generation is created in the crossover by applying crossover operations on members of the current generation. It is anticipated that the younger generation will be in better shape than the older one. To carry out the crossover operation, one can employ uniform crossover, random, single point, and multipoint, approaches. Furthermore, the acquisition of genetic variation in GA depends on the mutation process.

C. Substitution caesar cipher

In cryptography, the substitution cipher is essentially an encryption method that replaces the original text with ciphertext[30]. The replacement of individual characters is done on its own. One way to illustrate basic substitution is to write every letter of the alphabet in a specific order to represent the substitution. This alphabet is referred to as a substitute. The term "combined" or "deranged" refers to an extremely complex scrambling, reversal, or shifting of the cipher alphabet[30][31]. The text is ciphered again using Caesar crypt after substitution

cipher has been applied. Caesar cipher receives the output of substitution cipher. Each character in the original text is moved to a specific location in the alphabet in this type of substitution cipher. For example, if we were to shift one, A would change into B, B would ultimately become C, and it would continue. A key is employed in the Caesar cipher to change the message. The number of letters by which the alphabet for the cipher is shifted, as indicated by equation (1), is all that is needed in this case to determine the key.

$$e\,(x)\ =\ (x\ +\ k)\,(mod26) \qquad (1)$$

where x is the plaintext and k is the shift key for each letter.It is possible to express the decryption function as given in equation (2).

$$d\,(x)\ =(x-k)\ \ (mod\ 26) \qquad (2)$$

D. Advaced Encryption Standerd

AES is currently a top choice for guaranteeing the security of digital systems. The main data security standard utilized by cloud and Internet of Things services is AES. Because of its ease of use and quick processing, it is one of the greatest solutions now available for encrypting large data chunks that are processed, stored, and delivered via the cloud[32]. The AES algorithm was selected as the standard encryption technique by the US National Institute of Standards and Technologies (NIST) in 2001 (Federal Information). AES does not employ the Feistel network in contrast to DES. The same key used in the AES approach can be used to both encrypt and decode sensitive data. When meaningful data is encrypted and turned into cipher text an unintelligible format that needs the AES key to decode it can be decrypted and returned to plaintext, or its original meaning.

To satisfy cloud requirements, AES provides the benefits of various design options and topologies along with true security. It is necessary to carefully apply the architectural security provided by AES[33].

AES is a 32-bit block encryption that encrypts and decrypts data in numerous rounds using simple text which is 16 bytes (128 bits) in size. This cryptographic method can provide security with different key lengths of 128, 192, and 256 bits.The steps involved in the AES are as follows:

•**SubBytes or Byte Substitution**: Every byte is traded from one different byte to another at this point. The S-box is a reference table that is used in this process. A byte is never replaced by the same byte or by a byte which complements the existing one because of the way the substitution is carried out. This process produces a 16-byte matrix.

•**Shiftrows**: Everything about this process happens exactly as it should. There are allotted number of shifts for every row. The first row doesn't change, but the second, third, and fourth rows all move left once, twice, and three times, respectively.

• **MixColumns**: In this step, a matrix multiplication is carried out on each column, modifying the byte positions in each column by multiplying it with a certain matrix. It is crucial to keep in mind that this step is not included in the process's final step.

•**Addroundkey:** An XOR operation is performed on the result of the previous step using the corresponding round key. The 16-byte structure is handled as a 128-bit set of data in this context instead of being considered as a grid.

III.PROPOSED METHODOLOGY

In this work we have proposed a monitoring system for the smart agriculture by utilizing the cloud-based IoT. The monitoring system collect the sensor data and send it to the cloud server after every 2 sec. To protect against attackers, the sensor data is encrypted and then transferred to the cloud server. At first, the sensor data collected by the IoT device is encrypted using the substitution Caesar cipher. In cryptography, the substitution cipher is a mechanism for encrypting plain text by replacing it with cipher text. Following that, the ciphered data is encrypted using the Advanced Encryption Standard (AES). The cloud server collects encrypted sensor data continuously and decrypts it before transmitting it to the user. Afterward, the cloud server transfers the decrypted data to the designated user.

A. A Suggested Smart Agriculture Monitoring System

An innovative IoT-based Agriculture Monitoring System have been proposed in this section that makes use of IoT technology to create seamless communication between farmers and different nodes within the agricultural field. This system makes use of a Raspberry Pi device to get data from a DHT22 sensor [34]. This data is collected and then safely sent to the cloud server using public key encryption. Farmers can use their private key to unlock this encrypted data that they can access from the cloud. We provided temperature and humidity data from the agricultural field using the RaspController software, which acts as a medium [35][36]. Farmers may easily view this data by connecting the device's LCD display directly to their smartphone or tablet, or by using an internet-connected smartphone or tablet that has the RaspController app installed. But it's important to remember that, as Fig. 5 illustrates, using the smartphone or tablet app to access the system requires internet connectivity.

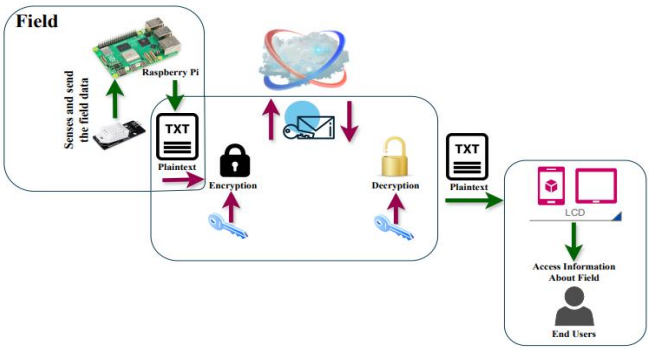

Fig. 5. Workflow of Temperature and Humidity Monitoring System

Any changes it detects in the field environment are transmitted to the Raspberry device by the sensor. The device forms these values as a single JSON object by combining them from packets when it retrieves data from the sensors. Temperature and humidity are extracted by the DHT22 sensor every two seconds. Through a designated GPIO (general-purpose input-output) port on the Raspberry Pi board, the gadget obtains the temperature and humidity values from the DHT22 sensor.

TABLE I : DHT22 SENSOR DATA

Reading	Temperature (°C)	Humidity(%)	Date &Time
1.	27.0	54.9	16-04-2024 10:03:18
2.	27.1	55.3	16-04-2024 10:03:26
3.	27.0	55.6	16-04-2024 10:03:28
4.	27.0	55.6	16-04-2024 10:03:31
5.	27.0	55.6	16-04-2024 10:03:36
6.	27.0	55.7	16-04-2024 10:03:39
7.	27.0	55.7	16-04-2024 10:03:41
8.	27.0	55.6	16-04-2024 10:03:46
9.	27.0	55.6	16-04-2024 10:03:49
10.	26.9	55.6	16-04-2024 10:03:51

B. Data Security

The conceptual and architecture workflow of the proposed model are given in this section. The data collected by the DHT22 sensor is transmitted to the cloud server [37]. Making sure that this data transfer is secure is crucial. In the proposed security approach, the initial data value from the sensor is encrypted using the Caesar cipher

technique, followed by a conversion of each character into an 8-bit binary representation to complete the first level of encryption.A 128-bit random key is created using GA, and the intended binary data is encrypted using the AES via this random key.The steps for key generation, data encryption, and decryption are outlined next.

• ***Key generation*:** The starting population of chromosomes is a sequence of letters that includes alphanumeric and special characters created using a random method. The starting population is set at a size of 200 individuals, with each individual having a chromosomal length of 16 characters, which is encoded as 128 bits. Each individual is sequentially passed through the fitness function using a loop. The fitness function is a maximization function, indicating that the individual with the highest fitness value will be chosen for further processing. Following this procedure, choose two persons and execute a byte-wise one-point crossover; the crossover point is determined by a random number. After executing the crossover operation, obtain the progeny resulting from the selected individuals. Subsequently, the result obtained from the preceding step is employed as the input for the mutation procedure. Following the mutation, the encryption mechanism utilizes the resulting key as the final key. The process of generating a key involves the following phases.

Initial population generation: The random function is utilized to create the initial population, which consists of 200 chromosomes. Each chromosome is composed of 16 characters, including alphanumeric and special characters. These characters are encoded using 8 bits per character, resulting in each chromosome being 128 bits long.

Fitness calculation: The fitness value of each individual is determined by computing the Shannon Entropy (H(X)). Eq.3 is utilized to measure the level of randomness in the final population compared to the initial population in a set of data.

$$H(X) = -\sum_{i=1}^{n} P(x_i)\, log_2 P(x_i) \qquad (3)$$

where the letter P stands for the probability of each character being present in the chromosome that was measured. Higher entropy means more difficult to crack.

Crossover: The process of byte-wise single-point crossover involves selecting two chromosomes, each with a length of 128-bits, as parents. A random value between 1 and 8 is then created for each byte, and this value is utilized to complete the crossover operation. The result of this procedure is an offspring chromosome.

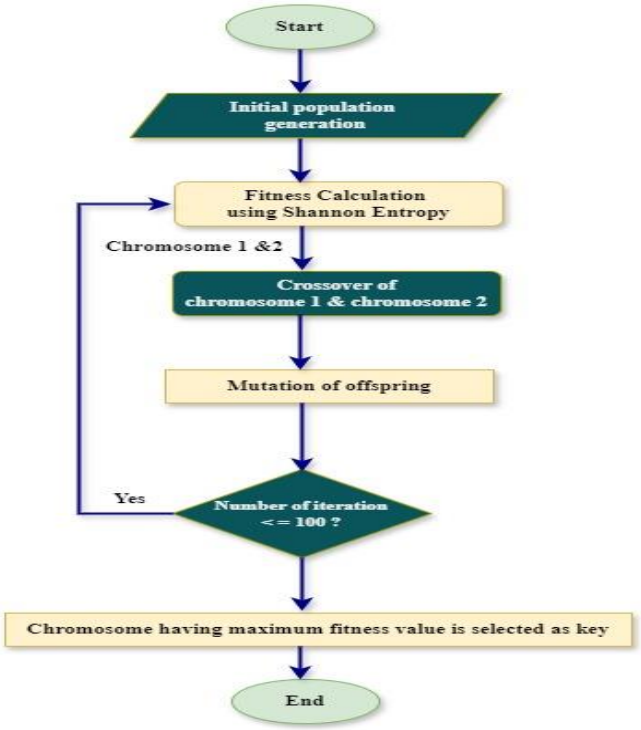

Fig. 6. Flow chart of key genetaion using GA

Mutation: The byte-wise mutation is applied to the recently created offspring chromosome using a randomly generated value within the range of 1 to 8.

The mentioned stages are executed repeatedly until the stopping requirement is met, specifically when the number of iterations is fewer than or equal to 100. During each iteration, the individual with the highest fitness value is recorded. When the stopping condition is satisfied, the chromosome with the highest fitness value is chosen as the encryption key. Figure 6 depicts the sequence diagram of the key generation process with GA.

- ***Encryption and decryption****:* A two-step encryption procedure is utilized to ensure the confidentiality and integrity of sensor data during transmission. Firstly, the sensor values are encrypted using the substitution Caesar cipher, which involves substituting each character value with another value determined by a random shift in position. Subsequently, the ciphered text is encrypted by employing the AES algorithm before it send to the cloud.

AES divides the ciphered message M from the substitution Caesar cipherinto n numbers of blocks, with each block being 128 bits long as defined by equation 4. These blocks are identified as b1, b2, b3, ..., bn. If necessary, add zeros to the last block. If the message M is an empty string, no further blocks will be appended throughout this operation.

$$M = \sum_{i=1}^{n} b_i \qquad (4)$$

In the specified process, every block undergoes transformation of a 4x4 matrix before being encrypted or decrypted utilizing the AES algorithm. Figure 7 represent this procedure and illustrating the key phases involved in securing the data. Implementing this method is crucial for protecting data, ensuring both its confidentiality and integrity are maintained effectively.

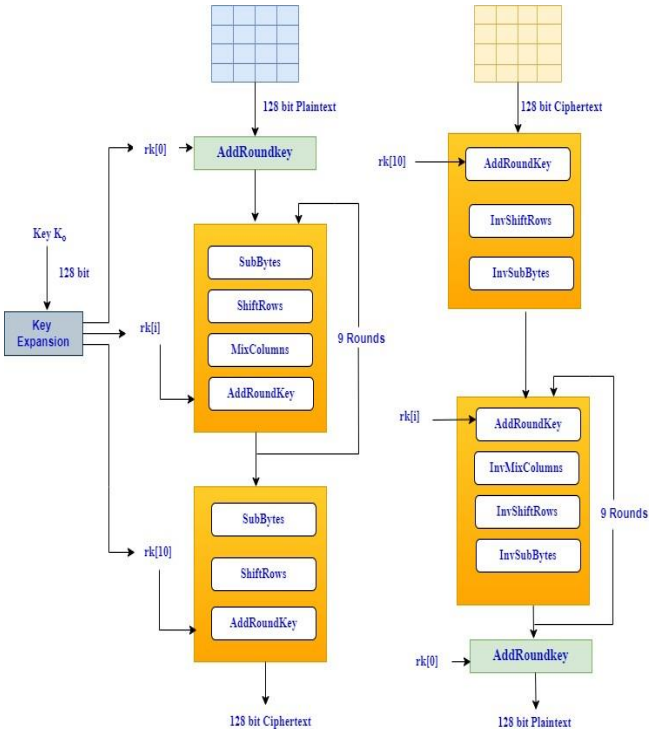

Fig.7. Encryption and Decryption through AES

C. Raspberry Pi and End User Connection

One of the most important steps in guaranteeing system security and integrity is the authentication of Raspberry Pis for unique identity[38]. A flexible single-board computer, Raspberry Pi can be used for a wide range of tasks, from industrial control systems to home automation. Cryptographic keys or hardware-based serial numbers are examples of unique identifiers that can be used to create a strong authentication system. This keeps unauthorized access and tampering at bay by guaranteeing that every Raspberry Pi device is uniquely recognized. The security status of Raspberry Pi deployments is improved when secure authentication techniques, like SSH keys, are used [39][40] as shown in figure 8. Administrators can strengthen the entire system's resilience against possible threats

by putting these precautions in place to protect sensitive data and services that are operated by Raspberry Pi device.

The stages listed below are part of the authentication process:

Step I:Turn on your Raspberry Pi and boot it up using the Raspbian operating system.

Step II:Use the subsequent command in the command prompt to configure SSH:

sudo apt update

sudo apt install openssh-server

Step III*:* Open the Raspberry configuration window, select the "Interfaces" tab, and turn on the SSH option. SSH is the method RaspController uses to connect to the Raspberry Pi.

Step IV*:*To find the Raspberry Pi's IP address, use the command "ifconfig" into the terminal.

Step V*:*Finally, we may open the RaspController software and connect to the associated Raspberry Pi by entering its IP address, username, and password. Port 22 is the SSH port by default.

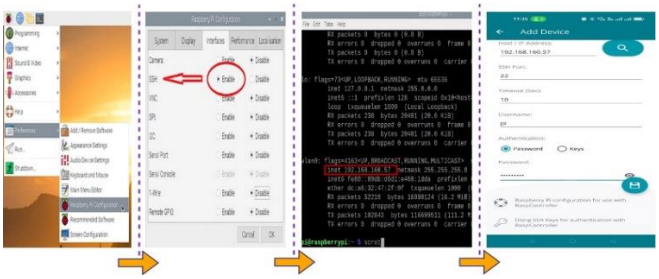

Fig. 8: Raspberry Pi authentication and connection scenario

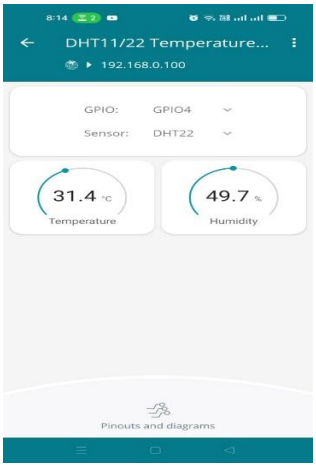

Fig. 9: Snapshot of raspcontroller app measuring temprature and humidity

IV. EXPERIMENTAL RESULT

The Raspberry Pi 4 Model B is the single-board computer that makes up our experimental arrangement. This small device has a powerful quad-core 1.4GHz 64-bit Cortex A-72 processor, 4GB of RAM, and Linux running on it. Using a DHT22 sensor, this Raspberry Pi microcontroller gathers temperature and humidity data, which is then safely sent to the cloud server via secured hybrid algorithm. This encrypted data is accessible to users via the cloud, where they can use secret key to decrypt it [41[[42].

TABLE II: NUMBER OF USER IN EXPERIMENT WITH SENSOR DATA

Symbol	Description	Data size
U1	Data is share to 1 number of User	81 bytes
U2	Data is share to 2 number of Users	81 bytes

U3	Data is share to 3 number of Users	81 bytes
U4	Data is share to 4 number of Users	81 bytes
U5	Data is share to 5 number of Users	81 bytes

The experiment is performed 500 times for each number of users to demonstrate the validity and accuracy of the results. The average time is then calculated and taken into account for a fair comparison. The throughput efficiency for encryption and decryption is measured in bytes per second, the execution time for each experiment is measured in milliseconds, and the efficiency of the hybrid method relative to other algorithms is estimated in percentage terms for consistency and readability [43]. In a cloud-based Internet of Things, some cutting-edge algorithms like ECC, DES, Blowfish, and RSA, function effectively. Thus, for the sake of comparison, these algorithms have been chosen.

A. Encryption Time Analysis

The average encryption time for several users' sensor data is displayed in Figure 10.

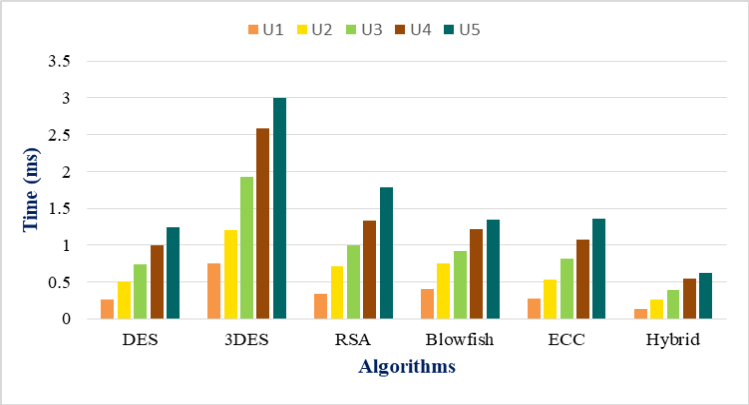

Fig. 10: Comarision of Encryption time

According to their results analysis, all users require less time when using the suggested hybrid algorithm when compared to other methods[44]. Figure 11 illustrates the encryption time's cumulative improvement efficiency. The suggested hybrid approach outperforms DES by 47.86%, Blowfish by 57.91%, ECC by 51.81%, 3DES by 79.39%, and RSA by 62.22%, according to the findings analysis of Figure 11.

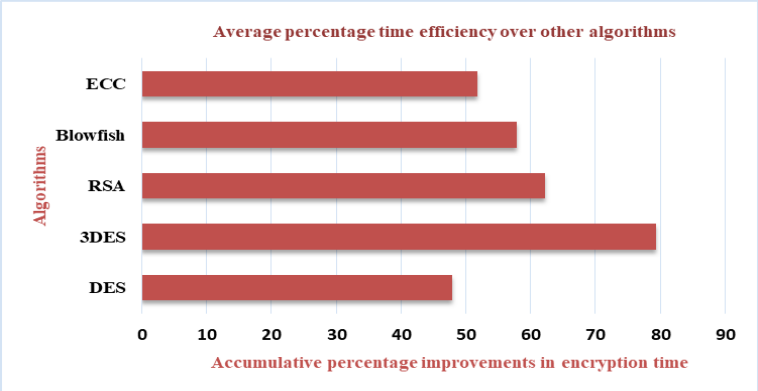

Fig. 11: The typical percentage improvement in encryption speed of hybrid model

B. Decryption Time Analysis

The average decryption time of sensor data for numerous users is displayed in Figures 12.

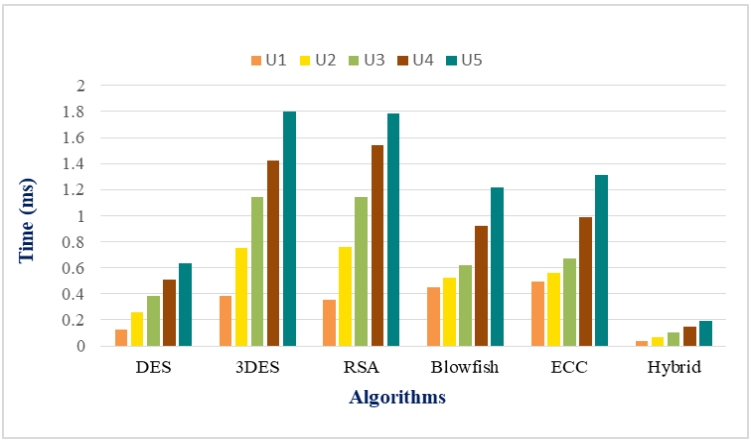

Fig. 12: Comarision of Decryption time

Their study of the results reveals that, in comparison to previous methods, the suggested hybrid method requires less time on all datasets. Figure 13 displays the progressive improved efficiency in decryption time. According to the data, the suggested hybrid model outperforms ECC by 86.33%, Blowfish by 85.22%,DES by 71.22%, 3DES by 89.98%, and RSA by 90.14%.

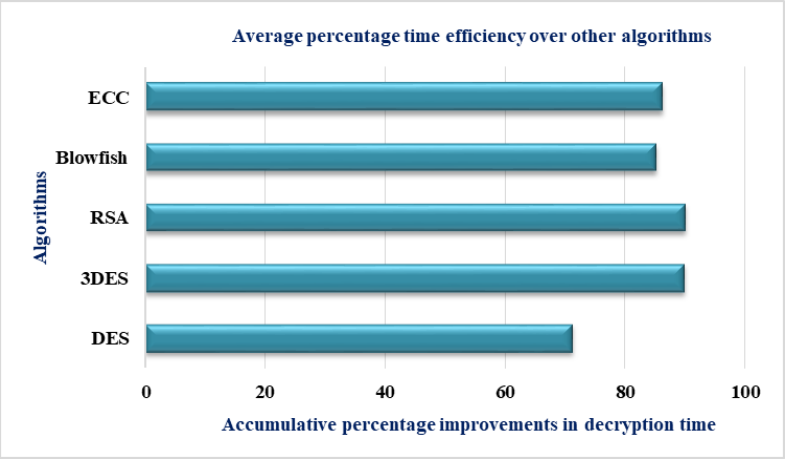

Fig. 13: The typical percentage improvement in decryption speed of hybrid model

C. Throughput Efficiency

The throughput efficiency of encryption of several algorithms and the suggested hybrid model is shown in Figure 14. The analysis demonstrates that the suggested method has a higher throughput efficiency than the others.

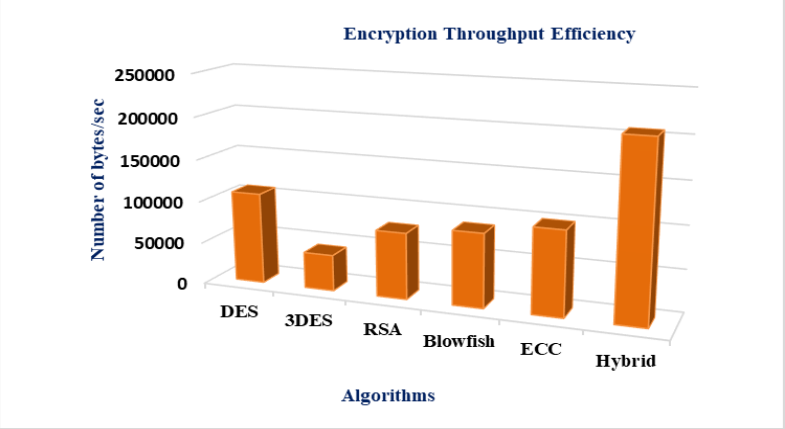

Fig. 14: Encryption throughput efficiency

Figure 15 shows the throughput efficiency of decryption of the proposed hybrid model and other techniques. The analysis demonstrates that the proposed model has a higher throughput efficiency compared to the other models [45].

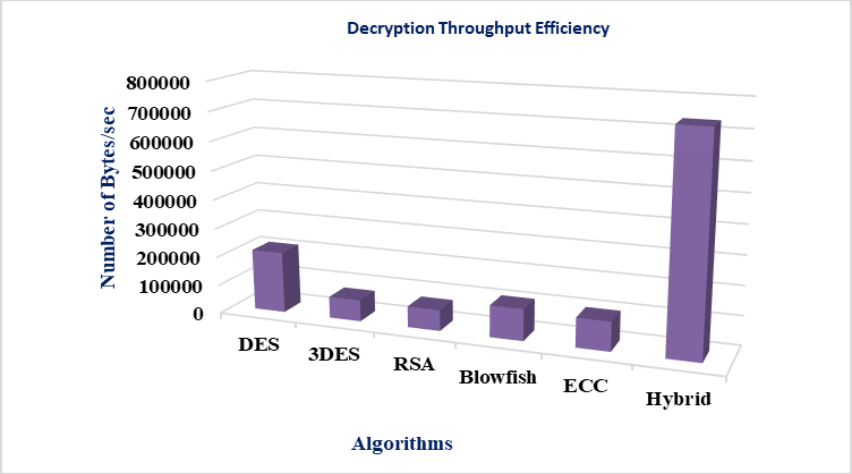

Fig. 15: Decryption throughput efficiency

D. Avalanche Effect Analysis

Eq. 5 is used to determine the differences between plaintext and ciphertext to estimate the avalanche effect. The suggested model has a significant avalanche effect across ten distinct datasets, as depicted in Figure 16.

$$A = \frac{\sum_{i=1}^{n} C_2 - \sum_{i=1}^{n} C_1}{\sum_{i=1}^{n} C_1} \qquad (5)$$

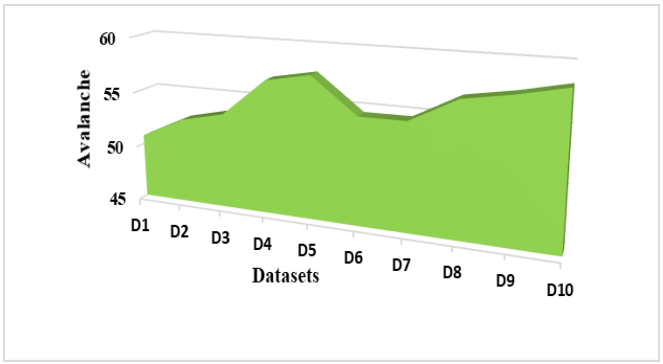

Fig. 16: Avalanche effect analysis

V. CONCLUSION

In summary, our study has successfully implemented an innovative IoT-based system for monitoring temperature and humidity using the Raspberry Pi 4 Model B. By incorporating a DHT22 sensor for data collection and a robust cryptographic mechanism, we ensure the secure transmission and storage of vital sensor data in the cloud. Our findings demonstrate that the monitoring system effectively records environmental temperature and humidity every 2 seconds, as evidenced by the RaspController application on a smartphone. Additionally, users can conveniently access sensor data on an LCD display connected directly to the device when internet connectivity is unavailable.The evaluation of the cryptographic system showed promising results across key parameters, confirming its efficiency and security features. The fast key generation process allows for quick adaptation to changing security requirements, enabling rapid system deployment. Additionally, the encryption and decryption operations exhibited good speed and used moderate memory, which are vital in agricultural settings with limited resources. The throughput of 1.1140 KB/s indicates the system's responsiveness, leading to improved efficiency in handling data encryption and decryption tasks. The avalanche effect, measured at 59%, demonstrates the algorithm's strength in magnifying the impact of input changes, thus enhancing the overall security of the cryptographic scheme.

Declarations

Conflicts of interest: The authors declare that they have no conflicts of interest.

Data availability: The data that support the findings of this study are generated from real-time environmental sensors.

REFERENCES

[1] Ayaz, Muhammad, et al. "Internet-of-Things (IoT)-based smart agriculture: Toward making the fields talk." IEEE access 7 (2019): 129551-129583.

[2] Raj, Meghna, et al. "A survey on the role of Internet of Things for adopting and promoting Agriculture 4.0." Journal of Network and Computer Applications 187 (2021): 103107.

[3] Madushanki, AA Raneesha, et al. "Adoption of the Internet of Things (IoT) in agriculture and smart farming towards urban greening: A review." International Journal of Advanced Computer Science and Applications 10.4 (2019): 11-28.

[4] Khan, Nawab, et al. "Current progress and future prospects of agriculture technology: Gateway to sustainable agriculture." Sustainability 13.9 (2021): 4883.

[5] Jamshed, Muhammad Ali, et al. "Challenges, applications, and future of wireless sensors in Internet of Things: A review." IEEE Sensors Journal 22.6 (2022): 5482-5494.

[6] Dhanaraju, Muthumanickam, et al. "Smart farming: Internet of Things (IoT)-based sustainable agriculture." Agriculture 12.10 (2022): 1745.

[7] Parween, Saria, Rasha Subhi Hameed, and Keshav Sinha. "IoT and Its Real-Time Application in Agriculture." Handbook of Research on Knowledge and Organization Systems in Library and Information Science. IGI Global, 2021. 103-123.

[8] Abu, N. S., et al. "Internet of things applications in precision agriculture: A review." Journal of Robotics and Control (JRC) 3.3 (2022): 338-347.

[9] Wójcicki, Krzysztof, et al. "Internet of things in industry: research profiling, application, challenges and opportunities—a review." Energies 15.5 (2022): 1806.

[10] Chanal, Poornima M., and Mahabaleshwar S. Kakkasageri. "Security and privacy in IoT: a survey." Wireless PersonalCommunications 115.2 (2020): 1667-1693.

[11] Mousavi, Seyyed Keyvan, et al. "Improving the security of internet of things using cryptographic algorithms: a case of smart irrigation systems." Journal of Ambient Intelligence and Humanized Computing 12.2 (2021): 2033-2051.

[12] Medileh, Saci, et al. "A flexible encryption technique for the internet of things environment." Ad Hoc Networks 106 (2020): 102240.

[13] Mousavi, Seyyed Keyvan, et al. "Security of internet of things based on cryptographic algorithms: a survey." Wireless Networks 27.2 (2021): 1515-1555.

[14] Liu, Shubo, et al. "Internet of Things monitoring system of modern eco-agriculture based on cloud computing." Ieee Access 7 (2019): 37050-37058.

[15] HaddadPajouh, Hamed, et al. "A survey on internet of things security: Requirements, challenges, and solutions." Internet of Things 14 (2021): 100129.

[16] Marques, Gonçalo, et al. "Internet of things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: a review." Electronics 8.10 (2019): 1081.

[17] Ali, Salman, and Faisal Anwer. "Secure IoT framework for authentication and confidentiality using hybrid cryptographic schemes." International Journal of Information Technology (2024): 1-15.

[18] Rehman, Saba, et al. "Hybrid AES-ECC model for the security of data over cloud storage." Electronics 10.21 (2021): 2673.

[19] Thakur, Divyansh, et al. "Applicability of wireless sensor networks in precision agriculture: A review." Wireless Personal Communications 107 (2019): 471-512.

[20] Rehman, Amjad, et al. "A revisit of internet of things technologies for monitoring and control strategies in smart agriculture." Agronomy 12.1 (2022): 127.

[21] Subahi, Ahmad F., and Kheir Eddine Bouazza. "An intelligent IoT-based system design for controlling and monitoring greenhouse temperature." IEEE Access 8 (2020): 125488-125500.

[22] Rao, R. Nageswara, and B. Sridhar. "IoT based smart crop-field monitoring and automation irrigation system." 2018 2nd International Conference on Inventive Systems and Control (ICISC). IEEE, 2018.

[23] Math, Anushree, Layak Ali, and U. Pruthviraj. "Development of smart drip irrigation system using IoT." 2018 IEEE Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER). IEEE, 2018.

[24] García, Laura, et al. "IoT-based smart irrigation systems: An overview on the recent trends on sensors and IoT systems for irrigation in precision agriculture." Sensors 20.4 (2020): 1042.

[25] Sinha, Bam Bahadur, and R. Dhanalakshmi. "Recent advancements and challenges of Internet of Things in smart agriculture: A survey." Future Generation Computer Systems 126 (2022): 169-184.

[26] Mrabet, Hichem, et al. "A survey of IoT security based on a layered architecture of sensing and data analysis." Sensors 20.13 (2020): 3625.
[27] Saiz-Rubio, Verónica, and Francisco Rovira-Más. "From smart farming towards agriculture 5.0: A review on crop data management." Agronomy 10.2 (2020): 207.
[28] Hassanat, Ahmad, et al. "Choosing mutation and crossover ratios for genetic algorithms—a review with a new dynamic approach." Information 10.12 (2019): 390.
[29] Thabit, Fursan, Sharaf Alhomdy, and Sudhir Jagtap. "A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions." International Journal of Intelligent Networks 2 (2021): 18-33.
[30] Shareef, Farah R. "A novel crypto technique based ciphertext shifting." Egyptian Informatics Journal 21.2 (2020): 83-90.
[31] Khan, Mohammad Ayoub, et al. "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data." IEEE Access 8 (2020): 52018-52027.
[32] Wright, Marie A. "The advanced encryption standard." Network Security 2001.10 (2001): 11-13.
[33] Swann, Ryan, and James Stine. "Evaluation of a Modular Approach to AES Hardware Architecture and Optimization." Journal of Signal Processing Systems 95.7 (2023): 797-813.
[34] Muhammad, Zuraida, et al. "Smart agriculture using internet of things with Raspberry Pi." 2020 10th IEEE International Conference on Control System, Computing and Engineering (ICCSCE). IEEE, 2020.
[35] Lean, Chong Peng, et al. "A Raspberry Pi-Powered IoT Smart Farming System for Efficient Water Irrigation and Crop Monitoring." Malaysian Journal of Science and Advanced Technology (2024): 149-158.
[36] Muhammad, Zuraida, et al. "Smart agriculture using internet of things with Raspberry Pi." 2020 10th IEEE International Conference on Control System, Computing and Engineering (ICCSCE). IEEE, 2020.
[37] Mohapatra, Debashish, and Bidyadhar Subudhi. "Development of a cost-effective IoT-based weather monitoring system." IEEE Consumer Electronics Magazine 11.5 (2022): 81-86.
[38] Hasan, Md Rakib, et al. "Reliable identity management system using Raspberry Pi." 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI). IEEE, 2020.
[39] Fei, Wen, Hiroyuki Ohno, and Srinivas Sampalli. "Design and implementation of raspberry house: an IoT security framework." 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS). IEEE, 2021.
[40] Arshad, Jehangir, et al. "Deployment of an intelligent and secure cattle health monitoring system." Egyptian Informatics Journal 24.2 (2023): 265-275.
[41] WajdaTarannum, Shafiqul Abidin “Integration of Blockchain and Cloud Computing : A Review”, International Conference on Emerging Computational Intelligence (ICECI 2023) / 10th International Conference on Computing for Sustainable Global Development 2023. 11-12 February 2023, (Scopus – Indexed).
[42] Faisal Ahmad, Faraz Hasan, Mohammad Imran, Mohammad Shahid, Shafiqul Abidin, ”A load balancing using multi-population grasshopper optimization approach for workflow tasks in clouds”, 11th International Conference on Recent Trends in Computing, Proceedings of International Conference on Recent Trends in Computing(ICRTC 2023) .
[43] Abidin, S., Swami, A., Ramirez-Asis, W., Alvarado-Tolentino, Joseph., Maurya, R, K., Hussain, N., July, 2022. Quantum Cryptography Technique: a way to Improve Security Challenges in Mobile Cloud Computing (MCC): Materials Today: Proceedings, pp. 508-514.
[44] Vadi, VR., Abidin, Shafiqul., Khan, Azimuddin., Izhar, Mohd. August, 2022. Enhanced Elman spike neural network fostered blockchain framework espoused intrusion detection for securingInternet of Things network: Transactions on Emerging Telecommunications Technologies, John Wiley.
[45] P. S. Ramesh , P. Srivani , Miroslav Mahdal ,, Lingala Sivaranjani , Shafiqul Abidin et al”, Contextual Cluster-Based Glow-Worm Swarm Optimization (GSO) Coupled Wireless Sensor Networks for Smart Cities”, Sensors, MDPI, pp 1-26 , July 2023.