International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2090
***Article Received**: 24 December 2021 **Revised**: 16 February 2022 **Accepted**: 22 February 2022 **Publication**: 31 March 2022*

Research on Smart Environment Monitoring Systems based on Secure Internet of Things (IoT)

Dr. Anasica S
MGM Department,
The Free University of Berlin, Germany
anasica.s@ubingec.ac.in

Abstract
Significant environmental threats include poor air quality, water contamination, and radiation pollution. A healthy society must be maintained for the planet to experience sustained growth. Environmental monitoring has transformed into smart environment monitoring (SEM) systems in recent years due to the growth of an internet of things (IoT). The Internet of Things (IoT) concept has developed into technology for creating smart environments and also has its disadvantage. To collect, evaluate, and recommend specific actions in smart environments for various purposes, a secure IoT-based platform is proposed. The proposed method follows the flow outlined here: data collection, normalization technique is used for data preprocessing, Linear Discriminant Analysis (LDA) is used for feature extraction, then data stored in IoT, Advanced Twofish encryption algorithm is proposed for securing the data, then user decryption, and finally performance is analyzed for smart environment monitoring using secure IoT. The proposed work aims to complete a critical evaluation of significant contributions to SEM that focus on the monitoring of water quality, air quality, radiation contamination, and agricultural systems. Secure IoT is based on the optimal integration and use of data gathered from several sources. This algorithm provides smart environment monitoring and also exhibits optimal integration.

Keywords: Smart Environment Monitoring (SEM), Internet of Things (IoT), Secure IoT, Linear Discriminant Analysis (LDA), Advanced Twofish encryption algorithm, Optimal integration.

I. INTRODUCTION

Environment monitoring (EM) includes preparing for and responding to natural and man-made disasters, limiting the spread of pollution, and overcoming obstacles brought on by unfavorable environmental conditions. Water pollutants, air pollution, hazardous radiation, weather fluctuations, and earthquakes are just a few of the environmental issues that are monitored via environmental monitoring (EM). It is the goal of environmental management (EM) to accurately handle problems to maintain a healthy environment for the benefit of a healthy human society and planet. Pollution comes from a variety of sources, some of that is caused by man and others by nature. Studies are also published on the development of standards and protocols for the Internet of Things-based SEM systems because they are crucial for the efficient implementation of smart environment monitoring (SEM) systems when wireless gadgets are utilized over a wireless sensor network (WSN), (Ullo and Sinha (2020)). The monitoring of environmental conditions involves the gathering of relevant data and information. The quality of the environment suffers as a result of industrial pollution. Therefore, anyone can estimate the short- and long-term effects of industrial initiatives on the ecosystem in a given area by monitoring environmental factors. Public health expert groups, corporations, and government agencies can all use this data to better prepare for and respond to environmental crises. When applied to things with network connectivity and computational capabilities, the Internet of Things (IoT) can be very helpful, (Tiwari et al. (2018)).

A smart environment is one in which various sensors, actuators, computation, and data exchanging devices are all seamlessly interconnected. High-quality, convenient, and adaptable services are made possible by such a setting. Real-world changes result from a smart environment. The specific characteristics of the smart environment, such as its ubiquitousness, invisibility, sense, or memory amplification, promote positive cultural transformations. The node in a wireless sensor and actuator networks (WSAN), Internet for Vehicles (IoV), Internet - Of - things (IoT), and other smart environments (smart

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2090
***Article Received**: 24 December 2021 **Revised**: 16 February 2022 **Accepted**: 22 February 2022 **Publication**: 31 March 2022*

households, smart buildings, hospitals, offices, and smart cities), etc., (Hussain and Jain (2020)). (Rugger et al. (2020)) IoT devices, including low-power sensors, actuators, smartphones, tablets, and robots, can't be connected using current communication protocols because they are often battery-powered and resource-constrained. These devices, when widely dispersed throughout the environment, might produce vast volumes of data, provide computational resources, and work together to do some activities locally while delegating others to more capable nodes. The introduction of new Internet of Things (IoT) devices into a smart environment calls for robust, scalable management platforms capable of dynamically discovering, integrating, and orchestrating these devices. Security services, such as authentication & data integrity, need the development of new, lightweight protocols. Figure 1 shows the IoT-based smart environment.

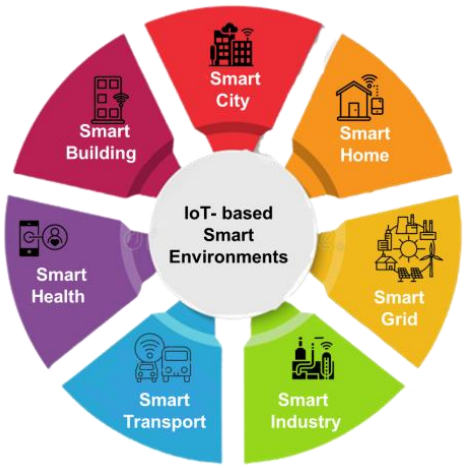

Figure 1. IoT-based smart environment

Bringing commonplace items online is the basis of the Internet of Things (IoT), a new computer and communications paradigm. The Internet of Things (IoT) has many advantages, including better management of scarce resources, higher output per worker, and a higher general standard of living. That's why the Internet of Things is crucial to the development of "smart" surroundings like "smart homes," "smart hospitals," "smart cities," and "smart factories," among many others. In fact, the shift toward smart-x holds the potential to revolutionize many facets of human life, (Gomez et al. (2019)). The issues of scientific significance in environmental monitoring include flexibility, representativeness, and integration of monitoring systems, as well as risk assessment.

Hence in this paper, the research on smart environment monitoring systems based on the secure internet of things was described. The further part of this article is categorized as follows: Part II provides the related works and problem statement; Part III explains the proposed method; Part IV explains the performance analysis; Part V explains the conclusion.

II. RELATED WORKS

(Hajjaji et al. (2021)) analyzed how big data and IoT are used in the modern smart environment. The goal is to uncover significant applications, emerging tendencies, data architectures, and pressing problems in these domains. The findings point to promising new avenues for implementing smart environment applications in the real world for monitoring, protecting, and bettering our planet's natural resources. (Nandanwar and Chauhan (2021)) proposed and analyzed in this article for reducing noise and air pollution. The method is particularly attractive because it relies solely on IoT to reduce pollution. With this setup, they can occasionally identify levels of air or noise pollution. The article delves into the various components, both hardware, and software, that make up the proposed system, and explains how the Internet of Things (IoT) functions, as well as how the Microcontroller (Arduino Uno R3), its architecture, gas sensor, & features are modeling and working with these fundamental elements. (Kumar (2020)) provided a summary of the deep ecological interface for environmental governance and management, as well as a description of the integrated method to a smart environment of the smart city. Vedic and Buddhist religious practices from multiple Asian countries are used to illustrate how faith-based smart living may bolster the Smart Environments for Smart City strategy. (Elmustafa and Mujtaba (2019)) presented a high-level overview of how the Internet of Things (IoT) technology might be applied to various environmental research fields, and will explore the rationale for applying IoT to environmental research. Furthermore, they will look into a wide range of suggested IoT-based environmental research applications. (Haji and Sallow (2021)) examined the most significant contributions to air pollution, water contamination, radiation contamination, & agricultural system monitoring made by smart environments monitoring (SEM) research. SEM techniques were used in this study to achieve a variety of objectives, and the results of sensor analysis, machine learning, & classification methods were presented for each of those objectives. (Malche et al. (2019)) proposed IoT-

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2090
***Article Received**: 24 December 2021 **Revised**: 16 February 2022 **Accepted**: 22 February 2022 **Publication**: 31 March 2022*

oriented environment monitoring and warning system proposed here. The proposed system keeps track of air quality and pollutants in a specific area while also allowing for safe data transmissions via a network to address IoT security issues. Figure 2 represents the environment monitoring with the internet of things.

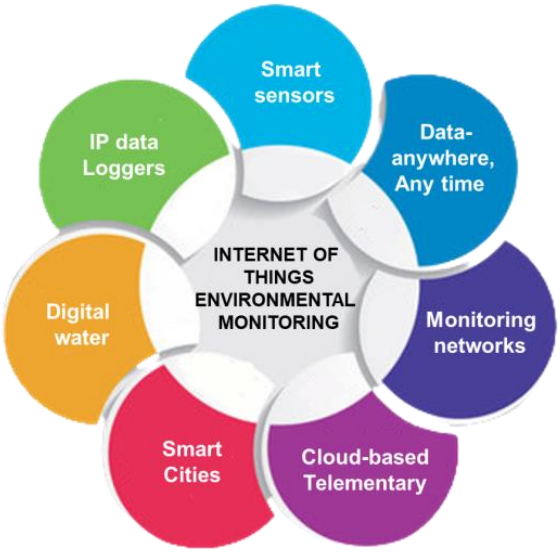

Figure 2. Environment monitoring with IoT

Networks of autonomous objects in real-time systems can be built using sensors and actuators to establish a reliable foundation for environment monitoring (EM). The Internet of Things (IoT) is rapidly expanding across the world's smart cities, daily life, and many industries. The Internet of Things (IoT) helps create smart environments by facilitating the development of technologies like home automation, wearable technology, surveillance system, and smart healthcare. (Shinde et al. (2018)) presented the infrastructure of an IoT system for environmental monitoring in both indoor and outdoor settings. Specifically, there are two sensor nodes and a gateway. Every so often, the gateway will collect data from the sensor node and upload it to the cloud, where they can access it, evaluate it, and make judgments. (Khan et al. (2019)) described an inexpensive and dependable Internet of Things (IoT) based system of remote sensing of CO_2, CO, methane, dust particulates, precipitation, temperature, and humidity. The suggested system is useful for geo-referencing the collecting, processing, and analysis of data on traffic-related pollution near roadways and how it affects the quality of life in Smart Cities. (Assante and Fornaro (2019)) explored the creation of an Internet of Things-based indoor environmental monitoring system. Students may manage the network's sensors, nodes, and configuration settings, as well as work with a variety of sensor and controller types, evaluate raw data and do post-processing from a distant location using the monitoring system. (Lashari et al. (2018)) used IoT technology to secure and monitor a poultry farm's surroundings. The suggested hardware and software system can track environmental factors like temperature, humidity, oxygen and carbon monoxide levels, and ammonia emissions. Saini, et al. (2022) provided a comprehensive analysis of how far Internet of Things-based air quality monitoring devices have come. This report summarises the research conducted over the past five years on monitoring system design, focusing on sensor types, microcontrollers, architectures, and connections, as well as implementation challenges.

Problem statement

Multiple environmental monitoring concerns, including humidity, temperatures, radiation, dust, UV signal, and more, are being addressed by the IoT system. A WSN serves as the system's backbone, acting as the actual interface among Internet of Things devices and data gathered via various smart sensors. While sensors, WSNs, and the Internet of Things have all been used to monitor the environment, there have been problems with cost, coverage, and installation.

III. PROPOSED METHODOLOGY

This part outlines the proposed procedure's overall flow. The schematic representations of a suggested technique include the processes like data collection, data preprocessing using normalization, feature extraction using linear discriminant analysis, secure IoT using an advanced twofish encryption algorithm, and user decryption.

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2090
Article Received: 24 December 2021 Revised: 16 February 2022 Accepted: 22 February 2022 Publication: 31 March 2022

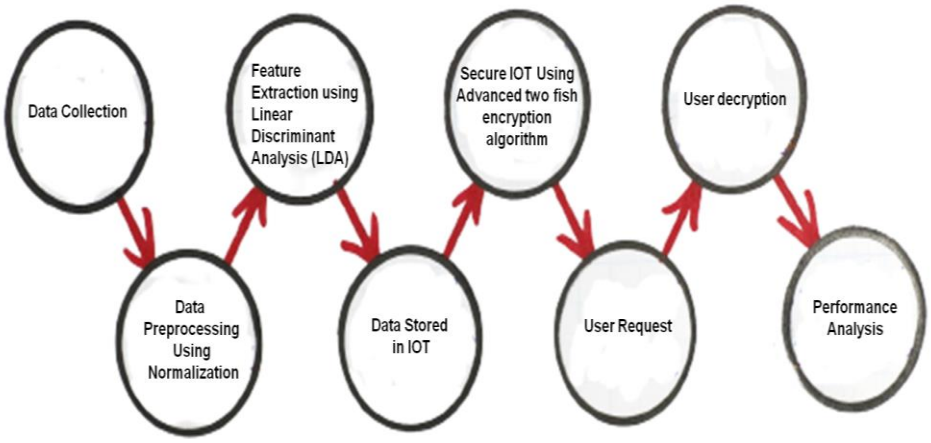

Figure 3. Flow of proposed work

A) Data collection

Two devices, buoys and hydrophones, are used by professionals to collect data for our Marine dataset. The information is then saved in the form of waveforms. Our 10,296 wave signals are now classified into 10 classes: "noise," "rain," "wind," 'humming', 'click', 'drum', 'invertebrate', & 'vessel'. To account for the environmental factor, three classes—"noise," "rain," and "wind"—depict the geophonia sound kind. In order to account for human activity, an antropophonia sound type is characterized by two classes, "vessel" and "sonar", (Belghith et al. (2018)). Table 1 shows the classes for datasets description.

Table 1. Classes for datasets Description

S.NO	Classes	Trainings	Tests	Bandwidth	Description
1.	Background noise	801	201	6 Hz-39063 Hz	After removing the individual sources of underwater noise.
2.	Rain	796	198	7000 Hz-39063 Hz	Bubbles of air make a variety of noises as they fall to the ground. Bubbles at the sea surface are caused by raindrops causing a local disturbance of the water surface.
3.	Wind	802	205	200 Hz-39064 Hz	The bubbles created by waves and the collective oscillation of the wave make sounds.
4.	Vessel	803	207	6 Hz-15001 Hz	Noise from boats with engines. Propeller cavitation, bow wave, and motorization line vibration all contribute to its creation.
5.	Sonar	805	204	2000 Hz-8000 Hz	Infrasound emissions are produced by ships.

B) Data preprocessing using normalization

Numerous methods, including Min-Max normalization, z-score normalization, decimal scaling, standardized moment, etc., can be used to normalize datasets. Min-Max & z-Score Normalization are the two widely used and popular normalization methods. Min Max technique was used for our work.

Min-Max normalization

The following equation is used in min-max normalization to normalize features in the range [0,1].

$$u' = \frac{u - min_B}{max_B - min_B} \quad (1)$$

The minimum and maximum values of feature B are shown here by min_B and max_B, respectively. The values u and u' indicate the attribute's original and

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2090
Article Received: 24 December 2021 Revised: 16 February 2022 Accepted: 22 February 2022 Publication: 31 March 2022

normalized values, respectively. The maximum and minimum feature values are transferred to 1 and 0, respectively, as can be seen from the equation above.

C) Feature extraction using linear discriminant analysis

In order to extract features, we have used linear discriminant analysis (LDA). To begin, a basic overview of LDA is in order. For each class, there is n training sample in the form of the column vector. Equations (1) and (2) are used to calculate the LDA's between and total scatter matrices.

$$S_b = \sum_{i=1}^{C} (a_i^j - a_i)(a_i^j - a_i)^T \quad (1)$$

$$S_t = \sum_{i=1}^{C} \sum_{j=1}^{n} (a_i^j - \bar{a})(a_i^j - \bar{a})^T \quad (2)$$

Where a_i^j denotes the ith class training sample with the jth training sample, $\bar{a}$ denotes the mean for all the training samples, while a_i stands for mean of a ith class.

$$S_b x = \lambda S_t x \quad (3)$$

If all of Eq. (3)'s eigenvalues are $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_N$ N... 1 2 and a corresponding eigenvectors were $X_1 \ldots X_N$. Following is a LDA eigen formula. Because of the way it works, LDA often employs the top two or three largest eigenvectors to create d-dimensional vectors out of samples. The sample vectors' dimensionality is denoted by the number N.

Dimension reduction can make use of both feature extraction & feature selection. A sample and an eigenvector of a LDA covariance matrix, respectively, are $x = [x_1 \ldots x_N]^T$ and $a = [a_1 \ldots a_N]^T$.

According to x, the outcome of a's LDA-based extracting features is,

$$z = a^T x = \sum_{i=1}^{n} a_i x_i \quad (4)$$

It is obvious that the size of $x_i (i = 1,2,..,N)$ statistically reflects the contribution of the ith component of the sample to the output of the feature extraction. It is obvious that the ith component of a sample contributes less the smaller the absolute value for x_i. Removing $a_k x_k$ $\sum_{i=1}^{N} a_i x_i$ from = N I I I an x 1 will only slightly modify the result of the feature extraction if an absolute value of x_k is small enough. This means that they can disregard the significance of the sample's kth element when x_k is of a modest absolute value. When assessing the relevance of a single component, they should consider several eigenvectors, because there are always multiple eigenvectors. Using this technique, they were able to identify the best features.

Step 1: The LDA between total scatter matrices are created using the initial training samples. Finally, the eigenvectors and eigenvalues of Eq. (3) are solved.

Step 1: They select the eigenvectors with the highest eigenvalues in the first m, designating them with the letters $V_{1,\ldots,}V_m$ in turn.

Step 3: jth component's impact on feature extraction is evaluated as follows.

$$c_j = \sum_{p=1}^{m} |V_{pj}| \quad (5)$$

where V_{pj} represents the jth element of the vector V_p, where j = 1, 2,..., N and p = 1, 2,..., m, and |a| V_{pj} denotes an absolute value of V_{pj}.

Step 4. Where j = 1, 2,..., N, they sort c_j in descending order and utilise d_j to record an order. For instance, if the original samples' sth and tth components are the first and second most significant features, respectively, among all the c_j, where j = 1, 2,..., N, then they should let $d_1 = s$ & $d_2 = t$ instead.

If n-dimensional features were required, the d_1 th, d_2 th,..., d_nth components will be the result of the feature extraction. The feature extraction data's are stored in IoT.

D) Secure IoT using advanced two fish encryption algorithm

Advanced twofish was a block cypher with a key length of 128 bits that can handle keys of arbitrary lengths. 16-round network with bijective F function and fixed 4-by-4 maximum distances separable matrices and four key dependent 8- by 8-bit S-boxes comprise the encryption. The output and input data were XORed with eight subkeys K0...K7 when utilising the advanced twofish approach. The X-OR operations performed on inputs and outputs are known as whitening. Key dependent S-boxes, Maximum Distance Separable (MDS) matrices, the Pseudo-Hadamard Transform(PHT), and a radial basis function are the five types of component operations that make up the F-function

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2090
***Article Received**: 24 December 2021 **Revised**: 16 February 2022 **Accepted**: 22 February 2022 **Publication**: 31 March 2022*

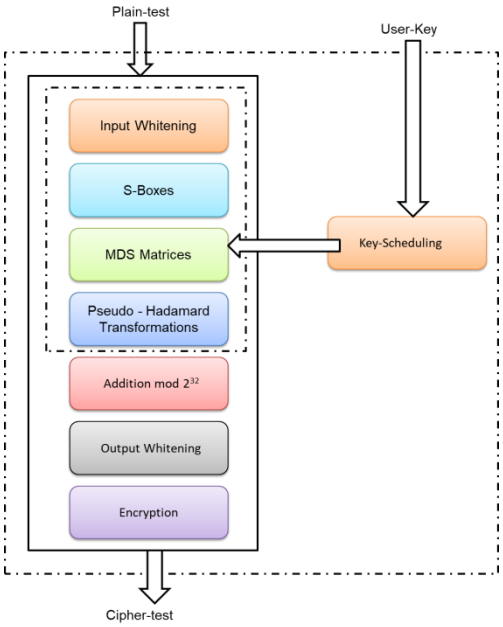

Figure 4. Advanced two fish algorithm

The eight sub K0...K7 are used to XOR the input and output data when employing the advanced twofish approach. Whitening refers to the X-OR procedures done on inputs and outputs. There are four distinct types of key-dependent S-boxes when a MDS matrix and g-function are coupled. The advanced twofish algorithm consists of 16 stages. Among the components of advanced twofish algorithms were, many algorithms make use of S-box, which is a table-driven replacement process. Its input and output sizes are both malleable and can be decided either at random or via an algorithm. The advanced twofish method employs four distinct types of s-boxes. An h-function is formed from the MDS matrix and the four distinct S-boxes. Because of the duplicate use of this h-function, the method wastes a lot of time. Each S-box in advanced Twofish is made up of two fixed permutations, q0 and q1, and three 8-by-8-bit permutations. Two sub-keys are used to conduct the XOR operation. In order to complete its calculations, the advanced twofish algorithm relies on a single Maximum Distances Separable (MDS) matrix, which is itself 4 by 4. The four bytes produced by four S-boxes are diffused mostly through the MDS Matrix. Given that MDS matrices ensure some level of dispersion, they make excellent building blocks for ciphers. The output must also vary if the input is altered. A modification to two inputs will necessitate adjustments to all but one of the outputs. One software mixing process that works relatively quickly is the pseudo-Hadamard Transform (PHT). One version of the advanced twofish encryption/decryption code was optimized for speed. The output of advanced twofish's two parallel 32-bit h -functions are mixed using a 32-bit PHT. A Feistel-like network with 16 rounds, advanced twofish is a block cypher. Directly mapping the 16-round encryption procedure into hardware would be too expensive. The 16-round loop operations are thereby collapsed into a single-round procedure. The F-function Unit executes the one-round procedure. To put it simply, advanced twofish revolves around the function h. The input and output of each S-box are both 8 bits. Using the 4x4 MDS, the four results are read as a vector of length four over GF(28). The resultant vector from h is a 32-bit word.

IV. RESULTS AND DISCUSSION

The overall behavior of the recommended framework is discussed in this section. Figures 5, 6, 7, and 8 show the comparison of parameters, like security level, encryption time, execution time, and decryption time for existing and proposed methods. For example, among the approaches that may be utilized are the advanced encryption standards (AES), elliptic curve integrated encryption schemes (ECIES), data encryption standards (DES), rivest, Shamir, and adleman (RSA) and advanced twofish encryption algorithm (ATEA).

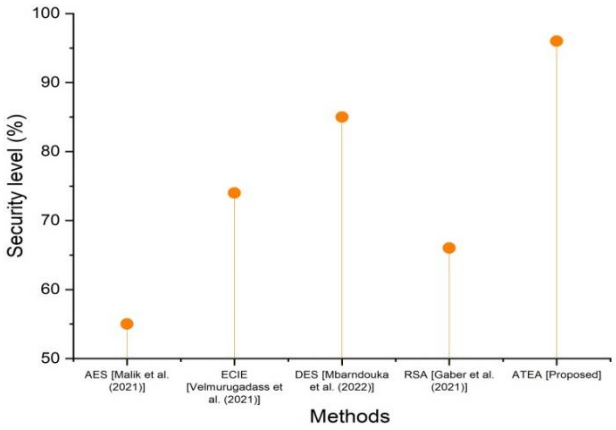

Figure 5. Security level results of proposed and existing methodology

The results of suggested and existing approaches' security level calculations are shown in Figure 5. According to the aforementioned graph, the proposed approach of advanced twofish encryption algorithm has a 96 % higher security level than the existing methods.

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2090
***Article Received**: 24 December 2021 **Revised**: 16 February 2022 **Accepted**: 22 February 2022 **Publication**: 31 March 2022*

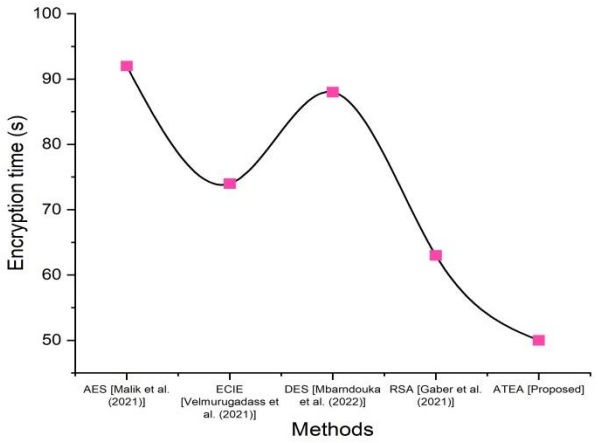

Figure 6. Encryption time results of proposed and existing methodology

Calculating the encryption process' throughput is done by dividing a total encrypted plaintext (in bytes) by the encryption time (in s). As shown in the figure 6, the suggested approach of ATEA has a lower encryption time than the existing methods.

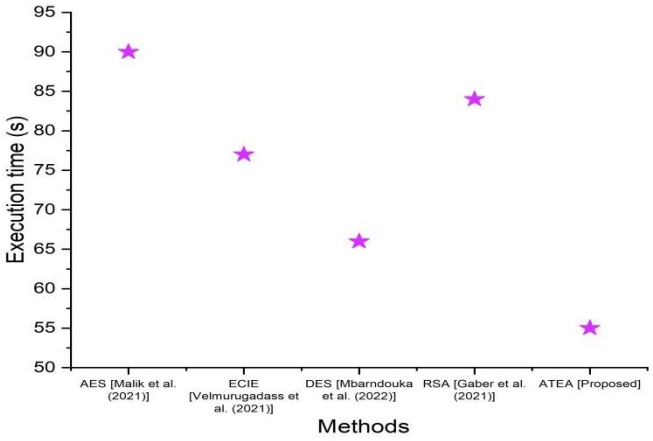

Figure 7. Execution time results of proposed and existing methodology

Figure 7 represents the execution time results with proposed and existing approaches. The above figure 7 shows that the existing methods have a high execution time when compared to the proposed method of advanced twofish encryption algorithm.

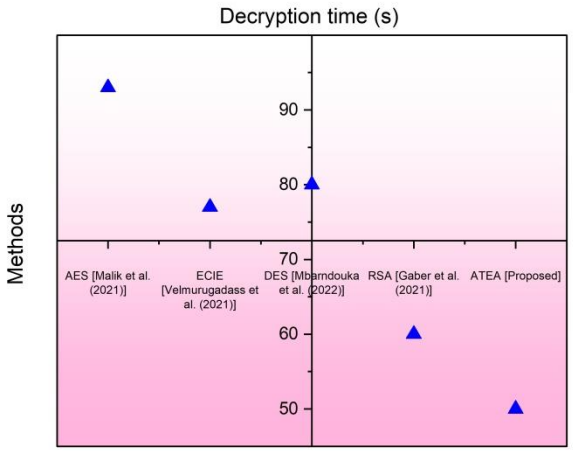

Figure 8. Decryption time results of proposed and existing methodology

Figure 8 represents the decryption time results with proposed and existing approaches. The above figure 8 shows that the proposed method of advanced twofish encrypton algorithm has a low decryption time when compared to the existing methods such as advanced encryption standard, elliptic curve integrated encryption scheme, data encryption standard, rivest Shamir adleman.

V. CONCLUSION

Monitoring the quality of the environment is the purpose of environmental monitoring systems. A smart environmental monitoring system (SEM) has emerged in recent years as the internet of things (IoT) transforms environmental monitoring. Although smart surroundings can be created using Internet of Things (IoT) idea, there is also a downside. A smart environment has two key drawbacks: low energy & low node-to-node communication bit rates. To overcome these issues, we have proposed an advanced twofish algorithm. Moreover, the results are compared to the current methods in terms of security level, execution time, encryption time, and decryption time. Sound pollution and natural disasters, for example, will be the subject of future research. Our suggested method performs better than the other methods that are presently in use.

REFERENCES

[1]. Ullo, S.L. and Sinha, G.R., 2020. Advances in smart environment monitoring systems using IoT and sensors. *Sensors*, *20*(11), p.3113.

[2]. Tiwari, A., Sadistap, S. and Mahajan, S.K., 2018. Development of environment monitoring system using

International Journal on Future Revolution in Computer Science & Communication Engineering (IJFRCSCE)
ISSN: 2454-4248 Volume: 8 Issue: 1
DOI: https://doi.org/10.17762/ijfrcsce.v8i1.2090
***Article Received**: 24 December 2021 **Revised**: 16 February 2022 **Accepted**: 22 February 2022 **Publication**: 31 March 2022*

the internet of things. In *Ambient Communications and Computer Systems* (pp. 403-412). Springer, Singapore.

[3]. Hussain, M. and Jain, U., 2020. Simple and secure device authentication mechanism for smart environments using Internet of things devices. *International Journal of Communication Systems*, *33*(16), p.e4570.

[4]. Ruggeri, G., Loscrí, V., Amadeo, M. and Calafate, C.T., 2020. The internet of things for smart environments. *Future Internet*, *12*(3), p.51.

[5]. Gomez, C., Chessa, S., Fleury, A., Roussos, G. and Preuveneers, D., 2019. Internet of Things for enabling smart environments: A technology-centric perspective. *Journal of Ambient Intelligence and Smart Environments*, *11*(1), pp.23-43.

[6]. Hajjaji, Y., Boulila, W., Farah, I.R., Romdhani, I. and Hussain, A., 2021. Big data and IoT-based applications in smart environments: A systematic review. *Computer Science Review*, *39*, p.100318.

[7]. Nandanwar, H. and Chauhan, A., 2021, August. IOT based Smart Environment Monitoring Systems: A Key To Smart and Clean Urban Living Spaces. In *2021 Asian Conference on Innovation in Technology (ASIANCON)* (pp. 1-9). IEEE.

[8]. Kumar, V., 2020. Smart environment for smart cities. In *Smart Environment for Smart Cities* (pp. 1-53). Springer, Singapore.

[9]. Elmustafa, S.A.A. and Mujtaba, E.Y., 2019. Internet of things in smart environment: Concept, applications, challenges, and future directions. *World Scientific News*, *134*(1), pp.1-51.

[10]. Haji, S.H. and Sallow, A.B., 2021. IoT for smart environment monitoring based on Python: a review. *Asian Journal of Research in Computer Science*, *9*(1), pp.57-70.

[11]. Malche, T., Maheshwary, P. and Kumar, R., 2019. Environmental monitoring system for smart city based on secure Internet of Things (IoT) architecture. *Wireless Personal Communications*, *107*(4), pp.2143-2172.

[12]. Shinde, V.R., Tasgaonkar, P.P. and Garg, R.D., 2018, August. Environment monitoring system through Internet of Things (IOT). In *2018 International Conference on Information, Communication, Engineering and Technology (ICICET)* (pp. 1-4). IEEE.

[13]. Khan, N., Khattak, K.S., Ullah, S. and Khan, Z., 2019, December. A low-cost IoT based system for environmental monitoring. In *2019 International Conference on Frontiers of Information Technology (FIT)* (pp. 173-1735). IEEE.

[14]. Assante, D. and Fornaro, C., 2019, April. An educational iot-based indoor environment monitoring system. In *2019 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1475-1479). IEEE.

[15]. Lashari, M.H., Memon, A.A., Shah, S.A.A., Nenwani, K. and Shafqat, F., 2018, November. IoT Based poultry environment monitoring system. In *2018 IEEE International Conference on Internet of Things and Intelligence System (IOTAIS)* (pp. 1-5). IEEE.

[16]. Saini, J., Dutta, M. and Marques, G., 2020. Indoor air quality monitoring systems based on internet of things: A systematic review. *International journal of environmental research and public health*, *17*(14), p.4942.

[17]. Belghith, E.H., Rioult, F. and Bouzidi, M., 2018, November. Acoustic diversity classifier for automated marine big data analysis. In *2018 IEEE 30th International Conference on Tools with Artificial Intelligence (ICTAI)* (pp. 130-136). IEEE.

[18]. Malik, Z., Saxena, A. and Singh, K., 2021, January. Designing a Secure IOT data Encryption algorithm for Smart Environmental Monitoring System. In *2021 International Conference on Advances in Technology, Management & Education (ICATME)* (pp. 106-111). IEEE.

[19]. Velmurugadass, P., Dhanasekaran, S., Anand, S.S. and Vasudevan, V., 2021. Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. *Materials Today: Proceedings*, *37*, pp.2653-2659.

[20]. Mbarndouka Taamté, J., Signing, F., Ruben, V., Kountchou Noube, M. and Bertrand, B., 2022. An efficient environmental monitoring data encryption algorithm based on DNA coding and hyperchaotic system. *International Journal of Information Technology*, *14*(3), pp.1367-1380.

[21]. Gaber, M., Khalaf, A., Mahmoud, I. and El_Tokhy, M., 2021. Advanced Protection Scheme For Information Monitoring in Internet of Things Environment.