International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 12 No. 1, 2026
https://theaspd.com/index.php

A Secure and Energy-Efficient Framework for Environmental Monitoring Data Using Laplace Transform–Based Encryption

V. Sree Ramani[1], P. HariKrishna [2], A. Padma [3], M. Santoshi Kumari[4]
[1,3,4] Department of Mathematics, Chaitanya Bharathi Institute of Technology, Hyderabad 500075 [1]Email: sreeramani_maths@cbit.ac.in.
[2] Department of H&S, Vignan's Institute of Information Technology, Visakhapatnam.
[2]Email: phk.2003@gmail.com

ABSTRACT
Recent years, environmental monitoring systems have become increasingly dependent on continuous data acquisition from distributed sensor networks to evaluate air quality, water pollution, and climate-related parameters. The reliability of such assessments strongly depends on the security and integrity of the collected data. However, environmental monitoring infrastructures often operate in open and resource-constrained environments, making transmitted data vulnerable to interception and manipulation.
The present study introduces a secure and computationally efficient framework for protecting environmental monitoring data using Laplace Transform–based encryption and inverse Laplace Transform–based decryption. The proposed approach preserves data confidentiality while maintaining low computational overhead, which is essential for long-term and real-time environmental monitoring applications. Performance analysis indicates that the framework achieves secure transmission with minimal processing delay, making it suitable for sustainable environmental data management.
Keywords: *Environmental monitoring, Environmental data security, Laplace transformation, IoT-based sensor networks, Sustainable environmental systems.*

1. INTRODUCTION

Environmental monitoring systems rely on continuous data acquisition from distributed sensors to assess air quality, water pollution, and climate variability. The accuracy and reliability of such data are critical for environmental analysis and policy formulation. However, environmental monitoring networks are often vulnerable to data interception, manipulation, and unauthorized access during transmission.
This study proposes a using Laplace Transform–based encryption and inverse Laplace Transform–based decryption. The proposed approach ensures confidentiality and integrity of environmental monitoring data while maintaining low computational overhead, making it suitable for resource-constrained environmental sensor networks.
A representative environmental data sequence is used to demonstrate the effectiveness of the framework. Performance analysis shows that the proposed method provides secure data transmission with minimal encryption and decryption time, supporting real-time and long-term environmental monitoring applications. The framework contributes to reliable and sustainable environmental data management systems.

2. Environmental Monitoring Data Security

Environmental sensor networks are typically composed of low-power devices that operate under strict energy constraints. Conventional cryptographic algorithms, although secure, may impose significant computational and energy overhead, limiting their applicability in environmental monitoring applications. Therefore, security mechanisms for such systems must balance robustness with efficiency.
The proposed framework addresses these requirements by employing Laplace transformation techniques, which offer mathematical simplicity and flexibility in key generation, thereby enhancing resistance to common security threats.
Advanced mathematical methods and secret keys are used in modern cryptography to safely encrypt and decrypt data. Numerous cryptographic methods have been thoroughly reported in the literature [8]–[11]. Among these, Hiwarekar [8], investigated matrix-based mathematical techniques. Using ASCII codes

(128-bit) for encryption, Sachin and Bani (2013) presented a novel cryptographic system that combines infinite series and the Laplace transform. Using keys placed at even places inside an array, they first encrypt data using infinite series before using the Laplace transform. The inverse Laplace transform is used for decryption.Further developments in Laplace transform-based cryptography can be found in the works of Naga Lakshmi, Ravi Kumar, and Chandra Sekhar [11], as well as Hiwarekar [9,10], where encryption is achieved through the series expansion of a function f(t) and its corresponding Laplace transform.

By using the Laplace transform as a key mechanism in the suggested cryptographic system, the authors of this work carry on this line of inquiry.

3.Proposed Secure Framework for Environmental Data

The proposed framework encrypts environmental sensor data using Laplace transformation prior to transmission. At the receiving end, inverse Laplace transformation is applied to recover the original data. The encryption and decryption processes are governed by dynamically generated keys derived from the input data sequence, which increases security and reduces susceptibility to key-based attacks.

4. **Definitions And Standard Outcomes**

Definition 4.1 A plain text message is one that is comprehensible to the sender, the recipient, and anybody else who has access to it.

Definition 4.2 A plain text communication is referred to as a cipher text when it is codified using any appropriate scheme.

Definition 4.3 A plain text transmission is changed into cipher text by encryption, and a cipher text message is changed back into plain text by decryption.

The algorithm and the key are the two components of every encryption and decryption procedure. The key's functions include encryption and
decryption that ensures the security of the cryptography procedure.

The writers here need the following outcomes [8].

4.1. Laplace Transforms

Two domains are involved in Laplace Transforms: (1) the frequency domain, where the signal is represented by its waveform f(t), and (2) the time domain, where the signal is
It is distinguished by its transformation. The Laplace transform of f(t), if f(t) is a function defined for all positive values of t, is defined as

$$\mathcal{L}(f(t)) = \bar{F}(s) = \int_0^\infty e^{-st} f(t)dt \qquad (1)$$

as long as the integral is present. In this case, the parameter s can be either real or complex. The matching Laplace inverse transform is

$$\mathcal{L}^{-1}(\bar{F}(s)) = f(t) \qquad (2)$$

Here, the Laplace transforms f(t) and F(s) are referred to as a pair.

4.2. Property of The linearity

Since the Laplace transform is a linear transformation, the sum of the waveforms' transforms is the transform of the waveforms themselves. Formally speaking, the linearity characteristic is

If $\mathcal{L}\{f(t)\} = F(s)$ and $\mathcal{L}\{g(t)\} = G(s)$,

then $\mathcal{L}\{af(t) + bg(t)\} = a\mathcal{L}\{f(t)\} + b\mathcal{L}\{g(t)\} = aF(s) + bG(s)$. (3)

where the constants a and b are used.

It is simple to generalize the aforementioned result to more than two functions.

4.3. Elementary Functions' Laplace Transforms

Algebraic and transcendental functions are examples of elementary functions.

$$\mathcal{L}(t^n)=\frac{n!}{s^{n+1}}\ , \qquad \mathcal{L}^{-1}\{\frac{n!}{s^{n+1}}\}=t^n \qquad (4)$$

A representative environmental monitoring data sequence is considered to illustrate the proposed secure transmission framework

5. SUGGESTED TECHNIQUE

An understanding of the suggested cryptographic technique can be gained from the following algorithm. The following procedures are used by the sender to transform the original message or plain text into cipher text to secure air pollution data.

The encryption method

I. Convert to ASCII code after selecting the message, M, to be sent. Let n be the message's length.

II. Based on the conversion mentioned above, the plain text message is arranged as a finite sequence of numbers. For instance, "DANGER ATAK" is our basic text. In this case, n=10.

The ASCII code of the pain text reads D=68, A=65, N=78, G=71, E=69, R=82, A=65, T=84,A=65, and K=75, based on the step above.

Let our plain text finite sequence is

Let

S0=68,, S1=65, S2=78, S3=71, S4=69, S5=82,

S6=65, S7= 84, S8= 65, S9=7,

Sn=0 for n≥10

III. Expressing these numbers as coefficients of t cosrt where r is a constant.

These authors take note of traditional expansion

$$Cos\ rt=1-\frac{(rt)^2}{2!}+\frac{(rt)^4}{4!}-\frac{(rt)^6}{6!}+\frac{(rt)^8}{8!}-\frac{(rt)^{10}}{10!}+\frac{(rt)^{12}}{12!}-\ldots\ldots\ldots\ldots$$

And

$$t\ Cos\ rt = =t-\frac{(rt)^3}{2!}+\frac{(rt)^5}{4!}-\frac{(rt)^7}{6!}+\frac{(rt)^9}{8!}-\frac{(rt)^{11}}{10!}+\ldots\ldots\ldots\ldots$$

Let us contemplate

$$f(t)=Gt\ Cos2t$$

$$=t\left[G_0.1-G_1.\frac{4t^2}{2!}+G_2.\frac{16t^4}{4!}-G_3.\frac{64t^4}{6!}+G_4.\frac{256t^8}{8!}-G_5.\frac{1024t^{10}}{10!}+G_6\frac{4096t^{12}}{12!}-G_7.\frac{16384t^{14}}{14!}+G_8\frac{65536t^{16}}{16!}-G_9\frac{262144t^{18}}{18!}\right.$$

$$\left.\frac{16\times t^5}{4!}-71.\frac{64\times t^7}{6!}+69.\frac{256\times t^9}{8!}-82.\frac{1024\times t^{11}}{10!}+65.\frac{4096\times t^{13}}{12!}-84.\frac{16384\times t^{15}}{14!}+65.\frac{65536\times t^{17}}{16!}-75.\frac{262144\times t^{19}}{18!}\right]$$

IV. Next take Laplace transform of a polynomial

$$F(S)=L[f(t),S] \qquad =L\Big(\left[68t-65.\frac{4\times t^3}{2!}+78.\right.$$

$$\left.\frac{16\times t^5}{4!}-71.\frac{64\times t^7}{6!}+69.\frac{256\times t^9}{8!}-82.\frac{1024\times t^{11}}{10!}+65.\frac{4096\times t^{13}}{12!}-84.\frac{16384\times t^{15}}{14!}+65.\frac{65536\times t^{17}}{16!}-75.\frac{262144\times t^{19}}{18!}\right]$$

$$=\frac{68}{s^2}-\frac{780}{s^4}+\frac{6240}{s^6}-\frac{31808}{s^8}+\frac{158976}{s^{10}}-\frac{923648}{s^{12}}+\frac{3461120}{s^{14}}-\frac{20643840}{s^{16}}+\frac{72417280}{s^{18}}-\frac{373555200}{s^{20}}$$

V. Subsequently, determine ri such that ri=Fi mod 200, where i=0,1,2,3,...,n.

$r_0=68\ mod\ 200=68=D$

$r_1=780 \quad =180=\ \dashv$

$r_2=6240\ =40=($

$r_3=31808=8-56(Back\ space)$

$r_4=158976=176=°\ (\ Degree)$

r_5=923648=48=0
r_6=3461120=120= ×
r_7=20643840=40 =(
r_8=72417280=80= *P*
r_9=373555200='0'

The message will be encrypted using the ASCII values of the aforementioned remainders.
The message 'DANGER ATAK' is therefore encrypted as

D⊣(__°0×(*P*'0'

VI.Next, given i=0,1,2,3,...n and any denominator, find ki such that ki=(Fi - ri)/200.

Key ki is thus obtained as

k_0=0,

$$K_1=\frac{780-180}{200}=\frac{600}{200}=3$$

$$K_2=\frac{6240-40}{200}=\frac{6200}{200}=31$$

$$K_3=\frac{31800}{200}==159$$

$$K_4=\frac{158976-176}{200}=794$$

$$K_5=\frac{923600}{200}=4{,}618$$

$$K_6=\frac{3461000}{200}=17305$$

K_7=103,219

$$K_8=\frac{72417200}{200}=362{,}086$$

K_9=1,867,776

Method of Decryption
I Examine the ciphertext and key that were sent by the sender in the case above.
whose key and ciphertexts are 0, 3, 31, 159,794, 4618,1305, 103219, 362086, 1867776 :*D*⊣(__°0×(*P*'0'

II. The provided ciphertext should be converted to the corresponding finite sequence of numbers 68,180,40,8,176,48,120,40,80,0, viz.
G_0^1=68, G_1^1=180, G_2^1=40, G_3^1=8, G_4^1=176,G_5^1=48,G_6^1=120,G_7^1=40,G_8^1=80,G_9^1=0
using the provided key
$F_i=200K_i+G_1^1$ for i=0,1,2,3...

F_0=200×0+68=68
F_1=200×3+180=780
F_2=200×31+40=6240
F_3=200×159+8=31808
F_4=200×794+176=158976
F_5=200×4618+48=923648
F_6=200×17305+120=3461120
F_7=200×103219+40=20643840
F_8=200×362086+80=72417280
F_9=200×1867776+0=373555200

Now consider $G\frac{s^2-4}{(s^2+4)^2}=\frac{68}{s^2}-\frac{780}{s^4}+\frac{6240}{s^6}-\frac{31808}{s^8}+\frac{158976}{s^{10}}-\frac{923648}{s^{12}}+\frac{3461120}{s^{14}}-\frac{20643840}{s^{16}}+\frac{72417280}{s^{18}}-\frac{373555200}{s^{20}}$

Next the inverse laplace transform of a polynomial

$f(t)=Gtcos2t=L^{-1}$

$$\left(\frac{68}{s^2}-\frac{780}{s^4}+\frac{6240}{s^6}-\frac{31808}{s^8}+\frac{158976}{s^{10}}-\frac{923648}{s^{12}}+\frac{3461120}{s^{14}}-\frac{20643840}{s^{16}}+\frac{72417280}{s^{18}}-\frac{373555200}{s^{20}}\right)$$

$$=68t-\frac{780t^3}{4!}+\frac{6240t^5}{6!}-\frac{31808t^7}{8!}+\frac{158976t^9}{10!}-\frac{923648t^{11}}{12!}+\frac{3461120t^{13}}{14!}-\frac{20643840\,t^{15}}{16!}+\frac{72417280t^{17}}{18!}-\frac{373555200\,t^{19}}{20!}$$

III. The numerical values of the aforementioned finite sequence correspond to the ASCII characters, yielding the original plaintext: 'DANGER ATAK.'

5 RESULTS AND DISCUSSION

5.1 Using the Laplace Transformation for Input-Output Cryptography

The following data is fed into the encryption algorithm:

'DANGER ATAK.' in simple text

The result following encryption is as follows: Cipher Text::*D*⊣(__°0×(*P*'0'

Decryption Key: 0, 3, 31, 159,794, 4618,1305, 103219, 362086, 1867776

Laplace Transform Inverse Decryption

The decryption method receives the following input: Cipher Text::*D*⊣(__°0×(*P*'0'

The output of the decryption process is the plain text "DANGER ATAK."

Performance Evaluation in Environmental Monitoring

The performance of the proposed framework is evaluated in terms of encryption and decryption time for varying data lengths. The results indicate a gradual increase in processing time with increasing data size, which is consistent with typical environmental data acquisition scenarios.

Notably, decryption time remains lower than encryption time, facilitating efficient data recovery at environmental monitoring and analysis centers. The overall computational efficiency contributes to reduced energy consumption, supporting long-term deployment of monitoring systems.

6.**Applications in Environmental Sciences**

1. Air Quality Monitoring Systems

Air quality monitoring systems employ distributed sensor networks to measure atmospheric pollutants such as particulate matter ($PM_{2.5}$), nitrogen dioxide (NO_2), and sulfur dioxide (SO_2). These systems support regulatory compliance, pollution trend analysis, and public health assessment. Since air quality data is transmitted from multiple monitoring locations to centralized processing units, ensuring secure and reliable communication is essential. Data protection mechanisms help prevent unauthorized access, data loss, and manipulation, thereby preserving the accuracy and credibility of air pollution assessments used in environmental decision-making.

2 **Water Quality Monitoring**

Real-time water quality monitoring plays a vital role in the management of surface and groundwater resources. Sensors deployed in rivers, lakes, and reservoirs continuously collect data related to pH, turbidity, dissolved substances, and potential contaminants. As these monitoring stations often operate in remote or unattended environments, secure transmission of sensor data is necessary to avoid data tampering and false reporting. Reliable protection of water quality information enables early detection of pollution events and supports effective water resource planning and environmental protection strategies.

3 Climate and Meteorological Monitoring

Climate and meteorological monitoring systems generate critical environmental data, including temperature, humidity, rainfall, and other atmospheric parameters. These observations are fundamental for climate modeling, weather forecasting, and impact assessment studies. The secure transmission of meteorological data ensures data integrity during inter-agency sharing and long-term storage. Maintaining the authenticity of climate datasets enhances the reliability of environmental analyses used for disaster management, agricultural planning, and climate adaptation policies.

4. IoT-Based Environmental Surveillance

The adoption of Internet of Things (IoT) technologies has significantly enhanced environmental surveillance capabilities by enabling continuous data collection from diverse ecosystems. IoT-based environmental monitoring systems are commonly deployed in energy-constrained and geographically remote locations, where communication security is a major concern. Secure and lightweight data protection mechanisms ensure confidentiality and authenticity without increasing computational overhead. Such secure IoT frameworks support long-term environmental monitoring, biodiversity conservation, and sustainable ecosystem management.

7.CONCLUSION

This paper presents a secure and energy-efficient framework for protecting environmental monitoring data using Laplace Transform–based encryption techniques. The proposed method ensures confidentiality and integrity of environmental data while maintaining low computational complexity.

The framework is suitable for real-time and long-term environmental monitoring applications, particularly in IoT-based sensor networks. Future work may focus on large-scale deployment and integration with environmental decision-support systems.

Cryptography represents among the primary defenses against unauthorized access and cyber threats in the modern digital landscape. As counterattacks grow in frequency and sophistication, cryptography is expected to remain a critical pillar of information security for years to come.

The rapid digital transformation across various sectors—particularly in banking and financial services—has led to widespread adoption of e-services and online platforms. However, this expansion of digital infrastructure also introduces new avenues for financial fraud, especially in the domain of internet banking, where unauthorized users often exploit security loopholes to carry out fraudulent activities. This necessitates the development of robust and efficient encryption techniques capable of safeguarding sensitive information.

8.Proposed Work

In the proposed study, a novel cryptographic algorithm based on Laplace transform is developed. The method is intentionally designed to be simple and straightforward, yet intrinsically strong and compact. It offers a high level of security while maintaining low computational complexity, thereby making it suitable for real-time encryption tasks in constrained environments.

A key feature of the proposed approach is a dynamic key generation scheme, which is entirely dependent on the input data. This design ensures that the encryption key varies with each message, making it highly resilient to cryptographic attacks. The algorithm allows for multiple levels of transformation, offering a flexible mechanism for key variation. This makes it extremely challenging for attackers to intercept or predict the encryption key, even when subjected to known-plaintext or differential attacks.

Furthermore, the methodology can be extended by applying the Laplace transform to other suitable mathematical functions, providing a foundation for future improvements and variant models in the field of symmetric key cryptography.

Performance Evaluation

The performance of the proposed encryption scheme has been evaluated by measuring encryption and decryption times across different input sizes. The results indicate a proportional increase in computation time with respect to input size. Notably, encryption time tends to be higher than decryption time, a typical characteristic of multi-stage cryptographic algorithms. Despite this, the execution times remain within practical limits, reinforcing the efficiency and feasibility of the approach.

Conclusion and Future Scope

This study presents a secure and energy-efficient framework for environmental monitoring data protection using Laplace Transform–based encryption techniques. By combining mathematical rigor with computational efficiency, the proposed approach ensures confidentiality and integrity of environmental data while remaining suitable for resource-constrained monitoring systems.

Future work will focus on large-scale implementation in real-world environmental monitoring networks and integration with advanced environmental decision-support platforms.

Acknowledgement:The authors would like to extend their heartfelt gratitutude to chaitanya Bharathi institute of technology(CBIT) For their generous funding and un weavering support under the minor project as per the sanction order no.CBIT/PROJ-IH/IO55/Maths/D004/2024,dated 26March 2024.

REFERENCES

[1]. World Health Organization (WHO), *Air Quality Guidelines: Global Update 2005 – Particulate Matter, Ozone, Nitrogen Dioxide and Sulfur Dioxide*, WHO Press, Geneva, Switzerland, 2006.
[2].Chapman D. (Ed.), *Water Quality Assessments: A Guide to the Use of Biota, Sediments and Water in Environmental Monitoring*, 2nd Edition, UNESCO/WHO/UNEP, London, 1996.
[3].Snyder E.G., Watkins T.H., Solomon P.A., et al., The changing paradigm of air pollution monitoring, *Environmental Science & Technology*, 47(20), 11369–11377, 2013.
[4].Intergovernmental Panel on Climate Change (IPCC), *Climate Change 2021: The Physical Science Basis*, Cambridge University Press, Cambridge, United Kingdom, 2021.
[5].Hart J.K., Martinez K., Environmental sensor networks: A revolution in the earth system science?, *Earth-Science Reviews*, 78(3–4), 177–191, 2006.
[6].Ma J., Li X., Wang S., Applications of Internet of Things in environmental monitoring, *Procedia Computer Science*, 154, 348–353, 2019.
[7]..Roman R., Zhou J., Lopez J., On the features and challenges of security and privacy in distributed Internet of Things, *Computer Networks*, 57(10), 2266–2279, 2013.
[8] A.P.Hiwarekar, Application of Laplace Transform For Cryptographic Scheme, Proceedings of the World Congress on Engineering 2013 Vol I, WCE 2013, July 3 - 5, 2013, London, U.K.
[9] A.P. Stakhov, "The golden matrices and a new kind of cryptography", Chaos, Soltions and Fractals 32((2007) pp1138–1146
[10] Blakley G.R., Twenty years of Cryptography in the open literature, Security and Privacy 1999, Proceedingsof the IEEE Symposium, 9-12, (May1999). International Journal of Computer Applications (0975 – 8887) Volume 136 – No.7, February 2016
[11] G.Naga Lakshmi, B.Ravi Kumar and A.Chandra Sekhar, A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2, 2515-2519, (2011).
[12] Stallings W., Cryptography and network security, 4th edition, Prentice Hall, (2005).