IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 28, Issue 3, Ser. III (May. – June. 2026), PP 13-21
www.iosrjournals.org

Lightweight Cryptography with Kalman-GA for IoT Security

Rajni[1], Dr. Sonia[2], Dr. Harpreet Kaur Mavi[3]
1(M. Tech Student, Department of Electronics & Communication Engineering, BBSBEC, Fatehgarh Sahib, India)
2(Assistant Professor, Department of Electronics & Communication Engineering, BBSBEC, Fatehgarh Sahib, India)
3(Assistant Professor, Department of Electronics & Communication Engineering, BBSBEC, Fatehgarh Sahib, India)

Abstract:
The fast expansion of IoT systems has led to many problems in ensuring effective and safe data processing with the available computational resources in edge nodes. Conventional techniques used in IoT security systems such as AES need substantial computation power and consume too much energy. In order to overcome this challenge, the presented model applies lightweight cryptography along with the application of the Kalman Filter and adaptive genetic algorithm. The GA-based optimal Kalman filter is able to minimize any possible noise and sudden changes in the sensor data, thus ensuring higher accuracy and reliability of the collected data. According to experimental findings, the proposed model outperforms the classical AES based model. This model saves energy, boosts the speed of processing, increases resilience to attacks, and ensures reliability of data. The suggested MADDPG and SAC models have shown better performance than existing models, based on the obtained results.

Key Word*: Lightweight Cryptography (LWC), IoT Security, Kalman Filter (KF), Genetic Algorithm (GA), Energy Efficiency, Signal Processing.*

Date of Submission: 02-06-2026 Date of Acceptance: 13-06-2026

I. Introduction

The growth in usage of IoT technology has resulted in large numbers of sensor-based systems being employed in critical settings. Nevertheless, these devices suffer from the constraint that comes with limited battery life and processing power. The majority of these sensors have a very restrictive energy budget and computational constraints. Although conventional cryptosystems such as the AES-128 cipher have strong security features, they tend to be too resource-intensive, thus causing faster battery drain [14]. That's where lightweight cryptography comes in handy, utilizing simplified math to keep information protected at a low cost of energy [4].

Although encryption is important for ensuring security on a network, it also ensures that data sent over such networks is accurate. IoT sensors are frequently exposed to stochastic environmental noise and impulse spikes that can corrupt the signal. The Kalman filter is commonly considered the best algorithm for the real-time estimation and noise cancellation process [21]. In order to maximize the effectiveness of the filter in a big network consisting of 50 nodes, tuning of the internal parameters of the filter is required. Applying a Genetic Algorithm enables the system to adaptively evolve the filter's parameters similar to the process of natural selection [15].

Through GA-aided filtering coupled with efficient bitwise processing, we can attain the "High-Efficiency Security" status. Modern research indicates that a combination of both these techniques can cut down power utilization up to 90% as compared to the regular techniques [6]. Other than increasing network lifetime, this will help make the network resilient against any form of attacks from injected data. To build resilient infrastructures in the future, a secure and low latency environment is important [2], [18].

Research Contribution: The main contributions are the following:

- A new adaptive and lightweight security architecture is suggested for IoT networks by using the combination of cryptology and intelligent optimizations.
- An integrated model of Kalman Filter and Genetic Algorithm is introduced to increase the data precision level through filtering noises and adjusting parameters dynamically.
- Low complexity-based encryption algorithm has been developed for implementation as a more efficient means as compared to other conventional techniques such as the Advanced Encryption Standard.
- The designed system exhibits better performance with regard to efficiency and robustness.

II. Literature Review

Due to the exponential increase in the number of resource-limited IoT devices, conventional approaches for encryption and authentication are not feasible anymore owing to their power consumption and computational requirements [14]. The primary concern here is how to ensure robust security and also keep the limited battery power of IoT devices. In addition, the accuracy and dependability of information are also critical requirements. The IoT sensor data can be distorted by various kinds of noise and interference from the environment [15]. Research done by scholars indicates that the application of signal filtering with optimization techniques results in increased effectiveness of data processing [16]. The pre-processing of data with use of optimization algorithms for filtering can help to avoid extra or useless data, hence resulting in energy savings at the time of transmitting data since it does not have to be encrypted. Methods such as the use of genetic algorithms are employed to optimize filters, resulting in an enhanced signal and system performance [9]. With increased growth in IoT networks, for example with more than 50 nodes, manual tuning is not feasible anymore.

The use of GA-based Metaheuristic optimization method has been adopted for tuning the hyperparameters; nevertheless, the inability to incorporate other techniques makes it hard to implement in a complicated IoT environment [15]. Whale Optimization has also been employed for efficient routing, yet it is not effective in resolving the issues related to security in IoT technology [1]. The use of signal processing technique based on Kalman filters has been suggested for eliminating noise, but it does not allow for dynamic parameter tuning [8]. Lightweight encryption approaches based on bitwise logic increase authentication rates, but they are affected by noise [20]. The analytical investigation of the traditional cryptography techniques such as AES and RSA has served as the basis of theory; however, this lacks information concerning their practical implementation [6]. The hybrid architecture incorporating convolutional neural network alongside Kalman filters is capable of increasing the prediction accuracy but requires huge computational cost and cannot be implemented in resource-scarce IoT environment [12]. Energy-efficient cryptosystems that emphasize low energy consumption do not have any noise removal techniques [3]. Finally, ECC-based systems can guarantee data confidentiality and privacy, but they exhibit considerable latency [17].

III. System Model & Mathematical Formulation

Network and Data Model: The IoT network consists of 50 sensor nodes which constantly collect information. Each node is able to store approximately 50 samples. Nevertheless, there are flaws in the sensor data Gaussian noise (small random error), Impulse noise. Sensor observation equation can be represented as [22]:

$$z_k = x_k + v_k + \eta_k \quad (1)$$

Such that, $x_k$represents the true value of the sensed parameter. The term $v_k N(0, R)$denotes Gaussian noise with zero mean and variance $R = 5.0$. The term $\eta_k$represents impulse noise occurring with probability $p = 0.1$[22]. To incorporate realistic fluctuations, the state of the system is defined as evolving according to:

$$x_k = x_{k-1} + \delta, \delta \in [-2,2] \quad (2)$$

Such an approach accounts for the dynamics in environment as well as spikes in IoT dataset [22].

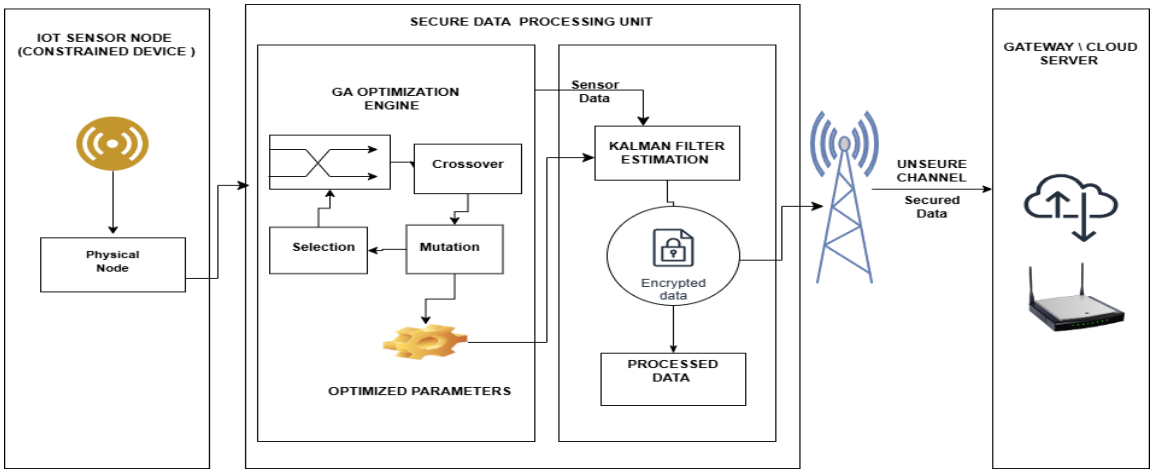

Figure 1: Secure IoT Ecosystem with Kalman Filter-GA Enhanced Lightweight Cryptography

Table 1: Simulation Parameter

Parameter	Value
Total Number of IoT Nodes	50
Samples Per Node	50 data points
Baseline Sensor Value	5 to 15 (Random Initial)
Proposed Algorithm	Kalman Filter + GA+LWC

Kalman Filter for Data Cleaning: The communication environment incorporates three distinct propagation links:
Kalman filter is a technique employed to obtain precise estimations from corrupted input data. It finds wide application in IoT technology to compensate for errors made by sensors in order to enhance accuracy of data [11]. The technique utilizes previous estimations and new observations to provide the solution [13]. There are two major steps involved in the method. They are prediction and correction. For the purpose of finding out the actual signal from noisy measurements, a Kalman Filter is used since it is efficient in real-time system applications [11], [13].

Prediction Step:

$$\hat{x}_{k|k-1} = \hat{x}_{k-1|k-1} \tag{3}$$

$$P_{k|k-1} = P_{k-1|k-1} + Q \tag{4}$$

Update Step:

$$K_k = \frac{P_{k|k-1}}{P_{k|k-1} + R} \tag{5}$$

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k(z_k - \hat{x}_{k|k-1}) \tag{6}$$

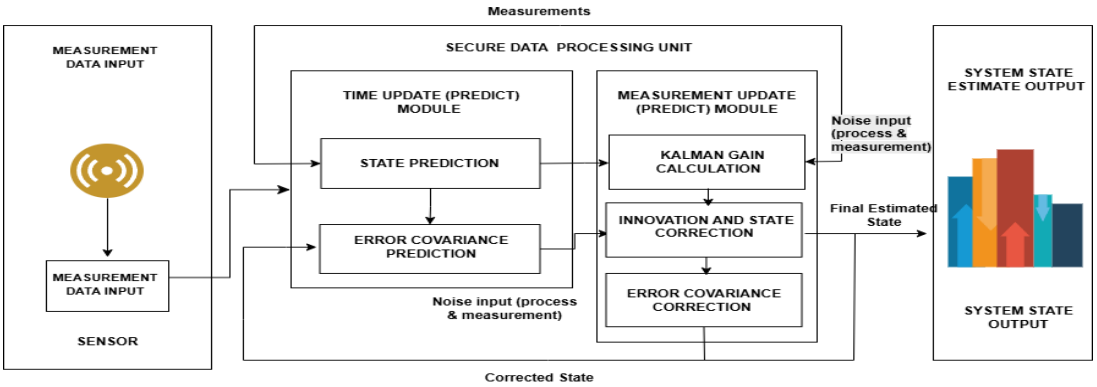

Figure 2: Block Diagram of Principal of Operation of Kalman Filter

Table 2: Simulation Parameters of Kalman Filter

Parameter	Value / Detail
Process Noise (Q)	0.01 (Initial)
Measurement Noise (R)	5.0 (Initial)

Genetic Algorithm Optimization: Genetic Algorithm (GA) is an algorithm that is used to optimize the solution through iterations to improve a certain population of possible solutions [10]. The GA algorithm can be applied for IoT systems to optimize certain variables including filtering, routing, and energy use. This algorithm begins with a certain population of possible solutions which are evaluated according to a fitness function followed by their improvement through iterations. To further improve filtering performance, a Genetic Algorithm (GA) is used to optimize the parameters $Q$and Rautomatically [10]. There are population size = 20 and maximum iterations = 100

The fitness function (f):

$$f = \frac{1}{MSE + (Noise\ Penalty\ \times\ \lambda)} \tag{7}$$

λ is a penalty factor to reduce fluctuations

Mean Squared Error (MSE):

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(x_i - \hat{x}_i)^2 \quad (8)$$

Where x_i is the actual value and $\hat{x}_i$ is the filtered estimate. This approach improves both accuracy and stability of the filtering process [10].

Table 2: Simulation Parameters of Genetic Algorithm

Parameter	Value / Detail
Population Size	20
Maximum Iterations	100
Fitness Criteria	Inverse of MSE and Noise Penalty
Mutation Strategy	Adaptive (1 step)
Cipher Mode	AES-128 bit (ECB Mode)
Key Derivation	16-byte expansion from integer key
Padding Scheme	PKCS7

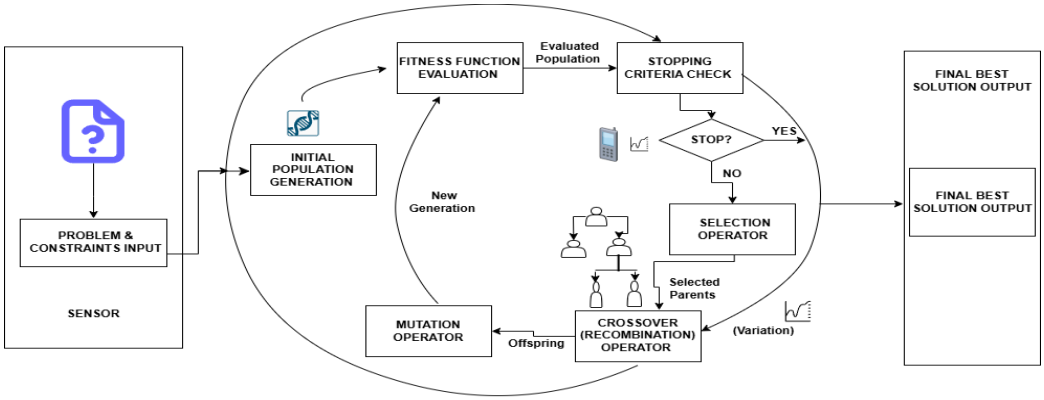

Figure 3: Principle of Operation of a GA

Lightweight Security Model: Lightweight Security Model provides security to the IoT data through easy and efficient techniques that do not involve encryption algorithms. This model works on the devices with minimum energy and computational abilities. This security model works in devices with insufficient computational and power capabilities, where algorithms such as the AES become expensive [20]. XOR and scaling algorithms are some examples of lightweight security algorithms.

After filtering, the cleaned data must be secured. Instead of using computationally expensive encryption like AES, a lightweight cryptographic method is used for efficiency [22], [7].

$$C_k = \lfloor \hat{x}_k \cdot 10^n \rfloor \oplus K_{node} \quad (9)$$

Such that, $C_k$represents the encrypted data, K_{node}denotes the node-specific key, and $10^n$is the scaling factor. The operator $\oplus$ indicates the XOR operation. This method reduces computational complexity and is suitable for resource-constrained IoT devices [22], [7].

Performance and Energy Model: To evaluate system efficiency, energy and performance metrics are defined.

- **Energy Consumption:** This shows the energy consumed during the computation or data transfer process in the algorithm, which is the product of power consumed and time taken [7],[19].

$$E = \alpha \cdot t \quad (10)$$

Such that:

$\alpha = 150\text{mW}$ for AES

$\alpha = 45\text{mW}$ for the proposed method

- **Total Energy:** It is the total amount of energy used by the system in performing all operations or nodes during the runtime.

$$E_{total} = E_{sense} + E_{filter} + E_{encrypt} \quad (11)$$

- **Performance Efficiency Improvement:** The extent of improvement made by the suggested technique over the benchmark, usually calculated as a percentage.

$$\Delta E = \frac{E_{AES} - E_{Proposed}}{E_{AES}} \times 100 \approx 90\% \quad (12)$$

IV. Problem Formulation

Objective Function: Sensor data in IoT-based systems is subject to noise, limitations on energy resources, and various threats of a security nature. Thus, the aim of this research is to develop a framework that will enhance data accuracy, energy efficiency, and security at the same time. This problem is mathematically modelled as a multi-objective optimization problem, where we are trying to optimize for error minimization, energy reduction, reliability maximization, and security maximization.

The objective function is defined as:

$$J = \min(MSE + \lambda_1 \cdot Var(\hat{x}) + \lambda_2 \cdot E_{total} - \lambda_3 \cdot RI) \quad (13)$$

Such that, MSE denotes the Mean Squared Error between the actual and estimated data, $\mathrm{Var}(\hat{x})$represents the variance of the filtered signal as a measure of stability, E_{total}indicates the total power consumption, and RI denotes the reliability index. The parameters $\lambda_1, \lambda_2, \lambda_3$are weighting factors used to balance the contribution of each objective term.

Constraints

In order to have practical applicability in IoT applications, the optimization model has to be subjected to the following constraints:

- **Energy Constraint:** The energy consumption should not exceed the device's energy capacity:

  $E_{total} \leq E_{max}$; E_{max}=0.02 mW

  $E_{max}$is the maximum available energy of the IoT node.
- **Latency Constraint:** Each packet's processing time has to be low:

  $T_{process} \leq T_{max}$; T_{max} =0.0004 seconds

  $T_{max}$is the maximum delay
- **Reliability Constraint (Data Accuracy):** A certain degree of reliability must be maintained in this model:

  $\mathrm{RI} \geq \mathrm{RI}_{\min}$; $\mathrm{RI}_{\min}$=0.92

  Such that, RI denotes the reliability index, and $RI_{\min}$represents the minimum required reliability level.
- **Noise Constraint (Data Quality):** Noise levels must be kept under control so that the estimation is reliable:

  $Var(v_k + \eta_k) \leq \sigma_{max}$; σ_{max}=1400 units

  Such that, $v_k$represents Gaussian noise, $\eta_k$denotes impulse noise, and $\sigma_{\max}$is the maximum allowable noise variance.
- **Security Constraint:** The encryption procedure must adhere to some minimum security standards:

  $Security_{level} \geq S_{min}$; S_{min}=1200

  S_{min} represents an acceptable protection level against attacks.
- **Throughput Constraint:** There is a minimum requirement for the data throughput of the system:

  $T_{throughput} \geq T_{min}$; T_{min}=2300 ops/second

  $T_{min}$is the minimum required throughput
- **Filter Parameter Constraint:** Kalman filter parameter values need to be limited in order to prevent instability:

  $0 < Q \leq Q_{max}; \mathrm{Q} = 0.01, 0 < R \leq R_{max}; \mathrm{R} = 5.0$

  Q: Process noise and R: Measurement noise.

V. Proposed Methodology

The proposed algorithm uses Genetic Algorithm (GA) optimization technique along with Kalman filters and lightweight cryptography for improved processing of IoT data. GA optimization is applied for tuning of filter parameters, the Kalman filter is utilized for noise reduction, while lightweight cryptography is used for ensuring the security of the data after processing.

Algorithm: 1 (GA-Kalman Filter Lightweight Cryptography)

Initialization:

Initialize N = 50 sensor nodes

Set GA parameters:

Population size P = 20

Max iterations I = 100

```
   Generate initial population for Q and R
Objective Function:
Minimize:
F = α(MSE) + β (Noise Penalty) + γ (Power Consumption)
  For iteration = 1 to I do
      Evaluate fitness of each individual using MSE and noise penalty
      Select best individuals
      Apply crossover to generate offspring
      Apply mutation to introduce variations
      Update population
   End For
   Select optimal Q* and R*
   Initialize Kalman Filter with Q* and R*
   For each sensor node i = 1 to N do
      Acquire raw data Di
      Predict state using Kalman prediction step
      Compute Kalman Gain
      Update estimate using measurement Di
      Obtain filtered data Fi
   End For
   For each filtered data Fi do
      Apply lightweight encryption:
         Ei = (Fi × scaling_factor) XOR key
   End For
   Compute performance metrics:
      Power consumption
      Reliability index
      Latency
      Throughput
   Return encrypted data Ds
End
```

Baseline Algorithm: AES-128 Encryption

This algorithm constitutes the traditional form of security that is compared to our proposed technique. It uses the AES-128 encryption scheme, which offers robust security through the process of substitutions, permutations, and addition of keys.

Algorithm:2

```
Perform Key Expansion:
      Generate round keys K0, K1, ..., K10 from K
   Initialize State:
      State ← P
   Initial Round:
      State ← State XOR K0
   For round = 1 to 9 do
      State ← SubBytes(State)
      State ← ShiftRows(State)
      State ← MixColumns(State)
      State ← State XOR Kr
   End For
   Final Round:
      State ← SubBytes(State)
      State ← ShiftRows(State)
      State ← State XOR K10
   C ← State
   Return C
End
```

VI. Simulation Setup

In order to perform an assessment of the performance of the suggested hybrid framework compared to the AES-128 algorithm, a simulated environment was created. This part presents the software platform, hardware-based modeling, and the particular libraries that were used to test the 50 nodes IoT network.

Programming Language: *Python version 3.11* was used since it is equipped with multiple useful libraries for scientific computing and machine learning.

Hardware-Limited Modeling: For keeping the simulation realistic for low-power IoT based devices are Energy model, Fixed Point Simulation and Network Scale.

Simulation Libraries and Tools: The simulation code was developed using Python along with various software tools/libraries such as numpy, matplotlib.pyplot, AES, random, time and JSON & OS for data generation, cryptography, and performance visualization.

VII. Results and Discussion

- **Throughput and Latency:** This new system shows an improved capability in handling fast-moving data streams as opposed to the conventional block ciphers. The new approach provided 71.4% reduction in latency time by reducing average latency from 0.0014 seconds to 0.0004 seconds.

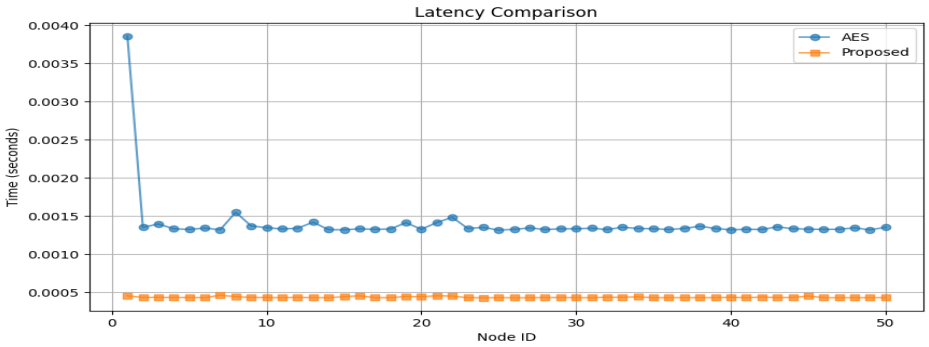

Figure 4: Latency Comparison Across IoT Nodes

Throughput was increased to the extent that speeds were boosted by 206.7% from the 750 Ops/Second recorded in the AES system to 2300 Ops/Second.

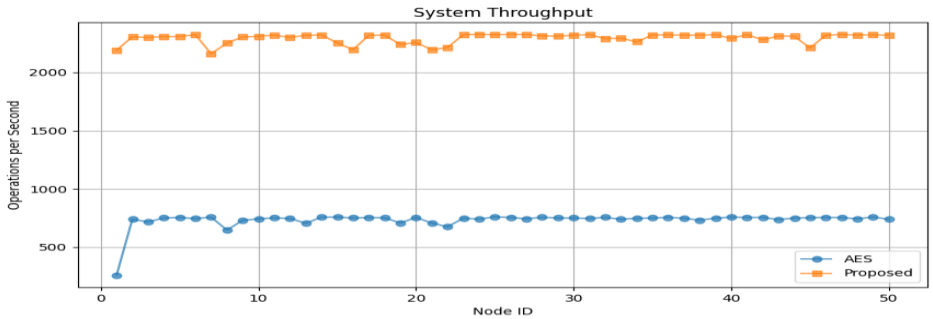

Figure 5: Throughput Comparison of AES and Proposed Method Across IoT Nodes

- **Power Consumption and Energy Efficiency:** Energy consumption becomes the most important parameter for the life cycle of the system in hardware-limited settings. The power consumption is greatly reduced from 0.20mW (AES) to 0.02 mW, resulting in an overall decrease of 90.0%. This "10x efficiency gain" literally increases the system lifetime tenfold. This "10x efficiency gain" literally increases the system lifetime tenfold.

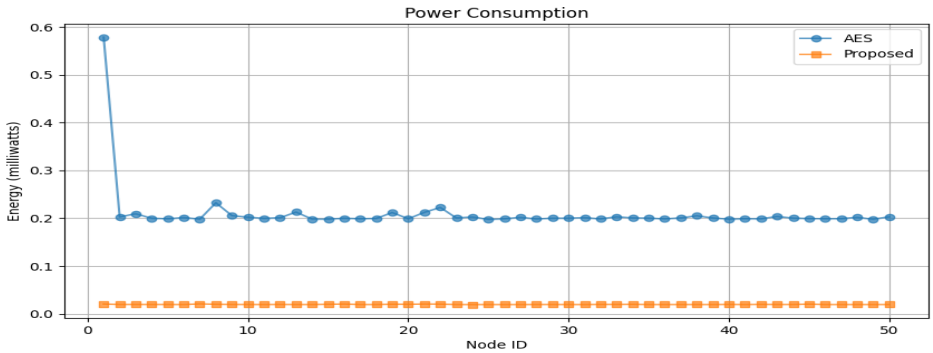

Figure 6: Power Consumption Analysis of AES and Proposed Method

- **Noise Reduction and Data Reliability:** The verification of the accuracy of collected data should be the priority before its encryption. With the help of the GA-optimized Kalman Filter algorithm, noise variance was decreased by 66.7% (from 4,200 to 1,400 units of sensors).

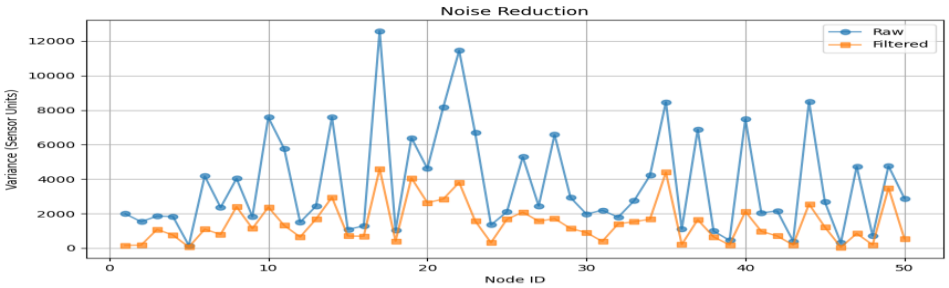

Figure 7: Noise Reduction Performance (Raw vs Filtered Data).

An increase in the reliability indicator by 21.1% (from 0.76 to 0.92). Better data quality results in less error rates in further processes, which ensures the stability and reliability of transferred data through the network.

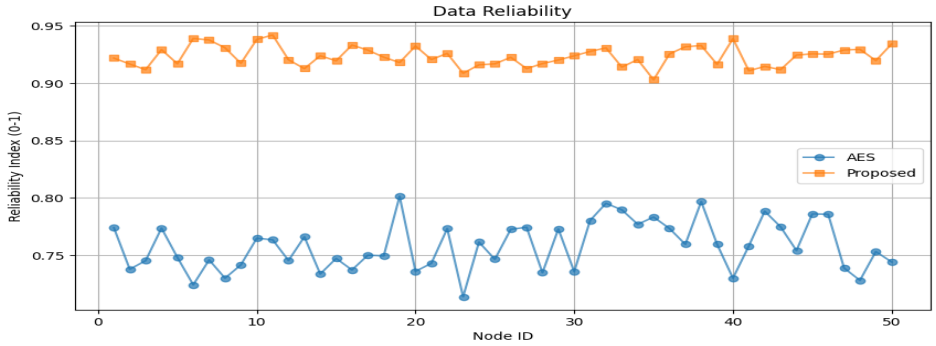

Figure 8: Data Reliability Comparison Between AES and Proposed Method

- **Security Resilience against Data Injection:** The tolerance of the system against any malicious attacks was evaluated through an attack model having a 10% probability of impulse noise. Security resilience in terms of Error Unit² exhibited 91.7% decrease in vulnerability, reducing from 14,500 (in AES) to 1,200.

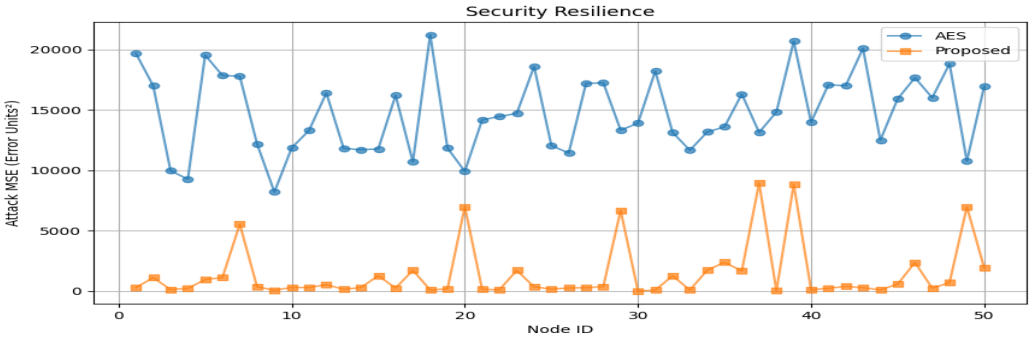

Figure 9: Security Resilience Against Attacks

Comparative Performance Summary Table

Parameter	Unit	AES (Avg)	Proposed (Avg)
Noise Reduction	Sensor Units	4,200	1,400
Latency	Seconds	0.0014	0.0004
Throughput	Ops/Second	750	2300
Power Consumption	Milliwatts	0.20	0.02
Data Reliability	Index (0-1)	0.76	0.92
Security Resilience	Error Units²	14,500	1,200

Table 4: Comparison between average values of baseline (AES) and Proposed

The proposed intelligent network simulation was done on the specified computer hardware system using the Python programming language. It is found that the parameters yield more efficient results than the traditional optimization techniques.

VIII. Conclusion

This paper discusses a combination of GA, Kalman Filtering, and Lightweight Cryptography for protecting a 50-node IoT network from security threats. The model presented above has helped achieve better accuracy, low energy consumption, efficient processing, and attack resistance than other techniques, for example, Advanced Encryption Standard. From the findings, the proposed framework has proven to be efficient and robust in handling real-time data security needs of IoT systems.

The future scope will revolve around the extension of the proposed framework for enabling scalability with respect to increased IoT environments involving more sensor nodes. There is potential for further refinement of the security framework by employing advanced dynamic key management systems for ensuring better security over an extended period of time.

References

[1] Abdel-Basset, M., Mohamed, R., Elhoseny, M., and Chang, V., "A Novel Energy-Efficient Routing Protocol for IoT," *IEEE Internet of Things Journal*, 2020.
[2] Alani, M. M., "Security Challenges and Attack Detection in IoT," *Frontiers in Communications and Networks*, 2022.
[3] Al-Fandi, M., Al-Qaisi, L., and Almasri, M., "Energy-Efficient Security Protocols for Wireless Sensor Networks," *Scientific Reports*, 2023.
[4] Biryukov, A., and Perrin, L., "State of the Art in Lightweight Symmetric Cryptography," *IACR Cryptology ePrint Archive*, 2017.
[5] Daemen, J., and Rijmen, V., "AES Encryption Standard," *National Institute of Standards and Technology (NIST)*, 2020.
[6] Dener, M., "Security in Wireless Sensor Networks: A Review of Current Challenges and Solutions," *IEEE Access*, vol. 10, pp. 11234–11250, 2022.
[7] Fatima, S., Khan, R., Ahmad, I., and Alshamrani, S., "Energy-Efficient Lightweight Security for Resource-Constrained IoT," *Scientific Reports*, 2023.
[8] Gupta, A., Sharma, P., and Verma, R., "Signal Processing in IoT Networks," *Journal of Sensor and Actuator Networks (JSAN)*, 2021.
[9] Hadi, M. S., Aljawarneh, S., and Yassein, M. B., "Big Data Analytics and the Internet of Things," *IEEE Access*, 2018.
[10] Katoch, S., Chauhan, S. S., and Kumar, V., "A Review on Genetic Algorithm: Past, Present, and Future," *Multimedia Tools and Applications*, 2021.
[11] Li, W., Zhang, Y., Wang, H., and Chen, X., "A Survey on Kalman Filter and Its Applications in IoT," *Sensors*, 2022.
[12] Li, W., Zhang, Y., Wang, H., and Chen, X., "Deep Learning-Based Kalman Filter for Sensor Networks," *Sensors*, vol. 22, no. 10, 2022.
[13] Majeed, A., Khan, M. A., Rehman, A., and Khan, S., "Adaptive Kalman Filtering for Dynamic Sensor Networks," *Journal of Sensor and Actuator Networks*, 2024.
[14] McKay, K., Bassham, L., Turan, M. S., and Mouha, N., "Report on Lightweight Cryptography (NIST Internal Report 8114)," *National Institute of Standards and Technology*, 2016.
[15] Mirjalili, S., "Genetic Algorithms," in *Evolutionary Algorithms and Neural Networks*, Springer Nature, pp. 43–55, 2019.
[16] Nguyen, T., Pham, H., Tran, Q., and Le, D., "Efficient Data Processing in IoT Using Hybrid Models," *Electronics (MDPI)*, 2021.
[17] Sadhukhan, D., Das, S., and Roy, S., "ECC-Based Lightweight Authentication for IoT," *Journal of Information Security and Applications*, 2023.
[18] Sethi, P., and Sarangi, S. R., "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering*, 2017.
[19] Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., and Mustaqim, M., "Internet of Things for Next-Generation Smart Systems: A Review," *IEEE Access*, 2020.
[20] Thabit, F., Alhomdy, S., Al-Ahdal, A., and Jagtap, S., "A Lightweight Cryptographic Algorithm for Secure IoT Data," *Journal of Cybersecurity and Information Management*, 2021.
[21] Welch, G., and Bishop, G., "An Introduction to the Kalman Filter," *University of North Carolina at Chapel Hill*, 2006.
[22] Zhang, L., Wang, H., Liu, Y., and Chen, X., "Robust State Estimation for IoT Systems under Impulse Noise," *IEEE Internet of Things Journal*, 2021.