

Securing IoT Data in Power Consumption Anomaly Detection Systems Using the Rivest–Shamir–Adleman Cryptographic Algorithm

Ardian Banuarta Frizi^{1*}, Arief Arfriandi², Djuniadi³

^{1,2}Universitas Negeri Semarang, Semarang, Central Java, Indonesia

e-mail: ardianbanuarta425@gmail.com^{1*}, arfriandi@mail.unnes.ac.id², djuniadi@mail.unnes.ac.id³

Article Information

Article History:

Received : 21 May 2026
Revised : 21 July 2026
Accepted : 6 September 2026
Published : 18 October 2026

*Correspondence:

ardianbanuarta425@gmail.com

Keywords:

Cryptography, RSA Algorithm,
Internet of Things, Data Security
System

Copyright © 2026 by Author.
Published by Universitas Dinamika.



This is an open access article under
the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



10.37802/joti.v8i2.1415

**Journal of Technology and
Informatics (JoTI)**

P-ISSN 2721-4842

E-ISSN 2686-6102

[https://e-](https://e-journals.dinamika.ac.id/index.php/joti)

[journals.dinamika.ac.id/index.php/joti](https://e-journals.dinamika.ac.id/index.php/joti)

Abstract:

The Internet of Things (IoT) enables real-time monitoring and transmission of power consumption data but introduces security risks, including unauthorized access, data interception, and manipulation. This study proposes an asymmetric cryptographic mechanism based on the Rivest–Shamir–Adleman (RSA) algorithm to secure sensor data in a power consumption anomaly detection system. RSA public-key encryption and private-key decryption were integrated into a power monitoring device to protect voltage, current, power, and energy measurements during data transmission. The security and computational performance of the proposed mechanism were evaluated using encryption and decryption time, Shannon entropy, and avalanche effect. Experimental results showed an average encryption time of 114.322 ms and decryption time of 7.893 ms, resulting in a total processing time of 122.215 ms, which remained below the defined system evaluation threshold. The resulting ciphertext achieved an average Shannon entropy of 7.173 bits, approaching the theoretical maximum of 8 bits, while the average avalanche effect reached 49.993%, closely matching the ideal value of 50%. These findings demonstrate that RSA can provide practical protection for periodically transmitted IoT sensor data while producing ciphertext with desirable randomness characteristics for power consumption anomaly detection applications.

INTRODUCTION

The advancement of digital technology has fundamentally transformed data communication and interaction, enabling rapid, efficient, and increasingly automated information exchange through open networks, including the Internet. One of the most significant developments in this domain is the Internet of Things (IoT), which enables interconnected physical devices to communicate and exchange data automatically through sensors and actuators [1]. This capability improves operational efficiency and supports real-time monitoring and decision-making across diverse application domains [2]. In power consumption monitoring systems, IoT

devices continuously acquire and transmit technical sensor parameters, including voltage, current, power, and energy, to remote servers for storage, analysis, and visualization. Because these data represent electricity consumption patterns and system operating conditions, unauthorized access, interception, or manipulation may result in financial losses, operational disruptions, privacy concerns, and inaccurate decision-making [3], [4]. Therefore, ensuring the confidentiality and integrity of IoT sensor data during transmission is an essential requirement for reliable and secure power monitoring systems.

Cryptography protects sensitive information by transforming plaintext into ciphertext accessible only to authorized parties [5]. This protection is particularly important in IoT environments, where sensor data are transmitted through networks vulnerable to unauthorized access and interception. Among cryptographic methods, Rivest–Shamir–Adleman (RSA) is a widely used asymmetric algorithm that employs separate public and private keys, reducing the need for shared-secret key distribution [6], [7]. RSA has been applied to electronic document security [8], evaluated for resilience against artificial intelligence-based attacks [9], and integrated into hybrid cryptosystems to improve ciphertext entropy [10]. More recently, hybrid AES–RSA schemes have been investigated for low-power IoT communication, addressing security and resource constraints [11]. In energy-related applications, real-time monitoring and anomaly detection are increasingly important for improving the resilience and reliability of complex energy systems [12]. However, these studies primarily address general cryptographic security, hybrid encryption, or energy-system monitoring rather than securing periodically transmitted IoT sensor data. This gap motivates evaluating standalone RSA for secure power-consumption monitoring.

Despite these contributions, an important research gap remains regarding the application and evaluation of RSA for technical sensor data generated by IoT-based power monitoring systems. Existing studies have predominantly focused on electronic document authentication, cryptographic resilience, hybrid encryption, and general information-system security [8]–[11]. Web-based data protection studies have also investigated cryptographic techniques for securing sensitive information stored in MySQL databases [13]. Similarly, hybrid encryption approaches have been proposed for secure and efficient data transmission in IoT devices, highlighting the importance of balancing communication security and computational efficiency [14]. Comparative studies of symmetric and asymmetric cryptographic algorithms further indicate that encryption mechanisms should be selected according to both security requirements and operational conditions [15]. However, limited attention has been given to the feasibility of standalone RSA for periodically transmitted IoT sensor measurements in power consumption monitoring and anomaly detection systems. Such systems require data protection without introducing excessive computational overhead that could affect transmission and system responsiveness.

In particular, the simultaneous evaluation of computation time, Shannon entropy, and avalanche effect for RSA-based protection of power consumption sensor data remains insufficiently investigated. Shannon entropy provides a quantitative measure of uncertainty and randomness in cryptographic outputs [16], while the avalanche effect evaluates the degree to which small changes in plaintext affect the resulting ciphertext [17]. Alternative cryptographic approaches, including Vigenère- and AES-based methods, have also been investigated for IoT and constrained environments [18], while previous evaluations have emphasized computational performance as an important consideration for cryptographic algorithms deployed on IoT devices [19]. Lightweight encryption studies further demonstrate the need to balance security with computational and communication efficiency [20]. Moreover, Rachmadini et al. [21] demonstrated the use of Transport Layer Security (TLS) for securing MQTT-based IoT data transmission and evaluated encryption processing time and data integrity, highlighting the importance of security-

performance trade-offs in IoT communication. Nevertheless, empirical evidence regarding the combined performance of standalone RSA in periodically transmitted power-consumption sensor data remains limited.

Based on this gap, this study investigates the implementation and feasibility of RSA for securing technical IoT sensor data in a power consumption anomaly detection system. The study considers voltage, current, power, and energy measurements generated by a power monitoring device and transmitted through an IoT communication architecture. Unlike previous studies addressing document protection, cryptographic resilience, hybrid encryption, or lightweight cryptographic mechanisms [8]–[11], [14], [18], [20], this research focuses on standalone RSA for periodically transmitted sensor data. The novelty lies in its integrated evaluation from three complementary perspectives: computational efficiency, ciphertext randomness, and sensitivity to plaintext changes. Computation time evaluates encryption and decryption overhead, Shannon entropy measures ciphertext randomness, and the avalanche effect assesses sensitivity to small plaintext modifications.

The main contribution of this research is empirical evidence regarding the feasibility of RSA for securing IoT sensor data in power consumption anomaly detection systems. By integrating evaluation dimensions examined individually in previous cryptographic and IoT studies [16], [17], [19], this study provides a comprehensive assessment of RSA for periodically transmitted power-consumption data. The results clarify whether RSA can provide effective data protection while maintaining acceptable computational performance and desirable ciphertext characteristics, thereby contributing practical evidence for the development of secure IoT-based power monitoring systems.

METHOD

This research method is designed to explain how the study was carried out, starting from problem identification, system implementation stages, and the data security testing process. The research workflow is shown in Figure 1.

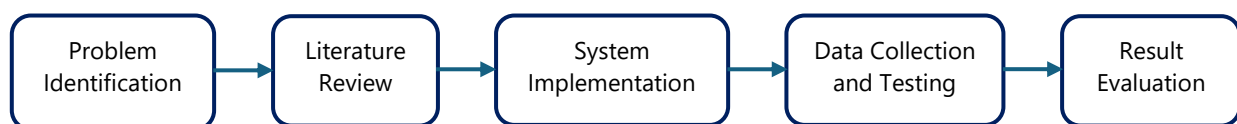


Figure 1. Research Flow Diagram

1. Problem Identification

Problem identification is the first step in this research. Its goal is to understand, define, and narrow down the issues to be studied in a systematic way. At this stage, we review the system workflow, the components involved, the types of data sent, and any possible weaknesses that could affect system security and reliability. In this study, the focus is on IoT data security in a power consumption anomaly detection system. The data from sensor devices, such as voltage, current, power, and energy, are the main sources for monitoring and decision-making. Figure 2 shows the system scheme to help explain this process.

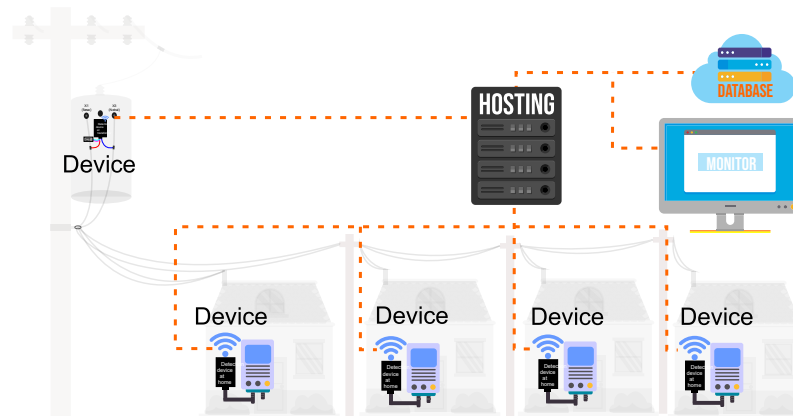


Figure 2. IoT System Scheme for Power Consumption Detection

Based on the scheme, the integration process between devices requires IoT connectivity so that data from the measurement device can be sent automatically to the processing system. However, the use of open networks in the data transmission process has the potential to be accessed, intercepted, or modified by unauthorized parties [1]. This issue is important because the anomaly detection system relies heavily on data accuracy. If power consumption data can be manipulated, the analysis and decision-making processes may produce incorrect conclusions [2]. Therefore, a security mechanism is needed to maintain data confidentiality and integrity during transmission from the IoT device to the server.

2. Literature Review

The literature review was conducted by collecting and analyzing literature from previous studies, such as journal articles, scientific proceedings, and research reports relevant to the research topic. The literature was used to strengthen the theoretical foundation and to understand the suitability of the RSA algorithm for securing data in IoT systems. In addition, the literature review also served as a reference for determining security testing parameters, such as entropy testing, avalanche effect testing, and computation time.

3. System Implementation

System implementation was carried out by integrating Internet of Things (IoT) devices, a server, a database, and a data security mechanism based on the Rivest-Shamir-Adleman (RSA) algorithm. The initial stage of system implementation began with generating an RSA key pair on the server, namely the public key and the private key. The public key is sent or made available so that it can be accessed by the microcontroller to encrypt sensor data. Conversely, the private key remains stored on the server and is not shared with other devices. After the device obtains the public key, the sensor measurement data are converted into numerical form and then encrypted using the RSA algorithm. The encrypted data are then sent to the server and stored in the MySQL database. Storing data in encrypted form in the database is an important part of the system security design, because data stored in encrypted condition can reduce the risk of plaintext exposure, unauthorized access, and data exploitation when database compromise occurs [3][4]. When the data are needed for monitoring, the server performs decryption using the private key so that the data can be restored to their original form and displayed on the website. The data security workflow design in this system is shown in Figure 3.

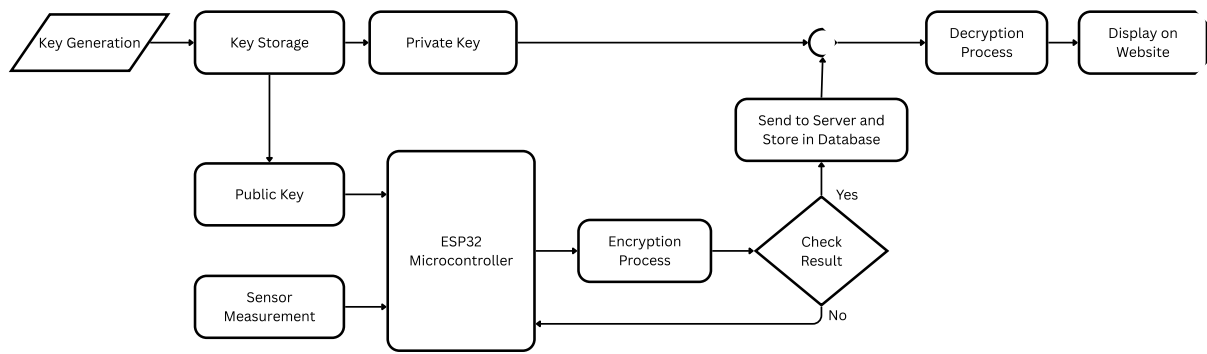


Figure 3. IoT Data Security System Flowchart

Based on the design shown in Figure 3, the IoT data security system in this study comprises three main stages: RSA key generation, data encryption, and data decryption. Each stage of the RSA algorithm implementation in the IoT-based power consumption anomaly detection system is described in the following subsections:

3.1 RSA Key Generation

RSA key generation is the process of creating a pair of keys consisting of a public key and a private key used for data encryption and decryption. The public key can be shared with anyone to encrypt messages, while the private key must be kept confidential because it is used to decrypt messages [5]. In this system, RSA key generation is performed on the server. The following equations describe the RSA key generation process.

- 1) The key generation process begins by calculating the modulus n by selecting two different prime numbers, namely p and q :

$$n = p \times q \quad (1)$$

- 2) Next, the Euler function $\varphi(n)$ is calculated to determine the coprimality space in selecting the public exponent e :

$$\varphi(n) = (p - 1)(q - 1) \quad (2)$$

- 3) The public exponent e is selected so that it is relatively prime to $\varphi(n)$ and lies within the following range:

$$1 < e < \varphi(n) \text{ and } FPB(e, \varphi(n)) = 1 \quad (3)$$

- 4) The private exponent d is selected, where if d is multiplied by the public exponent e , the result is equal to 1 in modulo $\varphi(n)$ calculation.

$$d \times e \equiv 1(\text{mod } \varphi(n)) \quad (4)$$

- 5) Through this process, the following key pair is obtained.

$$K_{\text{Publik}} = (e, n) \text{ and } K_{\text{Privat}} = (d, n) \quad (5)$$

3.2 Data Encryption Process

Encryption is the process of transforming original data (plaintext) into a form that cannot be read by unauthorized parties. In this system, data obtained from sensors, such as voltage, current, power, and energy, are first converted into ASCII codes.

Table 1. ASCII Code Example

Character	Decimal	Hexadecimal
A	65	41
B	66	42
C	67	43
D	68	44
...	...	...

After the plaintext is converted into numerical values, each plaintext value P is encrypted using the public key (e, n) . The RSA encryption process is expressed in equation 6.

$$C = P^e \bmod n \quad (6)$$

3.3 Data Decryption Process

Within this system, decryption occurs exclusively when users access the monitoring website to view power consumption data. At that point, the server utilizes the securely stored private key (d, n) to convert encrypted data (ciphertext) into their original form (plaintext). Consequently, the IoT device transmits only encrypted data using the public key, and the original data become accessible solely upon a request from the web monitoring system by the user. The RSA decryption process is represented by the following equation.

$$P = C^d \bmod n \quad (7)$$

4. Data Collection

Data collection was conducted after the RSA algorithm had been successfully implemented in the IoT-based power consumption anomaly detection system. The dataset consisted of 120 consecutive sensor readings collected directly from a single IoT monitoring device under normal operating conditions. The sensor measured four electrical parameters, namely voltage, current, power, and energy, and transmitted the measurements to the server at 5-minute intervals, resulting in a total monitoring duration of approximately 10 hours. Throughout the experiment, the same RSA public-private key pair was used for all encryption and decryption processes. The collected dataset represents actual sensor measurements rather than simulated data and was subsequently used to evaluate RSA performance in terms of computation time, Shannon entropy, and avalanche effect. The use of periodically collected sensor data reflects the operational characteristics of the proposed IoT monitoring system and enables a realistic assessment of RSA implementation in continuous data transmission scenarios.

5. System Testing

System testing was performed to assess the performance and security of the Rivest-Shamir-Adleman (RSA) algorithm for securing IoT data within the power consumption anomaly detection system. The evaluation utilized three primary parameters:

5.1 Encryption and Decryption Computation Time Test

The computation time test was conducted to determine the amount of time required by the Rivest-Shamir-Adleman (RSA) algorithm to perform encryption and decryption on IoT sensor data. This test aims to provide an overview of data processing duration when RSA is applied to a power consumption anomaly detection system. Encryption and decryption times are calculated based on the difference between process completion time and process start time.

5.2 Entropy Test

The entropy test was conducted to determine the level of randomness of the ciphertext generated by the RSA algorithm. The entropy calculation uses the Shannon Entropy concept

shown in Equation 8.

$$E_{(x)} = - \sum_{i=1}^n p(x_i) \log_2 p(x_i) \quad (8)$$

Description:

$E(x)$: Ciphertext entropy value

$P(x_i)$: Probability of occurrence of the i-th character

n : Number of characters in the ciphertext

5.3 Avalanche Effect Test

The avalanche effect test was conducted to determine how much the ciphertext changes when a small change occurs in the plaintext. In a good cryptographic algorithm, a change of one bit or one character in the plaintext should produce a large change in the ciphertext. The avalanche effect value is calculated using Equation 9.

$$AE = \frac{B_{diff}}{B_{total}} \times 100\% \quad (9)$$

AE : Avalanche effect value

B_{diff} : Number of different bits between two ciphertexts

B_{total} : Total number of bits compared

6. Result Evaluation

The determination of evaluation criteria in this study refers to information theory and cryptographic theory. The entropy reference value refers to the Shannon Entropy concept described in A Mathematical Theory of Communication, which has a maximum value of 8 [6]. The avalanche effect reference value refers to the Strict Avalanche Criterion concept by Webster and Tavares, which states that a small change in the input should ideally produce approximately 50% change in the output [7][8]. Meanwhile, the computation time limit does not refer to a specific book standard, but is determined based on the characteristics of the IoT system in this study, namely that data are transmitted once every 1000 ms. Therefore, the encryption and decryption processes are considered good if they do not exceed 1000 ms.

Table 2. Evaluation Value References

Parameter	Value	Determination Basis
Entropy	Maximum 8 bits	Shannon Entropy Theory
Avalanche effect	Ideal 50%	Webster and Tavares
Computation time	Maximum 1000 ms	Research system requirement

RESULTS AND DISCUSSION

1. System Implementation Results

This study implements the Rivest-Shamir-Adleman (RSA) algorithm using the Python programming language. Python is used to run the main RSA processes, namely key generation, encryption, decryption, and testing of encryption results. The first step is to generate an RSA key pair, consisting of a public key for encryption and a private key for decryption. Table 4 shows the RSA key pair generation results in this study.

Table 3. RSA Key Generation Results

Description	Result
Public Key	MIIBlJANBgkqhkiG9w0BAQEFAAOCAQ8A...TQIDAQAB
Private Key	MIIEvgIBADANBgkqhkiG9w0BAQEFAASCCKgw...D3yHAMiX

Following key pair generation, the system encrypted sensor data from the IoT device. The encrypted data were transmitted to the server and stored in a MySQL database. This database serves both as a storage medium and as a platform for data retrieval. MySQL supports export to various formats, such as CSV, which facilitates subsequent data analysis using Python.

Table 5. System Database Display

id	waktu	tegangan	arus	daya	energi	waktu_dekrip	waktu_enkrip
155	2026-05	GYNEh+fjC	rPIRzlrpcXF	XL67tmGVs	NEVZMfP/HX	6.590	114.679
156	2026-05	GDMhLWd2	KiB+1YReg1	HDjl5TuTo9c	1aL9OzfZsDW	7.589	114.169
157	2026-05	OPvGeanO9	2AAeR9sRZ/	fDsoSAJ1Z/b	qOWdHKJryA	4.530	114.337
158	2026-05	KNWrIAY6m	FB7zqfZAIQ	ZEHpCtZlAm	GACxSCbp2s	10.496	114.193

In addition to storing data in the MySQL database, this system also has a web dashboard that displays decrypted data. The dashboard shows that the data security process does not stop at encryption, but also successfully restores encrypted data into original data that can be read and used for monitoring. Figure 4 shows the system dashboard display.

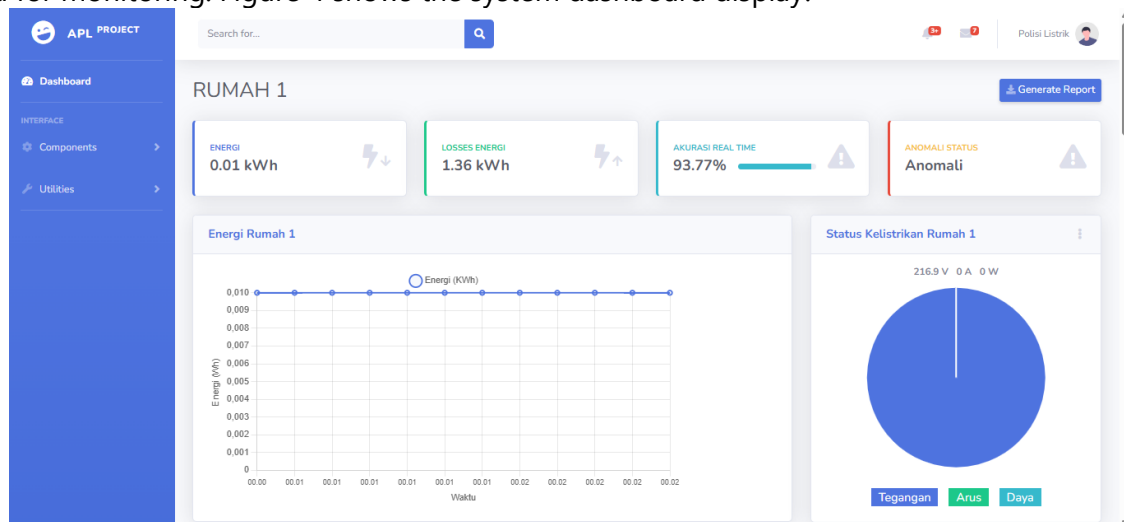


Figure 4. Web Dashboard Display

2. Computation Time Test Results

Computation time testing was conducted to determine the duration of the RSA encryption and decryption processes on IoT sensor data. The computation time test was conducted using the 120 periodically collected sensor readings described in the data collection stage. The observed parameters include minimum time, maximum time, and average processing time in the encryption, decryption, and total time processes.

Table 6. RSA Computation Time Results

Process	Samples	Min. (ms)	Max. (ms)	Average (ms)
Encryption	120	114.116	114.733	114.322
Decryption	120	3.362	15.786	7.893
Total Time	120	117.595	130.114	122.215

Based on Table 6, the encryption time ranged from 114.116 to 114.733 ms, with an average of 114.322 ms. The small-time difference indicates that the encryption process ran stably across all samples. With a maximum time of 114.733 ms, the data security process can still be performed quickly without disrupting sensor data transmission. In the decryption process, the obtained time ranged from 3.362 to 15.786 ms, with an average of 7.893 ms. This result indicates that decryption can be performed quickly, although some variations occurred in several samples. These variations are still acceptable because the decryption process is carried out on the server side and may be influenced by encrypted data retrieval, private key execution, and data processing before being displayed on the dashboard.

Overall, the total RSA processing time ranged from 117.595 to 130.114 ms, with an average of 122.215 ms. This value remains far below the system evaluation threshold of 1000 ms, indicating that the RSA encryption and decryption processes do not impose a significant computational burden on the system. With an average processing time of 122.215 ms, the RSA algorithm is feasible for implementation in a power consumption anomaly detection system that requires periodic data transmission. This result is comparable to the findings of Iftikhar et al. [9], who report that cryptographic algorithm performance in IoT environments should be evaluated based on speed, cost, and overall efficiency.

3. Entropy Test Results

The entropy testing results on 120 data samples show that the ciphertext from the four sensor variables has relatively high values and falls within a close range. The testing data are presented in Table 7, while Figure 5 is used to visualize the distribution of entropy values for each sample.

Table 7. Entropy Test Results

ID	Voltage	Current	Power	Energy
1	7.161842	7.231764	7.132998	7.183212
2	7.203463	7.149657	7.174366	7.203701
3	7.167197	7.087547	7.241001	7.121847
...	...	...	...	...
120	7.135709	7.134032	7.246356	7.103273
Average	7.17348	7.180361	7.170801	7.16956

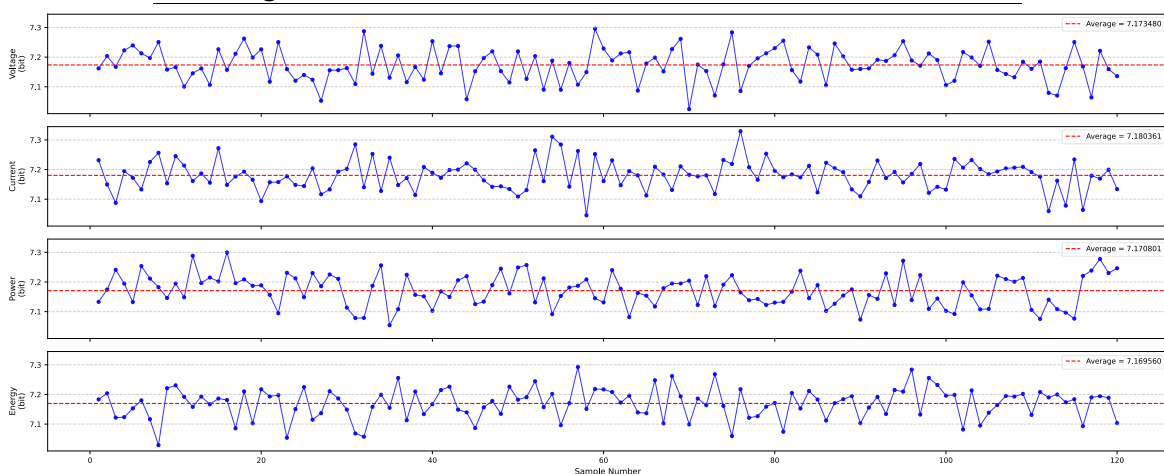


Figure 5. Entropy Test Results Graph

Based on Table 7, the results of testing 120 data items have an average entropy value above 7 bits. The highest average entropy value is found in the current variable at 7.180361,

followed by voltage at 7.173480, power at 7.170801, and energy at 7.169560. The data distribution in Figure 5 also shows that the entropy value of each sample fluctuates, but does not show extreme differences between variables. This indicates that the ciphertext generated by RSA has a stable randomness pattern across all sensor data, not only in one particular type of variable.

Overall, the average entropy obtained is 7.173551 bits. This value is close to the theoretical maximum entropy of 8 bits, indicating that the encrypted ciphertext exhibits a high degree of randomness in its character distribution. At this entropy level, the ciphertext does not easily reveal patterns from the original plaintext, meaning that the transformation from simple numerical sensor readings into encrypted data successfully produces a structure that is more difficult to analyze or recognize. This result aligns with the findings of Silva-Garcia et al. [10] in the study "A Hybrid Cryptosystem Incorporating a New Algorithm for Improved Entropy", which reports that entropy values approaching 8 bits indicate stronger randomness in encrypted data. Although the obtained entropy is slightly lower than the ideal maximum, it still reflects adequate randomness for IoT sensor data, which typically consist of short and structured numerical values.

4. Avalanche Effect Test Results

In the avalanche effect test, small changes in the original data produced ciphertext changes that were very close to the ideal value. The testing results on 120 samples are presented as follows:

Table 8. Avalanche Effect Test Results

ID	Voltage (%)	Current (%)	Power (%)	Energy (%)
1	48.29%	49.316406	50.146484	49.21875
2	48.4375	50.830078	50.292969	47.705078
3	49.511719	51.953125	51.660156	50.097656
...	...	...	...	...
120	49.902344	50.000000	51.074219	48.291016
Average	49.990234	49.952393	50.100505	49.93042

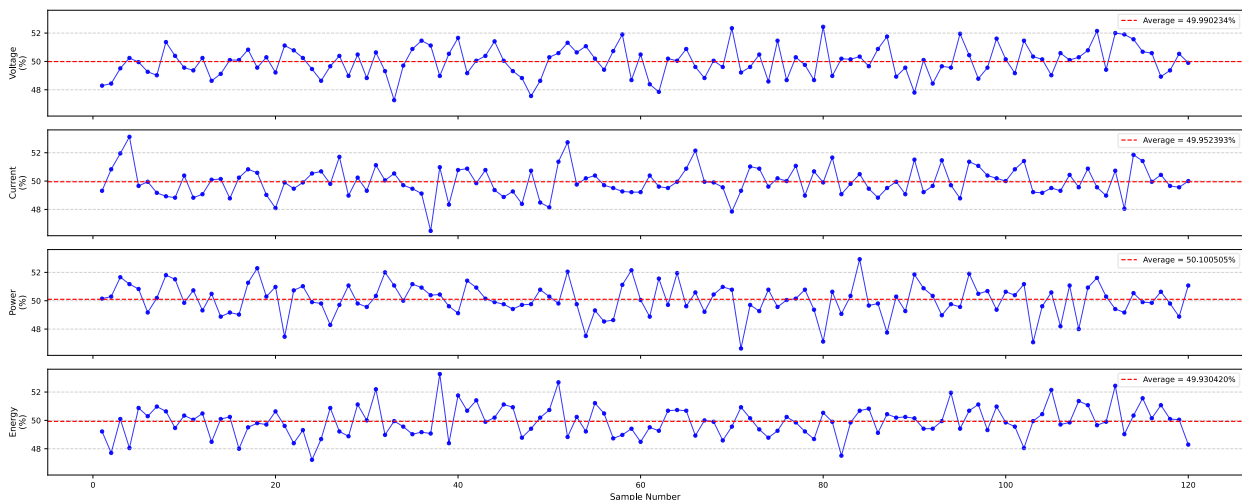


Figure 6. Avalanche Effect Test Results Graph

Based on the testing results, small changes in the plaintext produced ciphertext changes that were very close to the 50% reference value. The power variable had the highest average value at 50.100505%, while the energy variable had the lowest average value at 49.930420%. This very small difference indicates that RSA produces evenly distributed ciphertext changes across all sensor data variables. The average avalanche effect of 49.993388% confirms that the RSA

algorithm is highly sensitive to plaintext changes. These results indicate that RSA is capable of producing a stable and nearly ideal change effect on power consumption IoT data. This result is higher than the findings in the study entitled "Evaluation of the Effectiveness of Lightweight Encryption Algorithms on Data Performance and Security on IoT Devices" by Indrajati and Ashari [11], where AES128 produced the highest avalanche effect of 39.29% among the tested lightweight encryption algorithms. Thus, the average avalanche effect of 49.993388% in this study indicates that RSA produces ciphertext changes that are very close to the ideal 50% criterion for power consumption sensor data.

CONCLUSIONS AND SUGGESTIONS

This study demonstrates the feasibility of implementing the Rivest–Shamir–Adleman (RSA) algorithm to secure periodically transmitted IoT data in a power consumption anomaly detection system. The proposed system successfully encrypts voltage, current, power, and energy measurements before transmission and decrypts them for web-based monitoring. Based on 120 sensor readings, RSA achieved average encryption, decryption, and total processing times of 114.322 ms, 7.893 ms, and 122.215 ms, respectively, remaining well below the 1000 ms system threshold. The ciphertext achieved an average Shannon entropy of 7.173551 bits, approaching the theoretical maximum of 8 bits, while the average avalanche effect reached 49.993388%, closely matching the ideal value of 50%. These results indicate satisfactory computational performance and desirable ciphertext characteristics within the evaluated IoT environment. However, the findings are limited to the investigated system configuration, dataset, transmission interval, and implementation environment. Future research should evaluate different RSA key sizes, larger datasets, transmission frequencies, and resource-constrained IoT hardware, as well as compare RSA with lightweight symmetric and hybrid approaches such as AES and AES–RSA to assess security, computational overhead, communication efficiency, and scalability.

REFERENCES

- [1] M. M. Rahman, S. Al Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," *Cyber Security and Applications*, vol. 3, pp. 2–19, Dec. 2024, doi: 10.1016/j.csa.2024.100082.
- [2] M. Trigka and E. Dritsas, "Edge and Cloud Computing in Smart Cities," Mar. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/fi17030118.
- [3] I. R. Mukhlis and R. Santoso, "Perancangan Basis Data Perpustakaan Universitas Menggunakan MySQL dengan Physical Data Model dan Entity Relationship Diagram," *Journal of Technology and Informatics (JoTI)*, vol. 4, no. 2, pp. 81–87, Apr. 2023, doi: 10.37802/joti.v4i2.330.
- [4] A. N. Habibah, "Keamanan informasi dalam konteks teknologi komunikasi modern," 2024. [Online]. Available: <http://urj.uin-malang.ac.id/index.php/mij/index>
- [5] A. Cahya Putra and M. Simanjuntak, "PENERAPAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENGAMANKAN DATABASE PROGRAM KELUARGA HARAPAN (PKH)," *JIK*, vol. 5, no. 1, 2021.
- [6] U. Indriani, O. Alfina, and N. Syahputri, "Penerapan Algoritma RSA Dalam Keamanan File Ms Word," *Journal of Machine Learning and Data Analytics (MALDA)*, vol. 01, pp. 95–100, Aug. 2022.
- [7] Z. Arif and A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi," 2023.
- [8] I. B. G. Sarasvananda and I. B. A. I. Iswara, "Tanda Tangan Elektronik Menggunakan Algoritma Rivest Shamir Adleman (RSA) pada Sistem Informasi Surat Menyurat LPIK

- INSTIKI," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 11, no. 2, pp. 289–296, Sep. 2022, doi: 10.32736/sisfokom.v11i2.1403.
- [9] Z. Temirbekova, S. Tynymbayev, T. Chinibayeva, D. Asetova, and A. Imanbayev, "Analysis of RSA algorithm cryptographic resilience using artificial intelligence methods," *International Journal of Innovative Research and Scientific Studies*, vol. 8, no. 5, pp. 1866–1878, 2025, doi: 10.53894/ijirss.v8i5.9313.
- [10] V. M. Silva-García, R. Flores-Carapia, and M. A. Cardona-López, "A Hybrid Cryptosystem Incorporating a New Algorithm for Improved Entropy," *Entropy*, vol. 26, no. 2, Feb. 2024, doi: 10.3390/e26020154.
- [11] Q. Chang, T. Ma, and W. Yang, "Low power IoT device communication through hybrid AES-RSA encryption in MRA mode," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-98905-0.
- [12] A. Aghazadeh Ardebili *et al.*, "Enhancing resilience in complex energy systems through real-time anomaly detection: a systematic literature review," Dec. 01, 2024, *Springer Nature*. doi: 10.1186/s42162-024-00401-8.
- [13] R. D. Nugraha, M. D. Ali, N. Khairunnisa, D. Nurcahyo, and A. T. Zy, "Strengthening Web-Based Login Security Using Vigenère Cipher and AES ENCRYPT() Method in MySQL," *Journal of Technology and Informatics (JoTI)*, vol. 7, no. 1, pp. 90–99, May 2025, doi: 10.37802/joti.v7i1.954.
- [14] L. Zhang and L. Wang, "A hybrid encryption approach for efficient and secure data transmission in IoT devices," *Journal of Engineering and Applied Science*, vol. 71, no. 1, Dec. 2024, doi: 10.1186/s44147-024-00459-x.
- [15] D. I. Gunawan, M. R. Aldizar, and I. F. Nasution, "PERBANDINGAN ALGORITMA KRIPTOGRAFI SIMETRIS DAN ASIMETRIS," *UNES Journal of Information System*, vol. 8, pp. 42–47, Jun. 2023, [Online]. Available: <https://fe.ekasakti.org/index.php/UJIS>
- [16] B. Zolfaghari, K. Bibak, and T. Koshiba, "The Odyssey of Entropy: Cryptography," Feb. 01, 2022, *MDPI*. doi: 10.3390/e24020266.
- [17] J. Gáll, P. Gürgez, and G. Horváth, "Adding an Avalanche Effect to a Stream Cipher Suitable for IoT Devices," *Electronics (Basel)*, 2025, doi: 10.3390/electronics14132546.
- [18] N. A. Karima, A. N. Aisyah, H. V. Silla, L. B. Handoko, and R. R. Sani, "Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit," *Jurnal Masyarakat Informatika*, vol. 15, no. 1, pp. 1–13, May 2024, doi: 10.14710/jmasif.15.1.60836.
- [19] U. Iftikhar, M. Waqas, P. Kashif Asrar, and S. Abbas Ali, "Evaluating the Performance Parameters of Cryptographic Algorithms for IOT-based Devices," 2021. [Online]. Available: www.etasr.com
- [20] D. Indrajati and W. M. Ashari, "Evaluation of the Effectiveness of Lightweight Encryption Algorithms on Data Performance and Security on IoT Devices," 2025. [Online]. Available: <http://jurnal.polibatam.ac.id/index.php/JAIC>
- [21] D. Rachmadini, I. Puspasari, and Jusak, "Implementasi dan Analisis Fitur Keamanan Protokol MQTT pada Telehealthcare," *Journal of Technology and Informatics (JoTI)*, vol. 2, no. 1, pp. 10–19, 2020, doi: 10.37802/joti.v2i2.117.