Journal of Theoretical and Applied Information Technology
30th November 2025. Vol.103. No.22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTEGRATION OF DATA FILTERING WITH HYBRID RSA DEEP LEARNING ALGORITHM FOR IOT DATA SECURITY AND CLASSIFICATION

[1]ACHMAD FAUZI, [2]SUCI RAMADANI, [3]HUSNUL KHAIR, [4]AKIM M H PARDEDE
[1,2,3,4]STMIK Kaputama, Jl. Veteran No. 4A-9A, Binjai, North Sumatra, Indonesia
Email : fauzyrivai88@gmail.com

ABSTRACT

The Internet of Things (IoT) presents significant challenges in maintaining data security, particularly in ensuring confidentiality while simultaneously detecting anomalies intelligently. Therefore, this study aims to develop a hybrid model that integrates the RSA algorithm for encryption and decryption with a Convolutional Neural Network (CNN) as the classification mechanism for IoT data. The research workflow includes RSA key generation and validation, encryption of IoT image data, decryption with the RSA private key, and classification using CNN with the log-sum-exp and softmax methods. Simulation results produced outputs of $O_1 = -3945.78$ with a probability of 0%, $O_2 = -1972.89$ with 0%, and $O_3 = 0$ with ≈100%, confirming that the input almost certainly falls into the file under attack class and demonstrating the model's ability to preserve data confidentiality while achieving very high anomaly detection accuracy. The main contribution of this research is the development of a comprehensive approach to enhance the reliability of IoT systems against cybersecurity threats through the integration of RSA, which focuses on data confidentiality, and CNN, which ensures intelligent anomaly detection, so that the proposed model not only strengthens IoT security layers but also offers a practical solution that can be implemented to build more robust and adaptive security systems in the future.

Keywords: *CNN, Deep_Learning, Data_Security, IoT, RSA*

1. INTRODUCTION

The massive development of the Internet of Things (IoT) has created significant opportunities for the digitalization of various sectors, including industry, transportation, healthcare, and smart homes. IoT enables real-time communication among intelligent devices through interconnected networks, thereby promoting efficiency and automation. However, the rapid growth of IoT devices also introduces substantial challenges in terms of data security. Each connected device has the potential to serve as an entry point for cyberattacks, such as sniffing, spoofing, and data manipulation[1]. Data communication security has become a crucial aspect that must be ensured, particularly given the large volume of sensitive information transmitted within IoT environments[2][3][4].

Given the critical importance of system security in strengthening technological infrastructure, enhancing protection in the fields of science and technology is essential to foster both the creative economy and the green economy. Such efforts are also aligned with ensuring defense and security at both the system level and in the real world, in accordance with the national development agenda outlined in Asta Cita 2, 3, and 4[5].

A classical yet highly relevant approach to ensuring data security is the use of cryptography. The Rivest Shamir Adleman (RSA) algorithm is a widely adopted asymmetric cryptographic method employed to secure digital communications[6]. RSA is well recognized for its strength and stability in preserving both the confidentiality and integrity of data through its public and private key system[7]. However, in the context of IoT with its inherent resource constraints, the implementation of RSA requires optimization to remain efficient and avoid overburdening devices. Moreover, RSA is not designed for data classification or attack detection, thus necessitating integration with other approaches capable of handling the dynamic nature of IoT data in real time[8].

IoT data are first encrypted using ElGamal Encryption, with the encryption keys optimized through Slime Mold Optimization (SMO) to enhance strength and security. Subsequently, the

encrypted data are classified using a Hybrid Deep Learning (CNN–LSTM) model that estimates the probability of each instance. If P(anomaly|data) > **0.5**, the data are categorized as anomalous; otherwise, they are considered normal. The experimental results of this study demonstrated probabilistic performance with a precision of 98.75%**,** recall of 98.3%**,** and specificity of 98.5%[9].

To address these limitations, Deep Learning has emerged as a promising approach. Models such as Convolutional Neural Networks (CNNs) have proven effective in classifying and identifying anomalous patterns within network data [9][10]. Deep Learning enables systems to learn complex and unstructured data representations, as well as to detect attacks that may not be identified by conventional methods [11][12]. However, Deep Learning alone does not guarantee cryptographic data security. Therefore, an integration between RSA as an encryption system and Deep Learning as a data classification mechanism is required.

This hybrid approach enables IoT data filtering that is both secure and intelligent. this study designs a secure data filtering system within IoT environments by combining RSA for data protection and Deep Learning for data classification. In this system, data is encrypted at the initial stage using RSA, after which Deep Learning is employed to analyze and filter malicious or suspicious data before it reaches the server or cloud. Through this approach, not only are data security and integrity enhanced, but classification efficiency is also improved, thereby making the decision-making process within IoT systems more responsive and accurate [9][13][14].

The discussion of this research focuses on the hybrid integration of RSA and Deep Learning for data filtering in IoT systems[3][15]. Several previous studies have developed security systems based on AI or standalone encryption mechanisms; however, only a few have combined both into a single integrated architecture [16].

In previously published research, a different approach was employed by optimizing the ElGamal algorithm with Slime Mold Optimization (SMO) for key generation, followed by an encryption process and subsequent classification using a CNN–LSTM[9], with the primary objective of protecting public data in the Internet of Things (IoT) environment[9]. In contrast, this research proposes a design for randomly filtering IoT data through IP address identification to determine the image data source, followed by RSA encryption and subsequent RSA decryption**,** and finally classification using a Convolutional Neural Network (CNN) to evaluate and enhance the accuracy of security performance.

The system design integrates RSA for IoT data encryption and CNN for data classification. Raw data (such as images, audio, and files) is first encrypted using RSA and then transmitted to the server. The CNN subsequently classifies the data as normal, compromised, or attack-containing. The system then stores legitimate data, discards malicious data, or issues alerts accordingly.

The research approach and objectives are as follows:

1. Focus on IoT Data Security by applying the RSA algorithm for the encryption and decryption of IoT image data obtained randomly through IP addresses to ensure data confidentiality
2. Anomaly Detection and Classification by integrating CNN with the log-sum-exp and softmax methods on encrypted data to intelligently detect anomalies and enhance the reliability of IoT systems in addressing cybersecurity threats.

The primary research problem addressed in this study is as follows:

1. How can the encryption and decryption processes of the RSA algorithm secure IoT image data obtained randomly through IP addresses
2. How does CNN perform in classifying encrypted IoT data using the log-sum-exp and softmax methods, and to what extent is its accuracy in detecting anomalous data?
3. How can the hybrid integration of RSA and CNN enhance both security and intelligent classification to strengthen the reliability of IoT systems in addressing cybersecurity threats?

As a hypothesis in this research, the application of the RSA algorithm for the encryption and decryption of IoT image data obtained randomly through IP addresses, together with the integration of CNN using the log-sum-exp and softmax methods, is expected to ensure data confidentiality while intelligently detecting anomalies, thereby enhancing the reliability of IoT systems in addressing cybersecurity threats.

2. METHODS AND MATERIAL

The following literature review is presented as a theoretical foundation supporting the implementation of this research :

This research emphasizes that the hybrid approach can strengthen communication security while improving the reliability of data classification in IoT environments. The SMOEGE-HDL model applies the slime mold optimization algorithm to generate optimal encryption keys and employs the Nadam optimizer to enhance classification performance. Experimental results demonstrate superior performance compared to other methods, achieving accuracy, precision, recall, specificity, and F1-score above 98%[17].

This research develops an IoT intrusion detection model based on deep learning by utilizing BiLSTM and GRU architectures optimized with the JAYA algorithm. The model was tested on the IoT-23 and MQTTset datasets, achieving very high accuracy of up to 99.88% with a remarkably low false alarm rate (<1%). Experimental results indicate that JAYA-BiLSTMIDS outperforms JAYA-GRUIDS and other IDS methods, thereby confirming the effectiveness of optimized deep learning approaches in enhancing IoT network security[18].

2.1 Internet of Things (IoT)

The Internet of Things (IoT) is a modern technological paradigm that connects various physical devices through the Internet to communicate and exchange data automatically. IoT enables system automation, operational efficiency, and supports real-time data-driven decision-making[19].

2.2 Definition and Characteristics of IoT

The Internet of Things (IoT) is a modern paradigm in information technology that connects physical devices such as sensors, actuators, vehicles, and household appliances into digital networks for automatic data exchange. IoT enables real-world objects to become digital entities capable of interacting in real time without direct human involvement [3][19][20]. In the past five years, the development of IoT has accelerated with the increasing integration of sensors and artificial intelligence into distributed systems that require high efficiency and adaptive responsiveness [21][22].

Several studies define IoT as a dynamic network-based system capable of connecting various physical and virtual entities through standard communication protocols, enabling large-scale data acquisition, processing, and exchange [19][23]. IoT is now widely applied across various domains such as industry (Industrial IoT), healthcare (e-Health), smart agriculture, transportation, and smart homes.

The main characteristics of IoT are as follows

1. Real-Time Connectivity
   One of the fundamental characteristics of IoT is its ability to collect and transmit data in real time. This capability allows systems to respond directly and automatically to environmental changes[24].
2. Ubiquity and Scalability
   IoT supports the connection of billions of devices within widely distributed networks. Its presence is ubiquitous, and the system is designed with high scalability, enabling adaptation to diverse user scenarios.
3. Heterogeneity and Interoperability
   IoT devices originate from various vendors and employ diverse communication protocols. Therefore, ensuring interoperability among devices has become a critical challenge in IoT system development.[19][25].
4. Reliability and Energy Efficiency
   System reliability, particularly in maintaining uninterrupted communication, and energy efficiency are crucial characteristics, considering that many IoT devices operate on limited battery power.
5. Security and Privacy
   IoT is often used to process sensitive data (e.g., health or location information); therefore, secure communication (such as encryption) and data privacy protection constitute critical issues that cannot be overlooked[23][25].

The effective integration of these five layers and components is essential for establishing IoT systems that are reliable, secure, and resilient, particularly in the context of data security examined in this study.[19][23][24].

2.3 RSA Algorithm

Introduced in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman, RSA leverages the mathematical principle of factoring large prime numbers to generate a pair of keys: a public key for encryption and a private key for decryption. RSA is highly relevant for Internet of Things (IoT)-based systems that require secure key exchange schemes without the need to share secret keys directly[26].

The main advantage of RSA lies in its ability to perform encryption and decryption using two different keys: the public key and the private key.

The security of RSA systems is grounded in the computational complexity of factoring large prime numbers, which is still considered infeasible to solve within a reasonable time using conventional computing methods[26].

The fundamental principle of RSA lies in modular arithmetic and number theory. In this system, each entity (e.g., a user or an IoT device) possesses a pair of keys: a public key for encryption and a private key for decryption. The key generation process is carried out as follows:

1. Select two large prime numbers $p\ x\ q$
2. Calculate the value $n = p \times q$, which will be used as the modulus for encryption and decryption.
3. alculate the function totien Euler $\phi(n) = (p-1)(q-1)$
4. Select an integer e as the public exponent, subject to the following conditions $1 < e < \phi(n)$ dan $gcd(e, \phi(n)) = 1$.
5. Calculate the private exponent d such that $\phi(n)$: $d \equiv e\text{^}1\ mod\ \phi(n)$.

Thus, the public key is represented by the pair (e, n), while the private key is represented by (d, n). The data (plaintext) to be encrypted by the sender will be computed using the following formula:

$$C = M\text{^}e\ mod\ n \quad (1)$$

On the receiver's side, the data is decrypted using :

$$M = C\text{^}d\ mod\ n \quad (2)$$

RSA enables secure communication without the need to directly share a secret key. This is particularly crucial in open networks such as the Internet and IoT systems, which consist of numerous distributed nodes with public connectivity. Although RSA provides a high level of security, its strength largely depends on the size of the prime numbers employed. Current standards recommend using keys of at least 2048 bits to ensure protection against brute-force and quantum factorization attacks. In IoT systems, the RSA mechanism is often applied during the initial phase of communication for symmetric key exchange. Once the key exchange is successfully completed, subsequent data communication is carried out using more lightweight algorithms, such as AES, to enhance efficiency[27][28].

2.4 Deep Learning

Deep Learning is a subfield of machine learning that employs multilayered artificial neural networks (deep neural networks) to extract features, capture complex patterns, and generate predictions from large and unstructured datasets. In the era of big data and IoT systems that continuously produce data, Deep Learning has become a highly relevant approach for classification, anomaly detection, and data-driven cybersecurity[29][30]. Deep learning (DL) models are increasingly applied to extract lexical and stylistic patterns from URL sequences, minimizing manual feature design while strengthening resilience against adversarial techniques such as nested subdomains and obfuscated paths[31].

2.5 Convolutional Neural Network (CNN)

Convolutional Neural Network (CNN) is a deep learning architecture specifically designed to process spatial data, particularly two-dimensional images, and has become a fundamental framework in various computer vision applications. CNNs are inspired by the visual processes in the human visual cortex, which respond to localized stimuli within the visual field. Unlike conventional Artificial Neural Networks (ANNs), CNNs incorporate mechanisms such as local receptive fields, parameter sharing, and subsampling, making them highly efficient in recognizing spatial patterns[29][17]. The schematic architecture of a Convolutional Neural Network (CNN) is illustrated in the figure below:

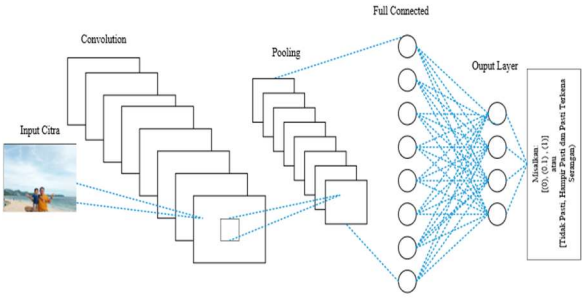

Figure 1. CNN Architecture

The predictive model is constructed using a Convolutional Neural Network (CNN) algorithm, which consists of one-dimensional convolutional layers, Max Pooling layers, and Dense (fully connected) layers [32][33].

The flowchart used in this study comprises several stages, starting from problem identification to the final output obtained[34]. The design can be seen in the flowchart below:

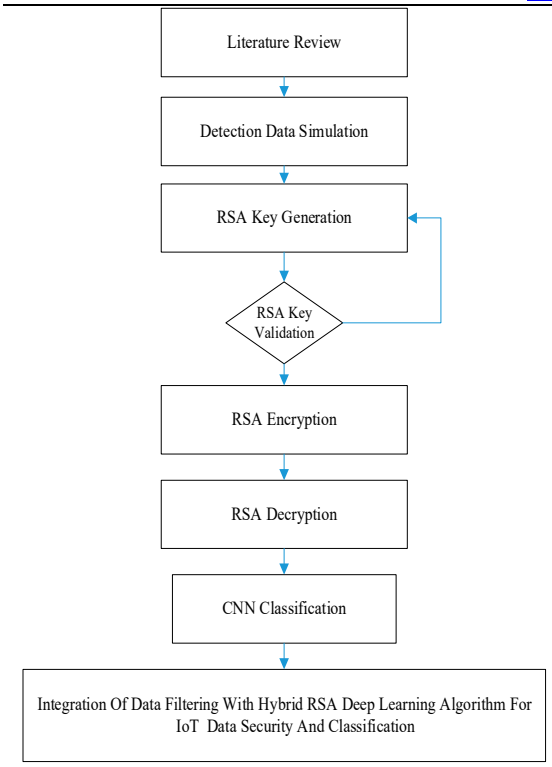

Figure 2: Research Flow Chart

the detailed explanation in the image above is as follows:

1. Literature Review
   Examines theories, methods, and prior studies relevant to IoT security, RSA encryption, and the application of CNN for anomaly detection.
2. Detection Data Simulation
   Constructs IoT datasets (e.g., images or network logs) obtained randomly through IP addresses to be used as detection simulation data.
3. RSA Key Generation
   Generates RSA public and private key pairs to be utilized in the encryption and decryption processes.
4. RSA Key Validation
   Validates the RSA keys to ensure the integrity and correspondence between the public and private keys. If validation fails, the process returns to key generation.
5. RSA Encryption
   Encrypts IoT data using the RSA public key to maintain confidentiality and security during transmission.
6. RSA Decryption
   Decrypts the encrypted data using the RSA private key, enabling the data to be further processed.
7. CNN Classification
   Processes the decrypted data with a Convolutional Neural Network (CNN) enhanced with the log-sum-exp and softmax methods to detect both normal and anomalous patterns.
8. Integration of Data Filtering with Hybrid RSA Deep Learning Algorithm for IoT Data Security and Classification
   The final stage integrates data filtering, RSA encryption, and CNN classification into a hybrid model to enhance IoT data security and enable intelligent anomaly detection.

3. RESULTS AND DISCUSSION

3.1 Model Architecture Design

In this research, the model is designed to illustrate the interrelation between the detected objects, the RSA algorithm, and the CNN model used for data classification. The research model architecture is constructed to conceptually represent the relationship among the key components that will be employed in the research process. This architecture serves as a blueprint that outlines how data are acquired, processed, secured, and analyzed to produce outputs aligned with the research objectives. The design of this model is developed based on theoretical foundations, prior studies, and the characteristics of the problem being addressed. The proposed model architecture can be seen in the figure below:

Journal of Theoretical and Applied Information Technology
30th November 2025. Vol.103. No.22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

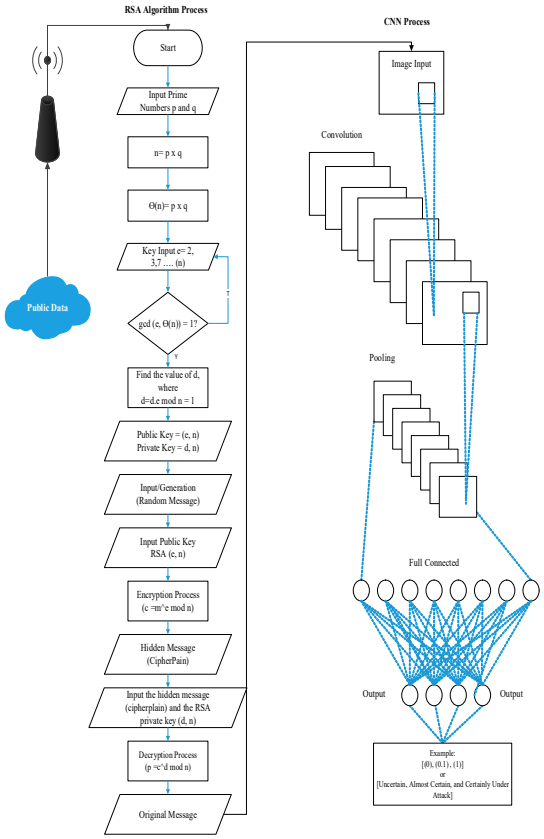

Figure 3. System Model for Filtering

Data with RSA Algorithm and CNN Model In the model above, the system workflow for data filtering from the Internet is illustrated. The process begins with packet capture, followed by IP filtering, data storage, encryption using the RSA algorithm, and concludes with classification using the CNN model for automatic analysis or object identification. The following section presents a simulation of object detection through an access point in a computer network

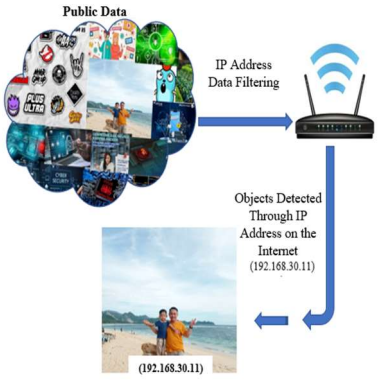

Figure 3. Simulation of Objects Detected with IP Addres

The figure above illustrates the workflow of public data filtering based on an IP Address. The process begins with a collection of public data containing various visual contents and information accessed through the Internet. The system then performs data filtering by utilizing a specific IP Address, in this example 192.168.30.11, to identify relevant data packets. The data corresponding to the specified IP Address are forwarded through a router or access point for further processing. The filtering results display the objects detected according to the IP Address, ensuring that only relevant information is retrieved. This process helps guarantee that the received data are more targeted, efficient, and aligned with analytical needs. The following is an example of the extraction or conversion of a detected image into a 6 × 6 pixel matrix, which will be used as a simulation for computational analysis. This simulation applies the RSA algorithm in the encryption process and the CNN algorithm in the deep learning process for data classification, as presented in the table below:

Table 1. Pixel Extraction Matrix of the Detected Image Data

	0	1	2	3	4	5
0	R=142, G=188, B=220	R=153, G=195, B=224	R=159, G=198, B=225	R=170, G=205, B=229	R=191, G=219, B=236	R=186, G=216, B=235
1	R=151, G=194, B=224	R=157, G=197, B=225	R=173, G=206, B=230	R=191, G=219, B=237	R=182, G=213, B=234	R=182, G=214, B=235
2	R=157, G=197, B=225	R=171, G=205, B=230	R=188, G=217, B=236	R=181, G=213, B=235	R=178, G=211, B=234	R=184, G=215, B=236
3	R=171, G=205, B=230	R=186, G=215, B=236	R=182, G=213, B=236	R=174, G=208, B=233	R=182, G=214, B=236	R=190, G=220, B=237
4	R=184, G=214, B=236	R=176, G=209, B=234	R=172, G=207, B=232	R=180, G=213, B=235	R=187, G=218, B=237	R=196, G=223, B=239
5	R=172, G=207, B=232	R=170, G=206, B=232	R=175, G=210, B=234	R=184, G=216, B=237	R=193, G=221, B=238	R=206, G=229, B=243

Subsequently, the detected and converted object will undergo encryption and decryption using the RSA algorithm

3.2 RSA Algorithm

Given the keys P and Q in the RSA algorithm, they can be seen as follows:

Step 1: Selection of Prime Numbers

$$p = 61$$
$$q = 53$$

Step 2: Calculating the Modulus (n)

Compute the value of the modulus n as the product of p and q:

$$n = p \times q = 61 \times 53 = 3233$$

Step 3: Calculating the Totient (φ)

Compute the value of the totient φ(n):

$$\phi(n) = (p-1) \times (q-1)$$
$$= (61 - 1) \times (53 - 1)$$
$$= 60 \times 52 = 3120$$

Step 4: Selecting the Public Exponent (e)

Select a value for the public exponent e that is relatively prime to φ(n).

Select e such that:

- $1 < e < \phi(n)$
- $gcd(e, \phi(n)) = 1$

For example, let e=17.

Because 17 and 3120 are relatively prime (gcd = 1)

Step 5: Calculating the Private Exponent (d)

Compute the value of the private exponent d using the Extended Euclidean Algorithm such that $e \cdot d \equiv 1 \, mod \phi(n)$

$$17 \cdot d \equiv 1 \, mod \, 3120$$

Or,

$$d = d.e \, mod \, \emptyset(n) = 1$$
$$d = d \, 17 \, mod \, 3120 = 1$$
$$= 2753.17 \, mod \, 3120 = 1$$
$$= 46.801 \, mod \, 3120 = 1$$

Thus, the value of d is obtained as 2753.

Using the Extended Euclidean Algorithm, we obtain:

$$d = 2753$$

The public and private key pair, with the given values, is as follows:

Public Key : $(e.n) = (17, 3233)$.

Private Key: $(d.n) = (2753, 3233)$

3.2.1 Encryption Process Using the RSA Algorithm

The following presents the encryption calculation using the combined algorithm:

RSA Algorithm Encryption Formula**:**

$$[\, \boldsymbol{C = M\text{^}e \; mod \; n} \,]$$

pixel (0,0)
Red = 142^{17} mod 3233= 1742
Green = 188^{17} mod 3233 = 3025
Blue = 220^{17} mod 3233 = 557
pixel (0,1)
Red = 153^{17} mod 3233 = 2727
Green = 195^{17} mod 3233 = 205
Blue = 224^{17} mod 3233 = 2101
pixel (0,2)
Red = 159^{17} mod 3233= 3180
Green = 198^{17} mod 3233 = 896
Blue =225^{17} mod 3233 = 2008
pixel (0,3)
Red = 170^{17} mod 3233 = 2637
Green = 205^{17} mod 3233 = 1765
Blue = 229^{17} mod 3233 = 1544
pixel (0,4)
Red = 191^{17} mod 3233= 455
Green = 219^{17} mod 3233 = 1998
Blue = 236^{17} mod 3233 = 155
pixel (0,5)
Red = 186^{17} mod 3233 = 601
Green = 216^{17} mod 3233 = 2341
Blue = 235^{17} mod 3233 = 712
pixel (1,0)
Red = 151^{17} mod 3233 = 2888
Green = 194^{17} mod 3233 = 1292
Blue = 224^{17} mod 3233 = 2101
pixel (1,1)
Red = 157^{17} mod 3233= 1958
Green = 197^{17} mod 3233 = 414
Blue = 225^{17} mod 3233 = 2008
pixel (1,2)
Red = 173^{17} mod 3233 = 429
Green = 206^{17} mod 3233 = 24
Blue = 230^{17} mod 3233 = 1782
pixel (1,3)
Red = 191^{17} mod 3233= 455
Green = 219^{17} mod 3233 = 1998
Blue = 237^{17} mod 3233 = 1840
pixel (1,4)
Red = 182^{17} mod 3233 = 182
Green = 213^{17} mod 3233 = 1909
Blue = 234^{17} mod 3233 = 1710
pixel (1,5)
Red = 182^{17} mod 3233= 182
Green = 214^{17} mod 3233 = 2971
Blue = 235^{17} mod 3233 = 712
pixel (2,0)
Red = 157^{17} mod 3233 = 1958
Green = 197^{17} mod 3233 = 414
Blue = 225^{17} mod 3233 = 2008
pixel (2,1)
Red = 171^{17} mod 3233= 405
Green = 205^{17} mod 3233 = 1765
Blue = 230^{17} mod 3233 = 1782
pixel (2,3)
Red = 181^{17} mod 3233= 2823
Green = 213^{17} mod 3233 = 1909

Blue = 235^{17} mod 3233 = 712

pixel (2,4)

Red = 178^{17} mod 3233 = 2099

Green = 211^{17} mod 3233 = 953

Blue = 234^{17} mod 3233 = 1710

pixel (2,5)

Red = 184^{17} mod 3233= 3112

Green = 201^{17} mod 3233 = 331

Blue = 236^{17} mod 3233 = 155

Subsequently, the encryption process is carried out up to pixel 6, starting from (pixel 5.0) and continuing through (pixel 5.5):

pixel (5,0)

Red = 172^{17} mod 3233 = 2856

Green = 207^{17} mod 3233 = 1578

Blue = 232^{17} mod 3233 = 161

pixel (5,1)

Red = 170^{17} mod 3233= 2637

Green = 206^{17} mod 3233 = 24

Blue = 232^{17} mod 3233 = 161

pixel (5,2)

Red = 175^{17} mod 3233 = 399

Green = 210^{17} mod 3233 =2382

Blue = 234^{17} mod 3233 =1710

pixel (5,3)

Red = 184^{17} mod 3233= 3112

Green = 216^{17} mod 3233 =2341

Blue = 237^{17} mod 3233 = 1840

pixel (5,4)

Red = 193^{17} mod 3233 = 2194

Green = 221^{17} mod 3233 = 647

Blue = 238^{17} mod 3233 = 2897

pixel (5,5)

Red = 206^{17} mod 3233= 24

Green = 229^{17} mod 3233 = 1544

Blue = 243^{17} mod 3233 = 304

The entire 6 × 6 pixel matrix has been encrypted using the RSA algorithm, thereby producing the cipher image shown below:

Table 2. Encrypted Cipher Image Matrix

	0	1	2	3	4	5
0	R=1742, G=3025, B=557	R=2727, G=205, B=2101	R=3180, G=896, B=2008	R=2637, G=1765, B=1544	R=455, G=1998, B=155	R=601, G=2341, B=712
1	R=2888, G=1292, B=2101	R=1958, G=414, B=2008	R=429, G=24, B=1782	R=455, G=1998, B=1840	R=182, G=1909, B=1710	R=182, G=2971, B=712
2	R=1958, G=414, B=2008	R=405, G=1765, B=2101	R=3025, G=2101, B=2008	R=2823, G=1909, B=1782	R=2099, G=953, B=155	R=3112, G=331, B=155
3	R=405, G=1765, B=1782	R=601, G=2907, B=155	R=182, G=1909, B=155	R=1017, G=3065, B=1453	R=182, G=2971, B=155	R=1576, G=557, B=1840
4	R=3112, G=2971, B=155	R=2816, G=909, B=1710	R=2856, G=1578, B=161	R=2937, G=1909, B=712	R=2241, G=2202, B=1840	R=2304, G=93, B=1184
5	R=2856, G=1578, B=161	R=2637, G=24, B=161	R=3999, G=2382, B=1710	R=3112, G=2341, B=1840	R=2194, G=647, B=2897	R=24, G=1544, B=304

The table above presents the data results that have been encrypted using the RSA algorithm.

3.2.2 RSA Decryption Process

The decryption process is presented below as follows:

RSA Algorithm Decryption Formula**:**

$[\boldsymbol{P = C\text{^}d \bmod n}]$

pixel (0,0)

Red = 1742^{2753} mod 3233 = 142

Green = 3025^{2753} mod 3233 = 188

Blue = 557^{2753} mod 3233 = 220

pixel (0,1)

Red = 2727^{2753} mod 3233 = 153

Green = 205^{2753} mod 3233 = 195

Blue = 2101^{2753} mod 3233 = 224

pixel (0,2)

Red = 3.180^{2753} mod 3233 = 159

Green = 896^{2753} mod 3233 = 198

Blue = 2008^{2753} mod 3233 = 225

pixel (0,3)

Red = 2637^{2753} mod 3233 = 170

Green = 1765^{2753} mod 3233 = 205

Blue = 1544^{2753} mod 3233 = 229

pixel (0,4)

Red = 455^{2753} mod 3233 = 191

Green 1998^{2753} mod 3233 = 219

Blue = 155^{2753} mod 3233 = 236

pixel (0,5)

Red = 601^{2753} mod 3233 = 186

Green = 2341^{2753} mod 3233 = 216

Blue = 712^{2753} mod 3233 = 235

pixel (1,0)

Red = 2888^{2753} mod 3233 = 151

Green = 1292^{2753} mod 3233 = 194

Blue = 2101^{2753} mod 3233 = 224

pixel (1,1)

Red = 1958^{2753} mod 3233 = 157

Green = 414^{2753} mod 3233 = 197

Blue = 2008^{2753} mod 3233 = 225
pixel (1,2)
Red = 429^{2753} mod 3233 = 173
Green = 24^{2753} mod 3233 = 206
Blue = 1782^{2753} mod 3233= 230
pixel (1,3)
Red = 455^{2753} mod 3233 = 191
Green = 1998^{2753} mod 3233 = 219
Blue = 1840^{2753} mod 3233 = 237
pixel (1,4)
Red = 182^{2753} mod 3233 = 182
Green = 1909^{2753} mod 3233 = 213
Blue = 1710^{2753} mod 3233= 234
pixel (1,5)
Red = 182^{2753} mod 3233 = 182
Green = 2971^{2753} mod 3233 = 214
Blue = 712^{2753} mod 3233 = 235
pixel (2,0)
Red = 1958^{2753} mod 3233 = 157
Green = 414^{2753} mod 3233 =197
Blue = 2008^{2753} mod 3233 =225
pixel (2,1)
Red = 405^{2753} mod 3233= 171
Green = 1765^{2753} mod 3233 = 205
Blue = 1782^{2753} mod 3233 = 230
pixel (2,2)
Red = 3025^{2753} mod 3233 =188
Green = 2132^{2753} mod 3233 =217
Blue = 155^{2753} mod 3233 =236
pixel (2,3)
Red = 1017^{2753} mod 3233= 181
Green = 3065^{2753} mod 3233 = 213
Blue = 1453^{2753} mod 3233 = 235
pixel (2,4)
Red = 2099^{2753} mod 3233 =178
Green = 953^{2753} mod 3233 =211
Blue = 1710^{2753} mod 3233 =234
pixel (2,5)
Red = 3112^{2753} mod 3233=184
Green = 331^{2753} mod 3233 =215
Blue = 155^{2753} mod 3233 = 236
Subsequently, the decryption process is carried out up to pixel 6, starting from (pixel 5.0) and continuing through (pixel 5.5).
pixel (5,0)
Red = 2856^{2753} mod 3233 =172
Green = 1578^{2753} mod 3233 =207
Blue = 161^{2753} mod 3233 =232
pixel (5,1)
Red = 2637^{2753} mod 3233=170
Green = 24^{2753} mod 3233 = 206
Blue = 161^{2753} mod 3233 = 232
pixel (5,2)
Red = 399^{2753} mod 3233 =175
Green = 2382^{2753} mod 3233 =210
Blue = 1710^{2753} mod 3233 = 234
pixel (5,3
Red = 3112^{2753} mod 3233=184)
Green = 2341^{2753} mod 3233 =216
Blue = 1840^{2753} mod 3233 = 237
pixel (5,4)
Red = 2194^{2753} mod 3233 =193
Green = 647^{2753} mod 3233 =221
Blue = 2897^{2753} mod 3233 =238
pixel (5,5)
Red = 24^{2753} mod 3233=206
Green = 1544^{2753} mod 3233 =229
Blue = 304^{2753} mod 3233 =243
The entire cipher image, after being processed through RSA decryption, is successfully reconstructed into the original image as shown below:

Table 3. Matrix of Decrypted Cipher Image Pixels Restored to the Original Image in the Detected Data

	0	1	2	3	4	5
0	R=142, G=188, B=220	R=153, G=195, B=224	R=159, G=198, B=225	R=170, G=205, B=229	R=191, G=219, B=236	R=186, G=216, B=235
1	R=151, G=194, B=224	R=157, G=197, B=225	R=173, G=206, B=230	R=191, G=219, B=237	R=182, G=213, B=234	R=182, G=214, B=235
2	R=157, G=197, B=225	R=171, G=205, B=230	R=188, G=217, B=236	R=181, G=213, B=235	R=178, G=211, B=234	R=184, G=215, B=236
3	R=171, G=205, B=230	R=186, G=215, B=236	R=182, G=213, B=236	R=174, G=208, B=233	R=182, G=214, B=236	R=190, G=220, B=237
4	R=184, G=214, B=236	R=176, G=209, B=234	R=172, G=207, B=232	R=180, G=213, B=235	R=187, G=218, B=237	R=196, G=223, B=239
5	R=172, G=207, B=232	R=170, G=206, B=232	R=175, G=210, B=234	R=184, G=216, B=237	R=193, G=221, B=238	R=206, G=229, B=243

The subsequent step involves applying the Convolutional Layer in the CNN. This is intended to simplify the explanation and presentation of the

computational procedures within the convolution layer

In the convolution process, a filter is applied to the image matrix. The pixel data from the three channels, namely red, green, and blue, are independently extracted, and zero-padding is added to preserve the spatial dimensions during the convolution operation.

Table 4. RGB Pixel Values of the Dataset from Image Detection on the Internet

Red Pixel

	0	1	2	3	4
0	R=142	R=153	R=159	R=170	R=191
1	R=151	R=157	R=173	R=191	R=182
2	R=157	R=171	R=188	R=181	R=178
3	R=171	R=186	R=182	R=174	R=182
4	R=184	R=176	R=172	R=180	R=187

Green Pixel

	0	1	2	3	4
0	G=188	G=195	G=198	G=205	G=219
1	G=194	G=197	G=206	G=219	G=213
2	G=197	G=205	G=217	G=213	G=211
3	G=205	G=215	G=213	G=208	G=214
4	G=214	G=209	G=207	G=213	G=218

Blue Pixel

	0	1	2	3	4
0	B=220	B=224	B=225	B=229	B=236
1	B=224	B=225	B=230	B=237	B=234
2	B=225	B=230	B=236	B=235	B=234
3	B=230	B=236	B=236	B=233	B=236
4	B=236	B=234	B=232	B=235	B=237

In this experiment, a 3 × 3 kernel is employed, with the values shown in table 4 below.

Table 5 . The 3×3 Convolution Kernel

1	**0**	**-1**
-1	**1**	**0**
0	**1**	**1**

The next step is to perform the computation in each channel by multiplying it with the 3×3 kernel shown in tabel 5. This process is iteratively conducted by shifting the kernel with a stride of 1 across each pixel (red, green, and blue) within the Convolution Layer, thereby obtaining the overall computation with the resulting values as follows:

Table 6. Results of Convolution Layer Calculations on Red, Green, and Blue Channels

Result = *Red* + *Green* + *Blue*

883	1210	1266	1298	671
1182	1225	1421	1385	1209
1243	1255	1370	1445	1243
1253	1199	1210	1272	1288
-3	-40	14	16	629

Following the convolution layer computations on the red, green, and blue pixels, the subsequent step involves applying the Rectified Linear Unit (ReLU) activation function. In this process, all negative valuesare converted to zero, resulting in the convolutional output shown in table 7:

Table 7. Output of Convolutional Layer after ReLU Transformation

883	1210	1266	1298	671
1182	1225	1421	1385	1209
1243	1255	1370	1445	1243
1253	1199	1210	1272	1288
-3	-40	14	16	629

$\mathcal{F}(z) = max\,(0, z)$

883	1210	1266	1298	671
1182	1225	1421	1385	1209
1243	1255	1370	1445	1243
1253	1199	1210	1272	1288
0	0	14	16	629

This process is iteratively performed on all images using 10 different filters, resulting in multiple feature maps as the output of the convolution stage. tabel 7 illustrates an example output of one such feature map. Subsequently to apply the Pooling Layer.

Table 8. Convolutional Layer after ReLU Transformation

883	1210	1266	1298	671
1182	1225	1421	1385	1209
1243	1255	1370	1445	1243
1253	1199	1210	1272	1288
0	0	14	16	629

From the results shown in table 8, the output of the convolution stage is used as the input for the pooling layer. In this stage, max pooling is applied with a kernel size of 2 × 2 and a stride of 2, based on the convolution output of 6 × 6 × 10. The illustration of the max pooling process is presented in Figure 9 below:

Journal of Theoretical and Applied Information Technology
30th November 2025. Vol.103. No.22

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

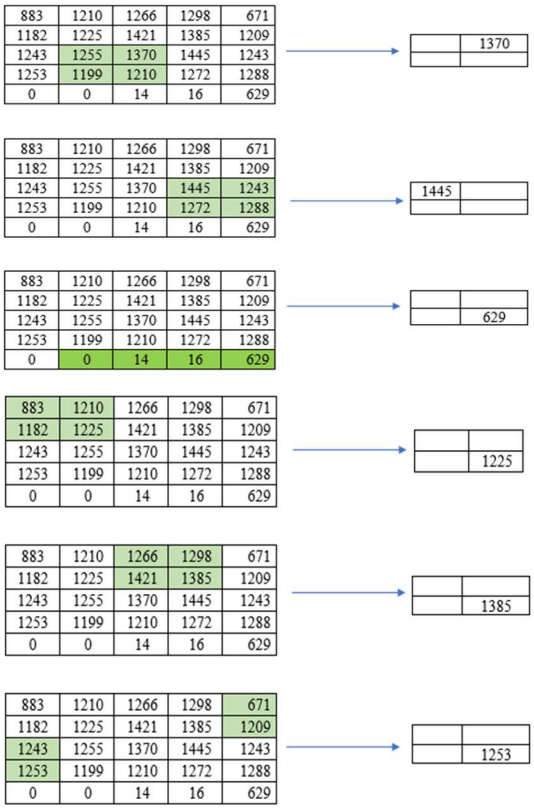

Figure 9. Illustration of the Max Pooling Process

From the above results, the next step is the Flatten Layer, which serves to transform the matrix into a one-dimensional vector/matrix. From the dropout layer output of size 6 × 6 × 10, a new vector representation is obtained. An illustrative depiction of this process is shown in Figure 9.

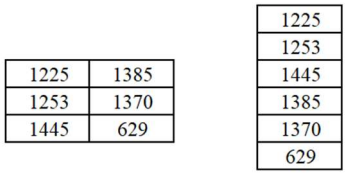

Figure 10. Illustration of Flatten Layer Computation

The next step is the process of the Fully Connected Layer. The output from the Flatten Layer, which is a one-dimensional vector, serves as the input to the Fully Connected Layer, resulting in three output layers. The following presents the computation results of the output layer with the predetermined weights.

The weights have been predetermined by the authors from the Hidden Layer to the Output.

The predefined weights from H to O are presented as follows:

$X_{10} = [0.1]$

$X_{20} = [0.2]$

$X_{30} = [0.3]$

1. Calculate the Output O_1

$$\boldsymbol{O_1} = (H_1.X_{10}) + (H_2.X_{20}) + (H_3.X_{30}) + (H_4.X_{40}) + (H_5.X_{50}) + (H_6.X_{60})$$
$$= (\mathbf{3288.15}\text{ x }0.1) + (\mathbf{5480.25}\text{ x }0.1) + (\mathbf{2192.10}\text{ x }0.1) + (\mathbf{4384.20}\text{ x }0.1) + (\mathbf{1096.05}\text{ x }0.1) + (\mathbf{3288.15}\text{ x }0.1)$$
$$\boldsymbol{O_1} = (328.815) + (548.025) + (219.21) + (438.42) + (109.605) + (328.815) = 1972.89$$

The obtained result $\boldsymbol{O_1}$: $\mathbf{1972.89}$

$$\boldsymbol{O_2} = = (\mathbf{3288.15}\text{ x }0.2) + (\mathbf{5480.25}\text{ x }0.2) + (\mathbf{2192.10}\text{ x }0.2) + (\mathbf{4384.20}\text{ x }0.2) + (\mathbf{1096.05}\text{ x }0.2) + (\mathbf{3288.15}\text{ x }0.2)$$
$$\boldsymbol{O_2} = (657.63) + (1096.05) + (438.42) + (876.84) + (219.21) + (657.63) = 3945.78$$

The obtained result $\boldsymbol{O_2}$: $\mathbf{3945.78}$

$$\boldsymbol{O_3} = (\mathbf{3288.15}\text{ x }0.3) + (\mathbf{5480.25}\text{ x }0.3) + (\mathbf{2192.10}\text{ x }0.3) + (\mathbf{4384.20}\text{ x }0.3) + (\mathbf{1096.05}\text{ x }0.3) + (\mathbf{3288.15}\text{ x }0.3)$$
$$\boldsymbol{O_3} = (986.445) + (1644.075) + (657.63) + (1315.26) + (328.815) + (986.445) = 5918.67$$

The obtained result : $\mathbf{5918.67}$

To conclude the output results above, the log-sum-exp method can be applied by subtracting all output values from the largest output value, as illustrated in the following simulation:

1. First Output

$$O^{1'} = 1972.89 - 5918.67 = -3945.78$$
$$\rightarrow \exp(O^{1'}) \approx 0(\text{very small, practically zero})$$

2. Second Output

$$O_2' = 3945.78 - 5918.67 = -1972.89$$
$$\rightarrow \exp(O_2')$$
$$\approx 0 \text{ (very small, practically zero)}$$

3. Third Output

$$O_3' = 0 \rightarrow \exp(O_3') = 1$$

Based on the softmax function results of the output values O_1, O_2, and O_3, it was obtained that class O_3 has a classification probability of approximately 1, while O_1 and O_2 are lower and also indicate the occurrence of an attack. This demonstrates that the CNN-based classification system successfully identifies the

key features accurately and consistently, with a high level of confidence in the detected target class. The model concludes that the input most certainly belongs to class O_3, with an almost 100% probability, thereby strongly confirming that the input corresponds to the 'file under attack' class.

This research still faces challenges in RSA performance for large data, limited datasets, and real-time intrusion detection in dynamic IoT environments. RSA and CNN integration may cause computational bottlenecks. Future research includes algorithm optimization for constrained devices, edge or fog computing systems, lightweight cryptography or blockchain integration, explainable AI adoption, and strengthening resilience against new threats including zero-day attacks.

4. CONCLUSION

This research successfully designed and implemented the integration of the RSA algorithm and Convolutional Neural Network (CNN) as a hybrid approach for intelligent data filtering in the Internet of Things (IoT) environment. The simulation results indicate that:

1. The system designed using the RSA encryption algorithm is capable of securing image data obtained randomly from the Internet of Things (IoT), where the filtered or detected data can be identified through random IP addresses. However, for large-capacity images, the encryption process still requires a considerable amount of time.
2. In this research, IoT data were secured using RSA encryption and classified with CNN. The simulation produced output O_1=−3945.78, O_2=−1972.89 and O_3= 0, applying the log-sum-exp and softmax methods yielded classification probabilities of 0% for O_1, 0% for O_2, and ≈100% for O_3, confirming CNN's high accuracy in detecting data and assigning the input almost certainly to class O_3 (file under attack).
3. The Hybrid RSA whit CNN integration exhibits advantages in both security (confidentiality) and classification (intelligent detection) simultaneously, thereby enhancing the reliability of IoT systems in addressing cybersecurity threats.

5. SUGGESTIONS

The suggestions in this study are as follows:

1. RSA performance optimization is necessary because encrypting large capacity images requires a long processing time and future research can focus on enhancing the algorithm through parallel processing techniques.
2. Future research is recommended to use larger and more diverse datasets to evaluate the consistency of accuracy, as well as to develop real-time attack detection systems in dynamic IoT environments by integrating additional security algorithms such as intrusion detection systems (IDS).
3. Future research is recommended to optimize the performance of the RSA and CNN hybrid algorithm for greater efficiency on resource constrained IoT devices, extend the system implementation for real-time attack detection, and evaluate its reliability under more complex cybersecurity threat scenarios using larger and more diverse datasets.

ACKNOWLEDGMENT

The authors would like to express their highest appreciation and sincere gratitude to the Directorate of Research and Community Service (DRPM), Directorate General of Research and Development Strengthening, Ministry of Research, Technology, and Higher Education of the Republic of Indonesia, for providing financial support through the Fundamental Research Grant (PFR), Fiscal Year 2024. The authors also wish to thank STMIK Kaputama for the valuable support provided during the implementation of this research activity.

REFERENCE

[1] H. Khair, M. Elveny, A. M. H. Pardede, S. Ramadani, and A. Fauzi, "Implementation of text data security using modular multiplication based block cipher modification," *J. Theor. Appl. Inf. Technol.*, vol. 15, no. 7, 2021.

[2] A. M. P. Achmad Fauzi, Yani Maulita, "Analisis Hybrid Cryptosystem Algoritma Algoritma Rsa Dan Triple Des," *J. Tek. Inform. Kaputama*, vol. 1, no. 2, pp. 36–44, 2017.

[3] A. Biju and S. W. Franklin, "Dual Feature-Based Intrusion Detection System for IoT Network Security," *Int. J. Comput. Intell. Syst.*, vol. 18, no. 1, pp. 1–19, Dec. 2025, doi: 10.1007/S44196-025-00790-Y/TABLES/6.

[4] M. A. Helmiawan, E. Firmansyah, and D. Herdiana, "Quantitative Analysis of the Key Factors Driving Cybersecurity Awareness Among Information Systems Users," vol. 6, no. 4, pp. 1897–1910, 2025.

[5] Prabowo and R. Gibran, "1276-Visi-Misi-Indonesia-Maju-2024-Final," 2024.

[6] H. K. Rani Rianda Br Ginting, Achmad Fauzi, "Penerapan Algoritma RSA Dan AES Dalam Pengamanan Data Tunggakan Tagihan PDAM Kota Binjai | Bulletin of Multi-Disciplinary Science and Applied Technology." Accessed: Mar. 27, 2025. [Online]. Available: https://ejurnal.seminar-id.com/index.php/bimasati/article/view/2476

[7] A. Fauzi and Y. Maulita, "Rivest Shamir Adleman (RSA) Super Encryption Algorithm with Vigenere Cipher Algorithm Modification for Image Security," vol. 4, no. 1, 2024.

[8] M. Rahmati, "Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities," Feb. 2025.

[9] C. Annamalai, C. Vijayakumaran, V. Ponnusamy, and H. Kim, "Optimal ElGamal Encryption with Hybrid Deep-Learning-Based Classification on Secure Internet of Things Environment," *Sensors*, vol. 23, no. 12, pp. 1–15, 2023, doi: 10.3390/s23125596.

[10] D. W. Pratama, A. Sudiarso, D. Sukma, and E. Atmaja, "Multi-architectural Transfer Learning CNN for Klowong Batik Fabric Defect Classification," vol. 6, no. 4, pp. 2123–2138, 2025.

[11] R. O. Tarigan and Achmad Fauzi, "Design And Development Of Karo Traditional Music Instrument Recognition Application Based On Digital Image Using Convolutional Neural Network Method," *J. Artif. Intell. Eng. Appl.*, vol. 3, no. 1, pp. 422–427, 2023, doi: 10.59934/jaiea.v3i1.348.

[12] R. Rosalina, A. Y. Husodo, and I. G. P. S. Wijaya, "Development of a Convolutional Neural Network Method for Classifying Ripeness Levels of Servo Variety Tomatoes," *J. Tek. Inform.*, vol. 6, no. 2, pp. 501–520, Apr. 2025, doi: 10.52436/1.JUTIF.2025.6.2.4168.

[13] N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," *Sensors 2025, Vol. 25, Page 79*, vol. 25, no. 1, p. 79, Dec. 2024, doi: 10.3390/S25010079.

[14] B. K. Rama and D. S. Thaiyalnayaki, "A Novel Integration Of Machine Learning - Based Data Classification With Optimized Cryptographic Techniques For Secure Cloud Storage," *J. Theor. Appl. Inf. Technol.*, vol. 15, no. 5, 2025.

[15] N. N. Albogami, "Intelligent deep federated learning model for enhancing security in internet of things enabled edge computing environment," *Sci. Rep.*, vol. 15, no. 1, p. 4041, Dec. 2025, doi: 10.1038/S41598-025-88163-5.

[16] Sigit Umar Anggono, Edy Siswanto, Laksamana Rajendra Haidar Azani Fajri, and Munifah, "User Interface Berbasis Web Pada Perangkat Internet Of Things," *Tek. J. Ilmu Tek. dan Inform.*, vol. 3, no. 1, pp. 35–54, 2023, doi: 10.51903/teknik.v3i1.326.

[17] C. Annamalai, C. Vijayakumaran, V. Ponnusamy, and H. Kim, "Optimal ElGamal Encryption with Hybrid Deep-Learning-Based Classification on Secure Internet of Things Environment," *Sensors 2023, Vol. 23, Page 5596*, vol. 23, no. 12, p. 5596, Jun. 2023, doi: 10.3390/S23125596.

[18] N. Dash, S. Chakravarty, and A. K. Rath, "Deep learning model for elevating internet of things intrusion detection," *Int. J. Electr. Comput. Eng.*, vol. 14, no. 5, pp. 5874–5883, 2024, doi: 10.11591/ijece.v14i5.pp5874-5883.

[19] H. F. A. and S. E. Sohail Aslam1, Maqsood Ahmad2, *Konsep dan Implementasi Internet of Things*, vol. 7, no. 2. 2021.

[20] H. ; Allioui, Y. Mourdi, H. Allioui, and Y. Mourdi, "Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey," *Sensors 2023, Vol. 23, Page 8015*, vol. 23, no. 19, p. 8015, Sep. 2023, doi: 10.3390/S23198015.

[21] D. Setyanto and P. Laksmini, "Studi Literatur Penggunaan Internet of Things (IoT) dalam Sektor Kesehatan," *Detect. J. Inov. Ris. Ilmu Kesehat.*, vol. 3, no. 1, pp. 26–37, Jan. 2025, doi: 10.55606/DETECTOR.V3I1.4783.

[22] A. T. Rosário and R. J. Raimundo, "The Integration of AI and IoT in Marketing: A Systematic Literature Review," *Electron. 2025, Vol. 14, Page 1854*, vol. 14, no. 9, p. 1854, May 2025, doi: 10.3390/ELECTRONICS14091854.

[23] T. Hidayat *et al.*, "Implementasi Enkripsi Data End-to-End pada Komunikasi Perangkat IoT Berbasis Lightweight Cryptography," *Pros. Semin. Nas. Teknol. Informasi, Mekatronika, dan Ilmu Komput.* ,

vol. 4, pp. 25–29, May 2025.

[24] A. Cahyadi Maseri, "Utilization Of Iot Technology To Support Interactive Learning And Management Of Facilities In Infrastructure In Islamic Educatio.," *Sibatik J. | Vol.*, vol. 4, no. 6, pp. 899–918, 2025.

[25] M. S. Ahsan and A. S. K. Pathan, "A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art," *Internet of Things*, vol. 6, no. 1, 2025, doi: 10.3390/iot6010009.

[26] A. Fauzi, *Asymmetric Cryptography: A Technical Analysis Of The RSA And Elgamal Algorithms*, no. 27. PT. Pustaka Pratama, 2025.

[27] M. Kumar *et al.*, "BBNSF: Blockchain-Based Novel Secure Framework Using RP2-RSA and ASR-ANN Technique for IoT Enabled Healthcare Systems," *Sensors 2022, Vol. 22, Page 9448*, vol. 22, no. 23, p. 9448, Dec. 2022, doi: 10.3390/S22239448.

[28] H. Small *et al.*, "Small Private Exponent Attacks on RSA Using Continued Fractions and Multicore Systems," *Symmetry 2022, Vol. 14, Page 1897*, vol. 14, no. 9, p. 1897, Sep. 2022, doi: 10.3390/SYM14091897.

[29] A. A. Hafiza and E. B. Setiawan, "Enhancing Cyberbullying Detection on Platform 'X' Using IndoBERT and Hybrid CNN-LSTM Model," *J. Tek. Inform.*, vol. 6, no. 2, pp. 655–672, Apr. 2025, doi: 10.52436/1.JUTIF.2025.6.2.4321.

[30] D. A. Wibowo, N. Suciati, and A. Yuniarti, "Hyperparameter Optimization Of Convolutional Neural Network For Flower Image Classification Using Grid Search Algorithms," *J. Tek. Inform.*, vol. 5, no. 1, pp. 313–320, Feb. 2024, doi: 10.52436/1.JUTIF.2024.5.1.1798.

[31] Y.-K. Lai, K. Hirata, M.-L. E. Alorvor, and S. Dadkhah, "Real-Time Phishing Detection for Brand Protection Using Temporal Convolutional Network-Driven URL Sequence Modeling," *Electron. 2025, Vol. 14, Page 3746*, vol. 14, no. 18, p. 3746, Sep. 2025, doi: 10.3390/ELECTRONICS14183746.

[32] C. H. Srilakshmi *et al.*, "A convolutional neural network with average pooling for chickpea disease detection and classification," *Int. J. Basic Appl. Sci.*, vol. 14, no. 1, pp. 156–165, May 2025, doi: 10.14419/pr4acd16.

[33] A. S. Lombu, I. V. Paputungan, and C. K. Dewa, "Predicting Fantasy Premier League Points Using Convolutional Neural Network And Long Short Term Memory," *J. Tek. Inform.*, vol. 5, no. 1, pp. 263–272, Feb. 2024, doi: 10.52436/1.JUTIF.2024.5.1.1792.

[34] R. . S. A M H PARDEDE, A FAUZI, Y MAULITA, "Optimization Of Public Service Model With Limited Resources Using Linear Programming," vol. 102, no. 21, pp. 7910–7922, 2024.