International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Integrating Machine Learning Algorithms with an Advanced Encryption Scheme: Enhancing Data Security and Privacy

Priyanka Rajan Kumar[1], Sonia Goel[2]

Submitted: 07/05/2023 **Revised**: 14/07/2023 **Accepted**: 07/08/2023

Abstract: Distributed computing is considered one of the most thrilling innovations considering its adaptability and versatility. The fundamental issue that happens in the cloud is security. To conquer the threats to security, another technique called Fog computing is developed. The concerns about privacy and security have become increasingly prominent in Fog, including data analysis and cryptography. One approach that has gained attention is the combination of logistic regression, a popular machine-learning technique, with cryptographic algorithms. This integration offers a powerful solution that addresses both privacy and security challenges. This paper explores the rationale behind the combination of logistic regression and cryptographic algorithms, highlighting their benefits and real-world applications. Here the hybrid combination of the (ECC+AES) algorithm and the application of logistic regression is applied to the data for security and the system's performance is measured in terms of encryption/ decryption time, and avalanche effect. The datasets of various kinds are thought of and applied the encryption method over those datasets, whole information over datasets is by and large precisely encoded and decoded back also. Subsequently, both best and worst-case scenarios among the datasets were analyzed, thus evaluating the suitability of the proposed model in a Fog environment.

Keywords: *Cloud Computing, Fog Computing, DES Algorithm, 3DES Algorithm, AES Algorithm, Encryption*.

1. Introduction

In today’s scenario, every association from huge scope to limited scope enterprises depends on distributed computing innovation [1] to store their information and utilize the assets according to their necessity. Cloud gives a pay-per-use idea. The number of gadgets associated with the web surpassed the total populace in the year 2010 and at present, it is twofold the total populace, and it would be around 50 billion gadgets associated with the web. It seems that currently, storing and retrieving data is sufficient. However, with the increasing number of internet-connected devices, there will likely be challenges in both data storage and recovery processes. Subsequently, to conquer the above issue the Fog processing idea has been presented in Fig. 1. In distributed computing idea every one of the information created by the clients will be straightforwardly put away into the cloud and afterward, the data is dissected within monstrous stockrooms, where examinations are conducted. Subsequently, decisions are made based on the information, and warnings are then issued to act upon those decisions. In Fog computing [2], clients are advised on the necessary actions to be taken based on the information. The Fog process involves the application accessing the information, rather than the information being delivered to the applications. Fog processing is intended to be an expansion of the cloud, not a substitution for it. The proliferation of internet-connected devices and advancements in the Internet of Things (IoT) has greatly contributed to the rapid increase in the number of gadgets. [3] In the future, the world will be filled with sensors, generating a massive amount of data, making it increasingly challenging to store and retrieve this data from the cloud. Subsequently, Fog has been introduced as a solution. For instance, currently, each airplane generates approximately 20 terabytes of data per hour, and storing all this data in the cloud poses significant challenges.[4] According to Cisco's prediction, in the following ten years, the Internet of Things will represent a $14.4 trillion worth of stake for organizations and businesses. The proliferation of devices generating a vast amount of data has driven the advancement of Fog computing within the Internet of Things. [5]

In distributed computing, there are numerous security issues, such as middle-man attacks, and surprisingly, the encryption of the information is not a foolproof method for securing the cloud. In distributed computing, there are various security concerns, including the lack of distinction between the client and the assailant, and it does not adequately prioritize the security of the information. [6,7] The cloud offers various services for storing and accessing data, but the main concern lies in its inability to provide sufficient security against attackers.[8] The lack of any

[1] *Department of Computer Science, Punjabi University, Patiala, Punjab, India*
[2] *Department of Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India*
* *Corresponding Author Email: srpriyankass@gmail.com*
* *Corresponding Author https://orcid.org/0000-0003-0421-0622*

degree of assurance to the client about the security of their information is concerning. Simply promoting a more profiled cloud is not sufficient, as there are persistent attacks occurring on the cloud, posing risks of data leaks or permanent loss.

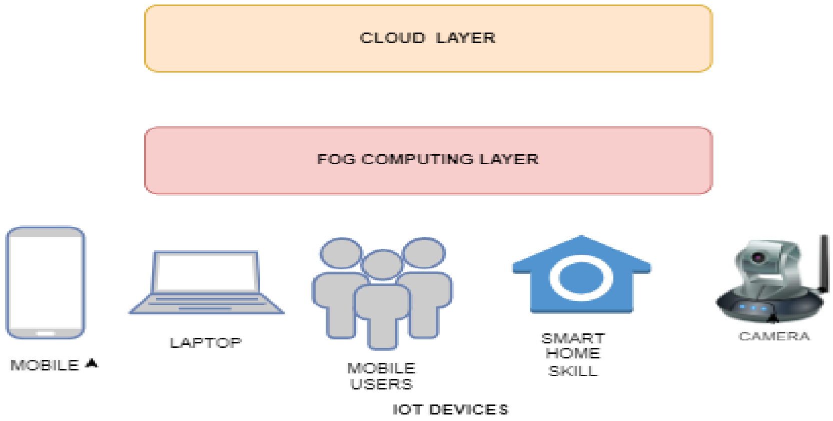

Fig. 1. Fog Computing Architecture

Consequently, Fog computing emerged as the most preferred form of data reservoir.[9]

Currently, various security techniques are being implemented in fog computing, each with its respective pros and cons. In Fog Computing, the Decoy framework is being utilized as the existing security framework for data authentication. The decoy framework is designed as a system of deception, wherein counterfeit components are strategically deployed to entice unauthorized users, thereby restricting unauthorized access to the network. It is a cycle where the records are filled with decoys and are included by the service provider. This decoy framework comprises counterfeit records with sensitive names, such as social security numbers and credit card details, used as file names. These decoy components are designed to be enticing to potential attackers, who may click on them and attempt to download the file. Once the file is downloaded, an alert is triggered, notifying the system of the attack. This decoy framework strategy has been integrated with client behavior profiling, ensuring that any unauthorized access is promptly reported to the system. There are still a few issues with the current strategy, leading to hacking and unauthorized access to information in the fog. This has prompted us to consider data encryption in the fog framework. Therefore, with this approach, our aim is to achieve enhanced security at the Fog tier by introducing encryption to the data using a Hybrid Encryption algorithm combined with a machine learning model. The paper introduces the proposed security model algorithm in the Fog environment. According to this model, when the user sends data to the Fog for storage in the cloud, the data will be encrypted by the Fog before transmission to the cloud. Additionally, whenever the client requests the data, the encrypted information travels from the cloud to the fog and finally to the end-user, where it will be decrypted.

This paper focuses primarily on implementing this algorithm on mobile phones as end clients. It also demonstrates the suitability of different types of datasets for this encryption process by evaluating their performance in encryption. It involves analysing the best and worst potential cases for each of the datasets to assess the feasibility of the proposed model in the Fog environment. This paper enhances data security by introducing a security model algorithm in Fog computing. This ensures that the end user's data remains more secure during its journey from the cloud to the Fog or from the Fog to the cloud. The paper is structured as follows: Section 2 presents the literature review, where various types of encryption standards currently available are discussed, along with the reasons for choosing the (ECC+AES) hybrid algorithm over other encryption principles. Section 3 provides Research methodology, Section 4 gives the problem definition, in which the paper outlines the current issue in Fog computing and defines our proposed technique to overcome the problem. Section 5 details the implementation results of the algorithm and the datasets used for encryption and decryption. Section 6 describes the conclusion, showcasing the metrics utilized to calculate the algorithm's effectiveness.

2. Literature Review

The various encryption techniques have been studied to see their structure, key size, round, block size, and flexibility so that encryption algorithms can be chosen for achieving security in the Fog environment. A comparison table is drawn out of the study of these algorithms. Table 1 depicts the comparison among various algorithms based on certain features enlisted in the table.

Data Encryption Standard (DES) was once the most widely used encryption standard, employing a symmetric key algorithm for data encryption. It was considered a fundamental building block for the development of modern cryptography in today's world. [17] DES has a key size of 56 bits and a block size of 64 bits. For certain applications, DES is considered to be the least secure strategy due to its relatively small key size, which poses a significant constraint. In fact, two organizations collectively managed to break the DES algorithm's key in just 22 hours and 12 minutes, highlighting its weakness. Some attacks that can break the key faster than brute force include Differential Cryptanalysis, Linear Cryptanalysis, and Improved Davies Attack. The predecessor of the DES algorithm is 3DES [6], which is known as Triple Data Encryption Standard. Triple DES made no significant changes to the previous DES algorithm except for an increase in the key size, which can be 56 or 112 or 168 bits, while the block size remains the same as DES at 64 bits. Triple DES was expected to be 2½ times more secure than the DES algorithm. However, even Triple DES is vulnerable to security compromise attacks.[17]

To address the aforementioned issue, the Advanced Encryption Standard (AES) is considered significantly more powerful. [21] It is regarded as the most advanced standard for electronic data encryption and is considered a replacement for DES in many US government agencies, utilizing standard symmetric key encryption. AES supports key sizes of 128, 192, and 256 bits. While 128 bits are currently considered robust, several open contests were held by numerous organizations to attempt to break the key, but they were never successful. After comparing all the available encryption algorithms, AES emerges as the superior and most suitable choice to be implemented in the Fog environment.

Elliptic curve cryptography, ECC, is a dual-key cryptosystem that utilizes a pair of two keys to encode and decode the information.[20] ECC has the primary advantage of a shorter key size, which offers increased security while requiring less computational cost. The benefits of both ECC and AES are combined to form a hybrid combination of the (ECC+AES) algorithm, which has been proposed.

Cryptographic algorithms have been compared with each other for performance evaluation on the basis of the number of keys used, keys in bits, rounds, and limitations. A comparative analysis of various algorithms is being conducted to evaluate their performance and space optimization capabilities in the context of Fog storage. The comparison is shown in Table 2.

Logistic regression is a statistical model used for binary classification tasks, where the goal is to predict the probability of an event occurring based on a set of input variables. It is called "logistic" regression because it uses the logistic function, also known as the sigmoid function, to transform the output into a probability value between 0 and 1. In logistic regression, the dependent variable is binary, meaning it can take only two possible outcomes: yes/no, true/false, or 0/1. The independent variables can be categorical or continuous, and they are used to estimate the probability of the binary outcome. The logistic regression model assumes a linear relationship between the independent variables and the log odds of the dependent variable. The log-odds, also known as the logit function, is the logarithm of the odds ratio, which is the probability of the event occurring divided by the probability of it not occurring. The logistic function then transforms the log odds into a probability value.[11]

Logistic regression is a powerful and interpretable model that can be applied in various fields where binary classification or probability estimation is required.[15] The reason to combine logistic regression with the encryption algorithm is to enhance the security and privacy of the data being transmitted and stored in the Fog environment. Logistic regression is a machine learning algorithm commonly used for classification tasks. By integrating logistic regression with the encryption algorithm, it enables the system to analyze and make predictions based on the encrypted data while preserving the confidentiality of the sensitive information. This combination allows for secure data processing and decision-making without compromising the privacy of the data.

Table 1. Basic Comparison of Encryption Techniques

ALGORITHM	DES **[17]**	Diffie Hellman **[18]**	**RSA** **[18]**	**3DES** **[17]**	**ECC** **[20]**	**RC2** **[17]**	**RC4** **[17]**	**IDEA** **[19]**	**BLOWFISH** **[19]**	**AES** **[21]**
YEAR	1975	1976	1977	1978	1985	1987	1987	1991	1993	2001
INVENTED BY	IBM	Whitefied Diffie, Hellman	Rivest, Shamir, Adleman	IBM	Miller, Koblitz	Ron Rivest	Ron Rivest	James Massey	Bruce Schneier	Vincent Rijmen, Joan Daemen

SIZE OF KEY	64 bits	1024 to 4096 bits	1024 to 4096 bits	112 or 168	Smaller key size	8 to 128, 64 by default	variable	128 bits	32-448	128, 192, 256
ROUND	16	-	1	48	-	16	256	8.5	16	10,12,14
BLOCK SIZE	64 bits	512	128	64		64	40-2048	64 bits	64 bits	128 bits
STRUCTURE	Feistel	Asymmetric algorithm	Public key	Feistel	Public key	Feistel	Feistel	Feistel	Feistel	Symmetric block cipher
FLEXIBILITY	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes
FEATURES	Not strong	Attacks can be there	Security is Excellent Speed is low	Secure	Faster, Security is excellent	Stream cipher	Stream cipher	Less strong	Security is excellent	Faster, Security is excellent

Table 2. Comparison of different Cryptographic Algorithms

FACTORS	PROPOSED {(ECC+AES) + MACHINE LEARNING}	RSA	BLOWFISH	AES	Diffie-Hellman
No. of keys	1	2	1	1	Key Exchange
Key length in bits	64–256	1024	32-448	128,192,256	Key Exchange
Rounds	10	1	16	10,12,14	56
Limitation	Brute force	Key generation weak	Key frequently changing	Brute force	Cannot encrypt data

3. Research Methodology

In this section, we present the research design adopted for this paper, including the methodology for the proposed approach, which will be further detailed in the subsequent section. Fig. 2 illustrates the conventional research methodology commonly employed, encompassing the comprehensive process of reviewing existing schemes and validating the proposed one. This systematic approach ensures a rigorous investigation and reliable results. The Fog environment has been created for the implementation of security algorithms. During this analysis, several limitations were identified in these existing schemes, particularly concerning the significant computation overhead and time required for their execution. While various other limitations were observed, the focus was on addressing a select few of the primary issues. To overcome these challenges, the paper proposes a new advanced encryption approach named (ECC+AES) integrated with machine learning, specifically designed to enhance data security over Fog storage.

An experimental setup was devised to evaluate the effectiveness of the proposed hybrid scheme, allowing for a comparison with other methods and existing hybrid schemes. Through rigorous testing, the results demonstrated that our proposed (ECC+AES) encryption scheme along with machine learning outperforms other security schemes in terms of both performance and efficiency. This highlights the potential of the proposed approach to provide a more secure and efficient solution for data protection in a Fog computing environment.

4. Proposed Framework

The security of data is a critical concern that can be vulnerable to compromise through various methods, whether from external sources or internal actors. To safeguard the transmission of data over the Internet, various encryption techniques are employed. The challenge with these techniques lies in their reliance on large key sizes, extensive memory requirements, and substantial computational power, all necessary to ensure data protection.

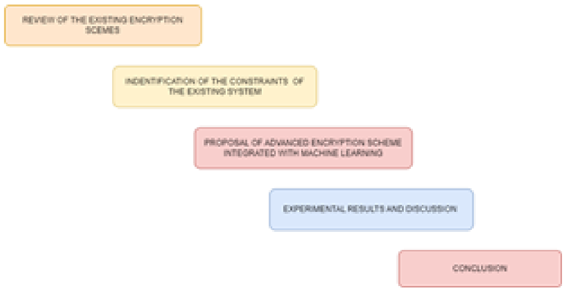
REVIEW OF THE EXISTING ENCRYPTION SCEMES
INDENTIFICATION OF THE CONSTRAINTS OF THE EXISTING SYSTEM
PROPOSAL OF ADVANCED ENCRYPTION SCHEME INTEGRATED WITH MACHINE LEARNING
EXPERIMENTAL RESULTS AND DISCUSSION
CONCLUSION

Fig. 2. Research Methodology

An evaluation has been conducted within the Fog environment to assess the effectiveness and efficiency of various encryption algorithms, including RSA, AES, and Blowfish. Additionally, hybrid encryption schemes involving the combination of RSA with AES and RSA with Blowfish have also been implemented. The objective of this evaluation is to analyze both the security and performance aspects of these encryption methods. The performance and security analysis encompasses multiple dimensions, considering factors such as encryption and decryption speed, computational resources required, and the level of data protection offered. Through this comparison, a comprehensive understanding of the strengths and weaknesses of each encryption approach can be obtained. The findings of this study will contribute to making informed decisions regarding the selection of encryption algorithms or hybrid schemes in Fog computing environments, aligning with the overarching goal of enhancing data security and system efficiency.

Table 3. presents a comprehensive overview of the compared parameters and their corresponding results. The table encapsulates the outcomes of the evaluation process conducted on the various encryption algorithms and hybrid encryption schemes within the Fog environment. This data-driven representation aids in the clear visualization and understanding of the performance and security aspects of the cryptographic methods under consideration.

Table 3. Comparison of Encryption Decryption Time and Throughput of RSA, AES, BLOWFISH, (RSA+AES), and (RSA+BLOWFISH) algorithms

ALGORITHM/ FILE SIZE(KB)		RSA	AES	BLOWFISH	RSA+AES	RSA+BLOWFISH
1	Encryption Time (ms)	200	83.33	168	13	5
	Decryption Time (ms)	166.67	62.51	4	2	3
	Encryption Throughput	0.005	0.012	0.005	0.0769	0.2
	Decryption Throughput	0.006	0.016	0.25	0.5	0.333
100	Encryption Time (ms)	675.67	243.9	171	39	27
	Decryption Time (ms)	452.62	191.2	26	21	11
	Encryption Throughput	0.148	0.41	0.584	2.56	3.703
	Decryption Throughput	0.219	0.523	3.846	4.761	9.090
1000	Encryption Time (ms)	1915.71	505.05	186	68	88
	Decryption Time (ms)	1360.54	429.18	47	74	115
	Encryption Throughput	0.148	1.98	5.376	14.70	11.363
	Decryption Throughput	0.735	2.33	21.276	13.513	8.695

In AES encryption, a key is generated shortly after the input file is uploaded, and it utilizes a symmetric key encryption method where a single key is employed for both encryption and decryption processes. Consequently, if the single key becomes known to a third party, they can easily decrypt the input file and re-encrypt it without the user's knowledge, potentially compromising the confidentiality of the data. Despite AES being considered one of the secure algorithms, its security can be compromised if the single key used for encryption and decryption becomes known to unauthorized individuals. On the other hand, Elliptic Curve Cryptography (ECC) employs asymmetric key encryption, utilizing a pair of keys for encryption and decryption, known as the public key and private key, respectively. This is the reason why ECC offers a higher security level, as it becomes challenging for hackers to simultaneously crack both the public and private keys, enhancing the overall security of the encryption scheme. ECC is also renowned for its smaller key size, as it can deliver the same level of security as other algorithms but with a reduced key size requirement. There is a compelling need to develop a system that ensures data security over the Fog while minimizing computational costs and reducing the time required for the encryption/decryption process. We combine the advantageous properties of both algorithms and incorporate them into our proposed model.

Machine Learning (ML) is a sub-category of artificial intelligence that encompasses the process through which computers acquire pattern recognition capabilities, enabling them to learn from data, make predictions, and adapt their behavior without explicit programming. [15] Logistic regression is applied to the data set for classification. Logistic regression is a classification algorithm. It is used to predict a binary outcome based on a set of independent variables. A binary outcome is one where there are only two possible scenarios—either the event happens (1) or it does not happen (0). Independent variables are those variables or factors which may influence the outcome (or dependent variable). So, Logistic regression is the correct type of analysis to use when you are working with binary data. Logistic regression is used to calculate the probability of a binary event occurring and to deal with issues of classification. Logistic regression is much easier to implement than other methods, especially in the context of machine learning. Logistic regression works well for cases where the dataset is linearly separable. Logistic regression provides useful insights. An (ECC+AES) hybrid algorithm has been implemented along with a logistic regression algorithm to achieve both data security and performance in a Fog environment.

In Fig. 3, the encryption method has been chosen to be applied to the data in the Fog environment for enhanced security. The objective of the research is to achieve security in the fog, which represents the second level of the cloud infrastructure. This is accomplished by utilizing the (ECC+AES) hybrid encryption algorithm along with logistic regression and applying it to the selected datasets, which are deployed on a mobile edge device. Performance metrics are then collected from the datasets, allowing for the evaluation of best and worst-case scenarios in various aspects of the datasets.

Different datasets, containing various sizes of information are chosen for testing the encryption technique. Execution is assessed for these datasets. The best and worst potential cases are examined by assessing encryption/decryption time, and avalanche effect for each dataset. Combining logistic regression with cryptographic algorithms can offer several advantages in various applications. Logistic regression is a popular machine learning algorithm used for classification tasks, while cryptographic algorithms provide secure data protection and confidentiality. By integrating the two, we can achieve secure and privacy-preserving machine learning tasks.

Algorithm for the Proposed Framework

1. The generation of a Public Key using Elliptic Curve Cryptography follows these steps:

Step I. Choose a prime number 'n'.

Step II. Select a number 'a' for the generation of the public key, where 'a' is less than 'n', (a<n).

Step III. Calculate the point 'G' on the curve, where 'G' is greater than 'n', (G>n)

Step IV. Compute the public key as: P = (G * a)

Step V. Return the public key 'P' after the calculation.

2. The Encryption and Decryption process using Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) can be summarized as follows:

Step I. Take the input file.

Step II. Apply logistic regression to the input file.

Step III. Add the public key generated by ECC to the input file.

Step IV. Perform AES encryption on the input file using the ECC-generated public key.

Step V. Upload the encrypted file to the Fog node after AES encryption.

Step VI. When the file is downloaded from the Fog node, it is decrypted using the ECC public key to obtain the original file.

Step VII. The system's performance is influenced by the combined effect of ECC and AES, leading to benefits like optimized storage space and enhanced security services in the fog.

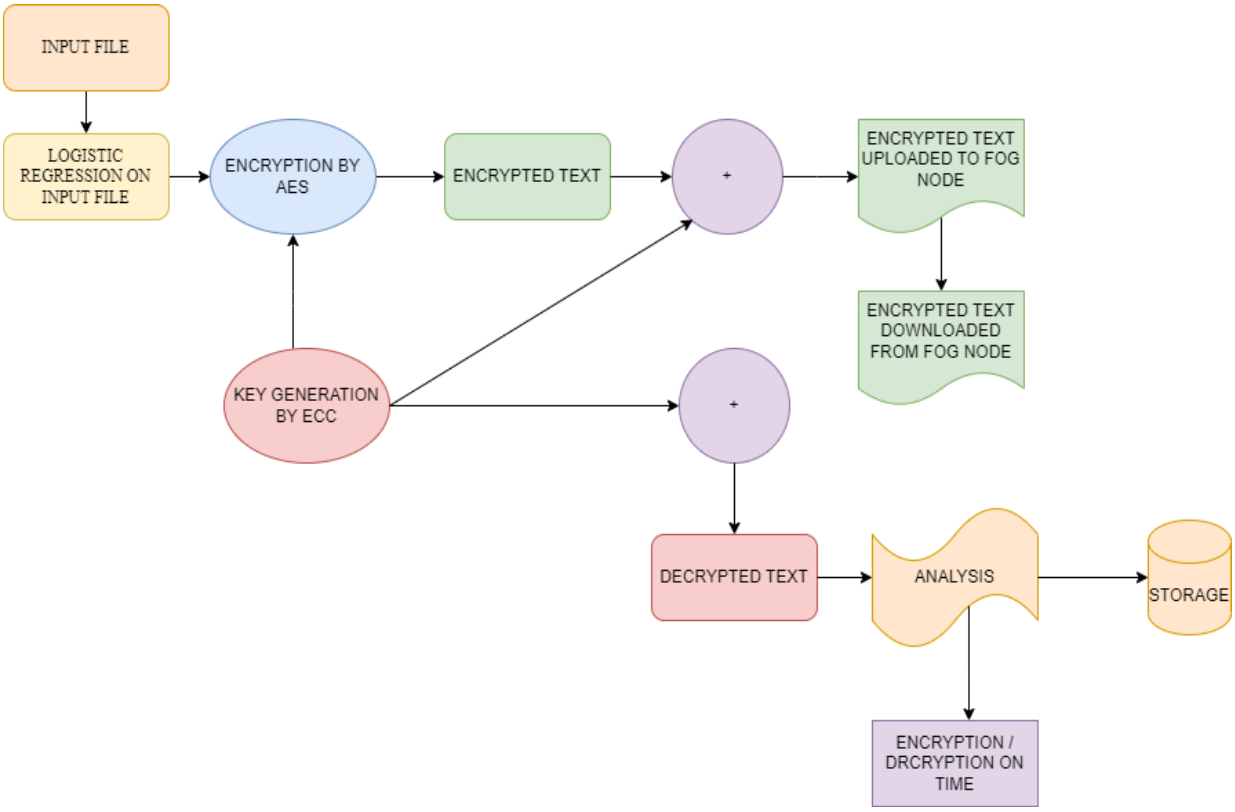
INPUT FILE
LOGISTIC REGRESSION ON INPUT FILE
ENCRYPTION BY AES
ENCRYPTED TEXT
+
ENCRYPTED TEXT UPLOADED TO FOG NODE
ENCRYPTED TEXT DOWNLOADED FROM FOG NODE
KEY GENERATION BY ECC
+
DECRYPTED TEXT
ANALYSIS
STORAGE
ENCRYPTION / DRCRYPTION ON TIME

Fig. 3. Representation of ECC and AES algorithm

One potential approach is to use logistic regression as a classification model for encrypted data. The data is encrypted using cryptographic algorithms before being processed by the logistic regression model. This allows the model to make predictions on the encrypted data without revealing the sensitive information it contains. Various cryptographic techniques such as homomorphic encryption or secure multiparty computation can be employed to perform computations on the encrypted data, enabling logistic regression to operate on encrypted inputs while maintaining data privacy. Another approach is to use logistic regression in conjunction with cryptographic techniques for secure model training. The training process involves encrypting the training data and performing computations on the encrypted data to update the model parameters. This ensures that the sensitive data used for training remains protected throughout the process. Techniques like secure aggregation or secure gradient descent can be employed to collectively update the model parameters while preserving data privacy. By combining logistic regression with cryptographic algorithms, we can leverage the advantages of both techniques: the predictive power of logistic regression and the data security provided by cryptographic algorithms. This enables the development of applications that necessitate privacy-preserving machine learning, such as healthcare analytics, financial analysis, or collaborative data sharing among multiple parties.

5. Experimental Results and Discussion

The combination of ECC and AES in our system enhances its uniqueness and efficiency in a distinct manner. By employing these two techniques, we achieve a higher level of data security for Fog storage, ensuring secured connections for both encryption and decryption processes. As a result, users can easily retrieve the original message with confidence, knowing that their data remains well-protected throughout its transmission and storage. The synergistic effect of ECC and AES along with machine learning provides a robust and user-friendly solution, ensuring the confidentiality and integrity of the data in a seamless manner.

1. Advantages of ECC and AES:

ECC offers significant advantages in ensuring data security for Fog storage. One notable benefit is the reduced key size, leading to optimized storage space utilization and efficient results. With the same level of security provided by a 3072-bit RSA key, ECC achieves this with a smaller key size. The encryption process, leveraging a public key, is also optimized for efficiency. Comparatively, ECC surpasses RSA in utilizing the latest algorithmic techniques for encryption and decryption, resulting in improved accuracy of decrypted data. On the other hand, AES is widely regarded as a high-performing encryption algorithm, specifically tailored for Fog nodes. It addresses various performance-related operations on Fog, such as statistical analysis and searching, effectively bolstering the overall security measures for Fog computing environments. Both ECC and AES offer the convenience of public key usage, enabling anyone with the public key to perform encryption and decryption operations. This user-friendly approach ensures that data transmission and access remain secure while maintaining simplicity in the encryption/decryption processes.

The integration of machine learning with the combination of ECC and AES further enhances the system's capabilities by optimizing resources. Machine learning algorithms can analyze patterns and behaviors in data usage, enabling the system to make intelligent decisions in resource allocation and utilization. Overall, the integration of machine learning with the combination of ECC and AES not only enhances data security but also enables resource optimization, making the system more robust and efficient in Fog computing environments. The key sizes of ECC over RSA are given in Table 3.

ECC offers enhanced security over RSA due to its requirement for a medium key size. (ECC+AES) in particular, achieves better security with smaller key sizes than many other cryptographic algorithms, optimizing memory space and reducing computational complexity. As a result, utilizing a medium key size in ECC can yield a high level of data security.

Table 3. Comparison of key sizes of ECC and RSA

ECC	**RSA**	**Key Size Comparison**
160	**1024**	**01:06**
256	**3024**	**01:12**
384	**7068**	**01:20**
512	**16360**	**01:20**

2. Encryption Decryption Time with Varying File Sizes:

In order to validate and confirm the effectiveness of our proposed hybrid algorithm, we conducted a thorough analysis of encryption and decryption times using various key sizes. A comparison was conducted among the proposed algorithm, the encryption methods outlined in the base paper, and the well-established encryption algorithms ECC (Elliptic Curve Cryptography) and Blowfish. For our tests, we used file sizes of 6.4 MB, 12.8 MB, 19.2 MB, and 25.6 MB.

To present the results, Tables 4 and 5 display the encryption and decryption times in seconds for all the algorithms and file sizes. Furthermore, we have included graphical representations of these values in Figures 4 and 5 to aid in a clearer comprehension and interpretation of the data regarding encryption and decryption times in seconds.

Table 4. Encryption time(s) calculated using different file sizes.

FILE SIZES (MB)	**PROPOSED {(ECC+AES) + MACHINE LEARNING}**	**BASE PAPER (ECC + AES)**	**ECC**	**BLOWFISH**
6.4	2.3	2.44	3.32	4.13
12.8	2.17	2.37	3.39	4.3
19.2	2.45	2.69	3.95	4.35
25.6	2.5	2.7	3.7	4.78

Table 5. Decryption time (s)calculated using different file sizes.

FILE SIZE (MB)	**PROPOSED {(ECC+AES) + MACHINE LEARNING }**	**BASE PAPER (ECC + AES)**	**ECC**	**BLOWFISH**
6.4	1.63	1.73	2.69	3.89

12.8	1.7	1.86	2.89	3.94
19.2	1.9	2	2.93	4.1
25.6	2.05	2.2	3.1	4.26

3. Encryption/Decryption Time of varying Image Sizes: To assess the computational efficiency and compare the performance of various algorithms in image encryption and decryption, the time required for these processes is measured. Due to the inherent complexity of encrypting and decrypting image data with high accuracy, determining the most efficient algorithm becomes crucial. Image encryption and decryption processes were performed on images of varying sizes, namely 1870KB, 2688KB, 3295KB, and 3750 KB. The goal was to analyze the performance of different algorithms and assess their computational efficiency in handling image data of different complexities. Fig. 6 and Fig. 7 visually present the image processing results in a graphical format, illustrating the outcomes of the encryption and decryption processes.

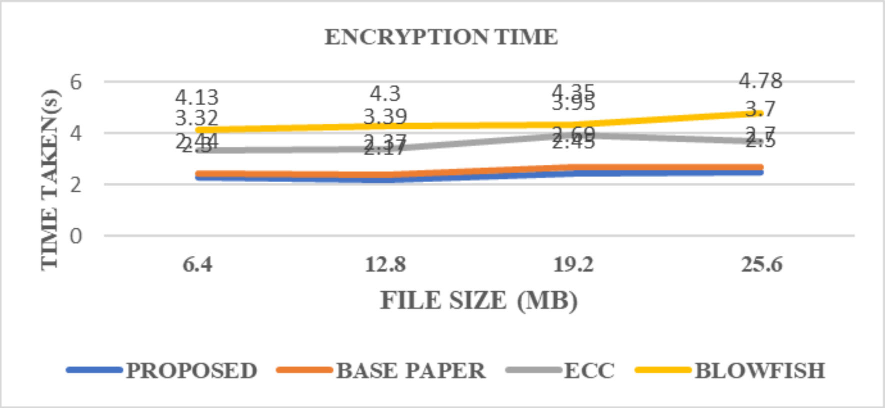

Fig. 4. Comparison of Encryption Time Between Proposed and Existing Algorithms Across Various File Sizes

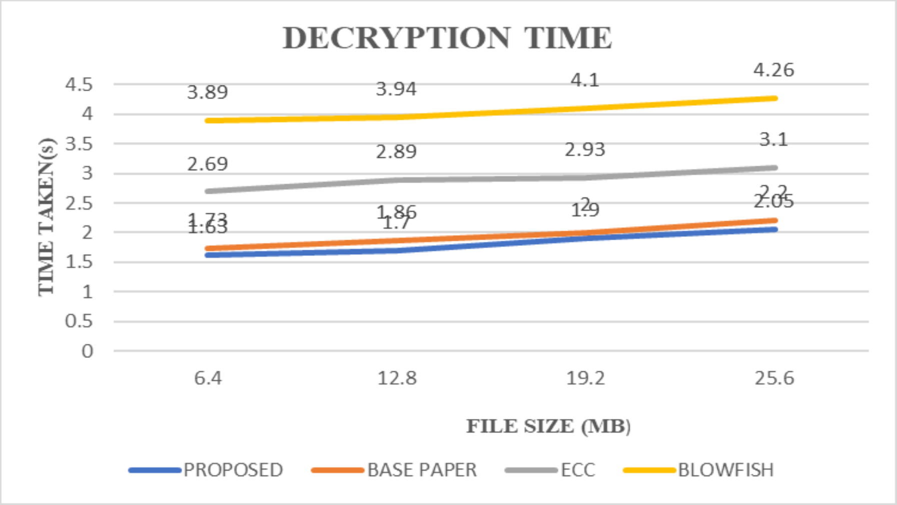

Fig. 5. Comparison of Decryption Time Between Proposed and Existing Algorithms Across Various File Sizes

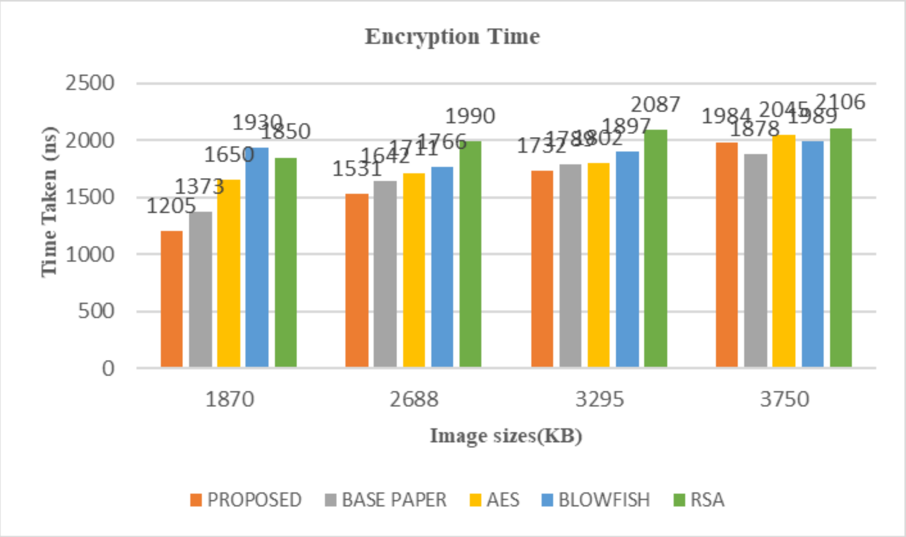

Fig. 6. Comparison of Encryption Time Between Proposed and Existing Algorithms Across Various Image Sizes

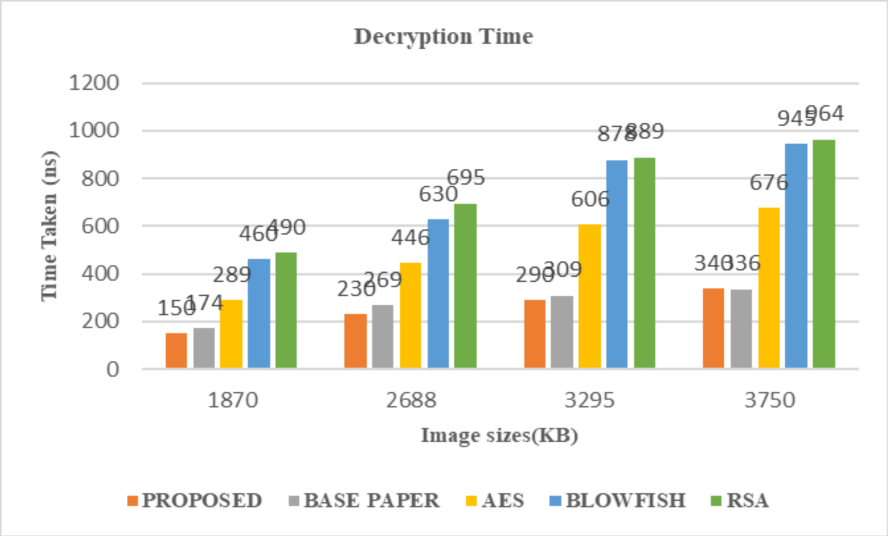

Fig. 7. Comparison of Decryption Time Between Proposed and Existing Algorithms Across Various Image Sizes

4. Avalanche Effect: The avalanche effect in cryptography refers to the phenomenon where a small change in the input of a cryptographic function, results in a significant and seemingly unrelated change in the output. This property is desirable in cryptographic functions because it makes it difficult for an attacker to predict the output of the function based on partial knowledge of the input. The formula by which we calculated the avalanche effect of our proposed algorithm.

Av = number of changed bits/total number of bits

An avalanche effect of more than 50% indicates that a certain algorithm has more security power than others.

Table 6 presents the avalanche effect observed when changing a single bit of the encryption key, while Table 7 displays the avalanche effect when altering a single bit in the plaintext.

Table 6. Avalanche effect 1-bit key change

ENCRYPTION ALGORITHM	1-BIT KEY CHANGE	AVALANCHE EFFECT
PROPOSED	73	0.61
BASE PAPER	68	0.55
AES	64	0.51
BLOWFISH	37	0.29

Table 7. Avalanche effect 1-bit Plain text change

ENCRYPTION ALGORITHM	1-BIT PLAINTEXT CHANGE	AVALANCHE EFFECT
PROPOSED	83	0.64
BASE PAPER	71	0.56
AES	70	0.55
BLOWFISH	23	0.18

6. Conclusion

IT-related services, such as Fog computing, offer efficient solutions that require minimal technical knowledge from users. These services enable data storage, management, and accessibility through user-friendly Fog nodes provided by Fog computing service providers via the Internet, regardless of the user's location. Fog computing services cater to a wide range of users, each benefiting from different types of Fog nodes. Notably, these services are cost-effective and allow users to access their data from anywhere, eliminating the need to carry specific devices. However, one significant drawback of Fog is the potential risk to data security, which can be mitigated through specialized strategies and robust security measures. The use of Elliptic Curve Cryptography (ECC) to generate keys has proven beneficial in reducing operational complexities due to its smaller key size, making it more efficient than other cryptographic techniques. Combining Advanced Encryption Standard (AES) with Elliptic Curve Cryptography (ECC) along with machine learning further enhances data optimization and security.

Looking ahead, the continued expansion of Fog computing through cryptographic techniques will demand heightened security measures. Future research can focus on enhancing the security of the hybrid approach by incorporating multiple security layers to bolster the system's productivity and efficiency. By addressing these security challenges, Fog computing's potential can be fully realized, providing even more reliable and secure IT services to users worldwide. The combination of logistic regression with cryptographic algorithms presents a promising approach to address privacy and security concerns in data analysis. By leveraging the strengths of both domains, organizations and researchers can achieve a balance between data utility and protection. Understanding the benefits, challenges, and real-world applications of this integration paves the way for novel solutions that ensure privacy and security in an increasingly data-driven world.

References

[1] .Lee and K. Lee, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises,” Business Horizons, vol. 58, no. 4, pp. 431–440, (2015).

[2] J. Ahamed and A. V. Rajan, “Internet of Things (IoT): Application systems and security vulnerabilities,” in Proc. 2016 5th Int. Conf. on Electronic Devices, Systems and Applications (ICEDSA), Ras Al Khaimah, United Arab Emirates, pp. 1–5, (2016).

[3] S. Wang, Y. Hou, F. Gao, and X. Ji, “A novel IoT access architecture for vehicle monitoring system,” in *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, pp. 639–642, Reston, VA, USA, (2016).

[4] Tekeoglu and A. S. Tosun, “An experimental framework for investigating security and privacy of IoT devices,” in Proc. Int. Conf. on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments, Vancouver, BC, Canada, pp. 63–83, (2017).

[5] M. Frustaci, P. Pace, G. Aloi and G. Fortino, “Evaluating critical security issues of the IoT world: Present and future challenges,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483–2495, (2018).

[6] Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., Priyan, M.K.: Centralized fog computing security platform for IoT and cloud in the healthcare system. In: Fog computing: Breakthroughs in research and practice (pp. 365–378). IGI global (2018).

[7] Tewari and B. B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” *Future Generation Computer Systems*, vol. 108, p. 909, (2018).

[8] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, “Fog computing security challenges and future directions [energy and security],” *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 92–96, (2019).

[9] Farjana, N., Roy, S., Mahi, M.J.N., Whaiduzzaman, M.: An identity-based encryption scheme for data security in fog computing. In: Proceedings of International Joint Conference on computational intelligence (pp. 215–226). Springer, Singapore (2020).

[10] Whaiduzzaman, M.: An identity-based encryption scheme for data security in fog computing. In: Proceedings of International Joint Conference on computational intelligence (pp. 215–226). Springer, Singapore (2020)

[11] Zhou, C., Fu, A., Yu, S., Yang, W., Wang, H., Zhang, Y.: Privacy-preserving federated learning in fog computing. IEEE Internet Things J. **7**(11), 10782–10793 (2020).

[12] Manogaran, G., et al.: Machine learning assisted information management scheme in service concentrated IoT. IEEE Trans. Ind. Inf. **17**(4), 2871–2879 (2020).

[13] Hameed, A.R., ul-Islam, S., Ahmad, I., Munir, K.: Energy-and performance-aware load-balancing in vehicular fog computing. Sustain. Comput. **30**, 100454 (2021).

[14] Kaviyazhiny, C., Bala, P.S., Gowri, A.S.: Fog computing perspective: technical trends, security practices, and recommendations. Smart Cyber Ecosyst. Sustain. Dev. **21**, 323–351 (2021).

[15] Hameed, A.R., ul-Islam, S., Ahmad, I., Munir, K.: Energy-and performance-aware load-balancing in vehicular fog computing. Sustain. Comput. **30**, 100454 (2021).

[16] Mengqi, Z., Xi, W., Sathishkumar, V.E., Sivakumar, V.: Machine learning techniques based on security management in smart cities using robots. Work, (Preprint), 1–12 (2021).

[17] Alshudukhi, J.S.; Al-Mekhlafi, Z.G.; Mohammed, B.A. A Lightweight Authentication with Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography. *IEEE Access* **2021**, *9*, 15633–15642.

[18] Supriya, Gurpreet Singh, “A study of Encryption Algorithms (RSA, DES, 3DES, and AES) for Information Security”, International Journal of Computer Applications (0975-8887), vol. 67, no.19, April 2013.

[19] Soheila Omer AL Farooq Mohammed Koko, Dr. Amin Babiker A/Nabi Mustafa, “Comparison of Various Encryption Algorithms and Techniques for improving secured data communication”, IOSR-Journal of Computer Engineering, vol.17, issue 1, pp 62-69, January-February 2015.

[20] Shaza D. Rihan, Ahmed Khalid, Saife Eldin F.Osman, “A Performance Comparison of Encryption Algorithms AES and DES” International Journal of Engineering Research & Technology (IJERT), vol.4, issue 12, December 2015.

[21] Bhawna Dakhare, NileshN.Shinde, Swanand S.Salvi, Ankit H.Kadam, Pooja G.Wagh, “Performance Analysis of Data Encryption Algorithms using AES BLOWFISH and SNAP” International Journal of Engineering Science and Computing vol. 8, issue no.3, 2018.

[22] G, M. ., Deshmukh, P. ., N. L., U. K. ., Macedo, V. D. J. ., K B, V. ., N, A. P. ., & Tiwari, A. K. . (2023). Resource Allocation Energy Efficient Algorithm for H-CRAN in 5G. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3s), 118–126. https://doi.org/10.17762/ijritcc.v11i3s.6172

[23] Anthony Thompson, Anthony Walker, Luis Pérez , Luis Gonzalez, Andrés González. Machine Learning-based Recommender Systems for Educational Resources. Kuwait Journal of Machine Learning, 2(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/181