RSA and AES Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing

RIMA AKTER[1], MD. ASHIKUR RAHMAN KHAN[1, *], FARDOWSI RAHMAN[1], SULTANA JAHAN SOHELI[1], NUSRAT JAHAN SUHA[1]
[1]Department of Information and Communication Engineering
Noakhali Science and Technology University
Noakhali-3814
BANGLADESH

Abstract: - Cloud computing security has become the most crucial problem in its growth. Encryption has been developed as a solution and plays a vital role in the security of information systems in cloud computing. Many methods are required to secure the shared data. The advanced internet, networking firms, health information, and cloud applications have significantly increased our data every minute. The current work focuses on cryptography to protect sensitive data exchanged between personal users, companies, organizations, or in the cloud applications and others during data transfer across the network. Firstly, data sent from the sender to the network receiver must be encrypted using the cryptographic algorithm. Secondly, the recipient shows the original data using the decryption technique. In this paper, we have proposed a model to use a hybrid encryption and decryption process based on AES-128 and the RSA algorithm. Furthermore, we used the HMAC algorithm to ensure the integrity and authenticity of data. Our experiment work has been done to explain the time required and throughput for encryption and decryption of three encrypting algorithms, AES, RSA, and hybrid algorithms, based on different data sizes, and their efficiency is compared. The results of the experiments show that the hybrid algorithm is better in terms of security.

Key-Words: - Cloud Security, Rivest, Shamir, and Adleman (RSA), Advanced Encryption Standard (AES), Hash-Based Message Authentication Code (HMAC), Hybrid Algorithm, Encryption, Decryption**.**

Received: June 29, 2022. Revised: August 26, 2023. Accepted: September 23, 2023. Published: October 31, 2023.

1 Introduction

Today's cloud computing (CC) is a rapidly evolving technology that is in use all over the world. Additionally, a cloud computing environment enables the sharing of resources among servers, users, and persons, making files and data stored there publicly available. As a result, it can be used by various sectors, including those in the healthcare, finance, business, organization, social network, and educational sectors. The most significant issue with cloud computing's expansion is its security measures. Between the cloud computing platform and the user, there are a lot of data interactions, [1] describe a process used to meet security criteria, [2]. One technique to guarantee data confidentiality and access to the receiving party without risk of interference from outside parties is through encryption. Cryptography includes creating and studying algorithms that prevent a third party or the public from reading private messages [3].

Cryptographic algorithms come in two different varieties. The first one is public cryptography (PKC), or an asymmetric cipher, which employs two keys, one for sender and one for receiver use only. The second is a symmetric cipher, which encrypts and decrypts data using the same key for both the sender and the recipient. Data that has been encrypted remains private by hiding the user's confidentiality [4]. This paper designs and builds a hybrid encryption algorithm based on the AES (Advanced Encryption Standard) + RSA (Rivest, Shamir, and Adleman) encryption algorithm. To ensure that user data is transferred securely, it uses double encryption technology in combination with hash-based message authentication code (HMAC) technology. Multiple cipher types, typically based on differing strengths, are used in hybrid cryptography. The plan is to create a unique encryption key, which will then be encoded using the participant's public key.

2 Related Works and Significance of Cloud Security

This section discusses the fundamental basics of cloud computing technology and issues related to security, mainly privacy, in cloud computing services. Understanding the cloud computing concept and how this concept is implemented in different service delivery and deployment models helps to identify the security issues facing this new technology. The service delivery and deployment models of cloud computing services are described in sections 2.1 and 2.2. In sections 2.3 and 2.4, challenges and issues in cloud computing are generally investigated, and some specific examples are provided.

2.1 Cloud Service Models

Unquestionably, cloud computing offers a variety of hosted services over the internet. These hosted services can be broadly categorized into three primary service models [5], namely Infrastructure as a Service (IaaS), Platform as a Service (Platform as a Service), and Software as a Service (SaaS), which have been explored in Figure 1.

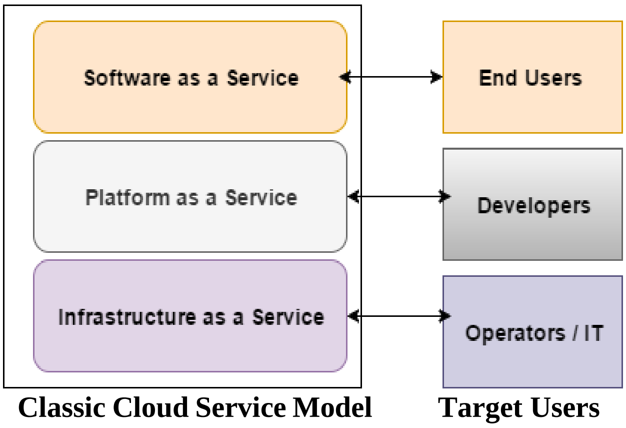


Fig. 1: Cloud service delivery models

The cloud service delivery models, as in Figure 1 [6], include:

- **Infrastructure-as-a-Service (IaaS)**: Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provides access to networking features, computers (virtual or on dedicated hardware), and data storage space.
- **Platform-as-a-Service (PaaS)**: Platforms-as-a-Service allows you to concentrate on deploying and administering your applications by removing the need for companies to manage the underlying infrastructure (often hardware and operating systems).
- **Software-as-a-Service (SaaS)**: With software as a service, the service provider gives you a finished product that is operated and managed on your behalf. Usually, end-user applications are meant when software as a service is mentioned.

2.2 Cloud Deployment Models

A paradigm for providing various services in an on-demand delivery manner is cloud computing. The four types of cloud computing deployment models—Public cloud, Private cloud, Community cloud, and Hybrid cloud—are categorized to coexist peacefully with other components [5] based on the cloud services and features already discussed.

- **Public cloud:** a platform where anyone can sign up and access the available infrastructure.
- **Private cloud:** a cloud platform is intended for a particular business.
- **Community Cloud:** the infrastructure of the cloud is shared by several organizations and supports a specific community with shared concerns.
- **Hybrid cloud:** a cloud infrastructure composed of two or more clouds, i.e., private, community, or public.

2.3 Challenges to Cloud Security

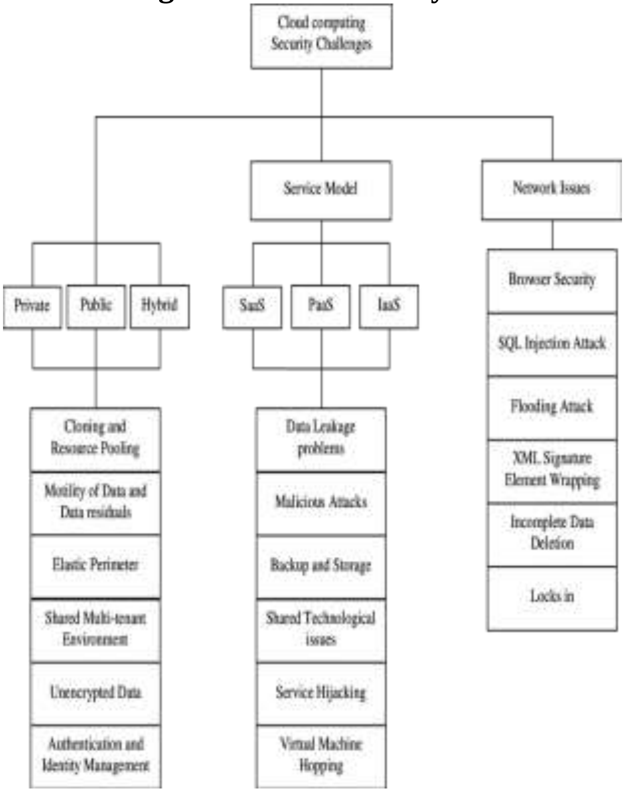


Fig. 2: Cloud Computing Security Challenges.

Security has been one of the most challenging problems for IT leaders, especially when using clouds. Numerous security concerns exist, keeping businesses from utilizing the cloud's benefits. Security is described as the main challenge for cloud users in several studies [7]. This section contains a taxonomy of cloud computing security terms. Figure 2 is a schematic diagram of the cloud computing hierarchy highlighting the security vulnerabilities that might arise with deployment, service models, and network-related problems [8].

2.4 Cloud Computing Security

Cloud Computing refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Data misuse is possible when multiple organizations share resources. Therefore, protecting data repositories and the data involved in processing, transport, or storage is essential to reduce risk. The most significant difficulties in cloud computing are related to data protection. It's crucial to offer authentication, authorization, and access control for cloud-stored data to improve cloud computing security.

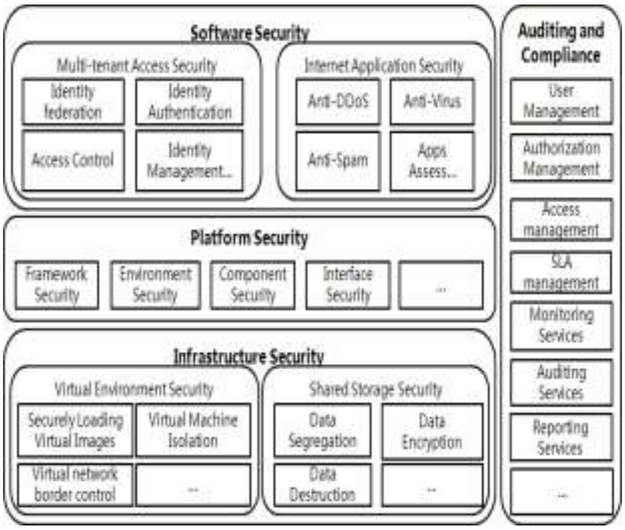


Fig. 3: Cloud Computing Security Architecture [13]

There are two primary facets to data security:

Authentication: The security of the cloud is significantly influenced by authentication. Authentication is the process used to assess user identities with confidence. The degree of authentication assurance must be correct and appropriate given the sensitivity of the application, the information assets accessible, and the risk present [9].

Confidentiality: To keep private or confidential data in the cloud, users must ensure data confidentiality. Data confidentiality is typically protected by authentication and access control techniques [10, 11]. Access to sensitive and protected data is made possible by confidentiality in the context of computer systems [12].

2.5 Related Works of Cloud Security

Various researchers discuss cloud computing security challenges and issues. The Cloud Computing Use Cases group [14] discusses the different use case scenarios and related requirements that may exist in the cloud computing model. They consider use cases from different perspectives, including customers, developers, and security engineers. ENISA [15] investigated the different security risks related to adopting cloud computing along with the affected assets, the risks, likelihood, impacts, and vulnerabilities in cloud computing that may lead to such risks. Similar efforts are discussed in "Top Threats to Cloud Computing" by CSA [16]. A work discusses the tools and materials for cloud computing security and cryptographic algorithms [17-18] used in cloud computing security.

A hybrid cryptographic algorithm is developed to provide data security [19]. This hybrid algorithm combines famous symmetric (AES-128) and asymmetric (RSA-1024) encryption algorithms implemented in eye-OS. Some authors reviewed the security challenges encountered in cloud services with various stats and mentioned some critical issues in cloud security [20]. Their proposed model provides the solution to these key issues using AES encryption. They have compared symmetric encryption algorithms like 3DES, DES, and RC2 with parameters like encryption speed. Another research developed an enhanced hybrid data security algorithm using various algorithms like AES, ECDSA, and SHA256 for providing security to data stored inside [21]. These algorithms are arranged appropriately for securely communicating, uploading, and downloading data on the cloud. Some researchers developed a hybrid cryptography algorithm using four symmetric encryption algorithms (AES, RC6, BLOWFISH, and BRA) for secure file storage in a cloud environment [22]. A paper developed a hybrid encryption algorithm using three symmetric encryption algorithms and digital technique [23] for secure cloud file storage [24]. Based on the statistics [25], various hybrid cryptographic models suggest to using AES and FHE to overcome security issues like data confidentiality, privacy, and integrity [26]. Another research work implemented a hybrid security model for securing medical patient's data stored in the cloud [27]. The authors have modified the AES algorithm and named it P-AES, which is used with RSA to provide privacy and security to medical data stored in the cloud [28].

3 Materials and Methods

In this paper, we have proposed a model to use a hybrid encryption and decryption process based on AES-128 and the RSA algorithm. Furthermore, we used the HMAC algorithm to ensure the integrity and authenticity of data. The research methodology is described in distinct sections:

3.1 Modules Description

The three types of modules are described below.

User Module: The user module views two options: Encryption and Decryption. The options are selected depending on the user. If the user wants to encrypt the file, select the encryption option. Otherwise, select the decryption option.

Encryption Module: This module is used to encrypt the document easily. First, select the encryption option and then the encrypting file. After clicking the encryption button, the file is to be encrypted.

Decryption Module: This module is used to decrypt the document easily. First, select the decryption option and then the encrypted file. Finally, click the decryption button. The file is to be decrypted.

3.2 AES Algorithm

A popular symmetric block cipher algorithm is AES. According to the AES standard, the algorithm can only take blocks of 128 bits. The name of the standard is AES-128, AES-192, or AES-256, depending on the version being utilized (Douglas, 2010). More extensive data must be divided into blocks to be encrypted because AES only supports 128-bit blocks. Four steps make up the AES algorithm's round, which is iterated ten times for keys with 128 bits, twelve times for keys with 192 bits, and fourteen times for keys with 256 bits. A list of key schedule words is then created using the expanded key. The four stages are as follows: Substitute bytes, Shift rows, Mix columns, and Add round key. Its algorithm proceeds as follows:

- Given a plaintext x, initialize State to be x and perform an operation ADD ROUND KEY, in which using the x-or operation, perform Add Round Key with State.
- For each of the first N^{r-1} rounds, perform a substitution operation called SubBytes on State using an S-box;
- Perform a permutation ShiftRow on State; operate MixColumns on State; and perform Add Round Key.
- Perform SubBytes, perform ShiftRows, and perform Add Round Key.
- Define the cipher text y to be State.

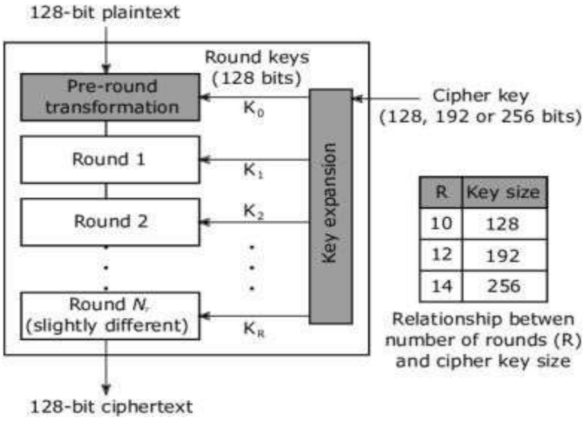


Fig. 4: AES algorithm grouping and encryption diagram.

3.3 RSA Algorithm

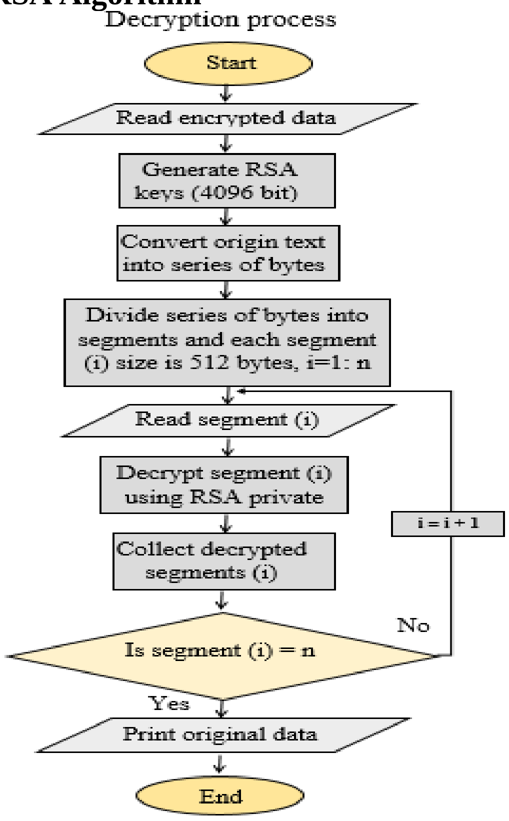


Fig. 5: RSA decryption algorithm flowchart

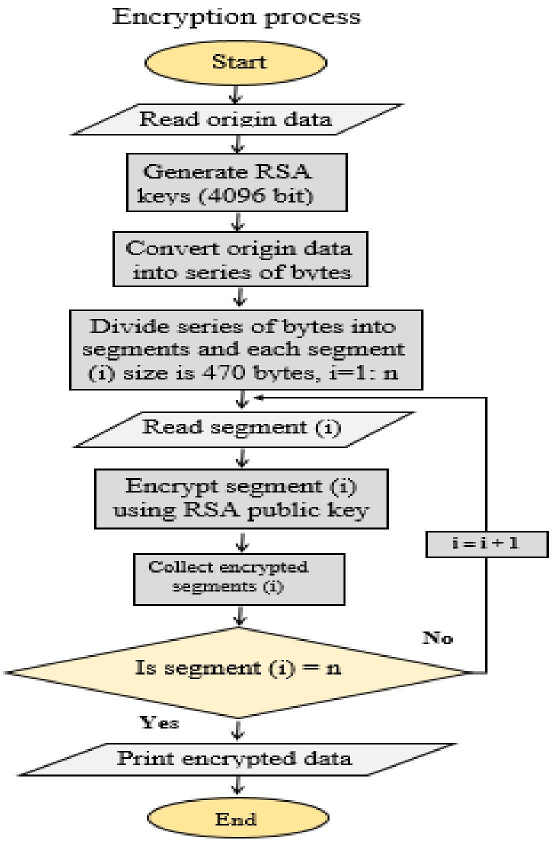

Encryption process
Start
Read origin data
Generate RSA keys (4096 bit)
Convert origin data into series of bytes
Divide series of bytes into segments and each segment (i) size is 470 bytes, i=1: n
Read segment (i)
Encrypt segment (i) using RSA public key
i = i + 1
Collect encrypted segments (i)
No
Is segment (i) = n
Yes
Print encrypted data
End

Fig. 6: RSA encryption algorithm flowchart.

The RSA algorithm consists of three phases: key generation, encryption, and decryption. Figures 5 and 6 give the encryption and description process of the RSA algorithm.

Key Generation

- Select random and secret two large primes p, q and check that p!=q.
- Compute modulus n = pq
- Compute phi, ϕ (n) = (p – 1) (q – 1)
- Select random public exponent: e such as 1 < e < n and gcd (e, ϕ) = 1
- Compute d such as e. d ≡ 1 mod ϕ(n) and 1 < d < ϕ (n)
- Public key: (n, e)
- Private key: (n, d)

Encryption Algorithm

- Obtain the recipient's public key (n, e)
- Represents the plaintext message as a positive integer m
- Compute the cipher text c = me mod n

Decryption Algorithm

- Uses his private key (n, d) to compute integer m=cd mod n
- Extract the plaintext from the integer representative m.

3.4 Hash-Based Message Authentication Code (HMAC)

Two parties want to communicate, but they want to ensure that the contents of their connection remain private. They also distrust the internet and need a way to verify that the packets they receive haven't been tampered with. HMAC is a valid solution. Hash-based message authentication code is a tool for calculating message authentication codes using a cryptographic hash function coupled with a secret key "HMAC" keys consisting of two parts. These are:
Cryptographic keys: An encryption algorithm alters data; a recipient needs a specific code (or key) to make it more readable. HMAC relies on two sets of keys. One is public, and one is private.
Hash function: A hash algorithm alters or digests the message once more. HMAC uses generic cryptographic hash functions, such as SHA-1, MD5. When complete, the message is considered irreversible, and it's also resistant to hacking. Someone who intercepts this message won't even be able to guess at its length.

3.5 Procedure methodology

The fundamental tenet of our suggested architecture is that to transfer the secret key of AES securely, we first encrypt the plaintext using the AES method before encrypting the secret key using the RSA technique. Thus, we may utilize these two algorithms' essential benefits, such as RSA secret key management's ease and security and AES's high-speed encryption [29] [30]. To further confirm the integrity and validity of the message, we also executed the HMAC function using the secret key and the generated cipher text to attach the generated value to the end of the encrypted message before sending it to the cloud server [31]. This fusion of the strength of AES and RSA algorithms is known as a Hybrid Algorithm.

3.5.1 Hybrid Algorithm

A hybrid encryption approach uses two different types of encryption to protect data transfer: Text files are encrypted using the AES technique, and the AES key is encrypted using the asymmetric RSA algorithm to prevent third parties from confirming the transmission between clients or clients and servers and to make it more difficult for attackers to access. The algorithm has three steps to it. They are Key generation, Encryption, and Decryption.

Hybrid Algorithm Encryption Principle: The hybrid encryption algorithm employs two-layer AES and RSA encryption, and the encryption process goes through a series of adjustments and steps. The actions involved in the two methods' file encryption schemes are detailed below in the order of encryption. The AES algorithm clusters the processing units, and the ordered 128-bit data is assigned to a four-by-four state matrix. All transformations in the algorithm are finished and centered on the state matrix. Four straightforward arithmetic operations—Sub Bytes, Shift Rows, Mix Columns, and Add Round Key are used in the procedure.

Hybrid Algorithm Decryption Principle: In the hybrid algorithm, the private key of the RSA algorithm is used to decode the cipher text encrypted by the public RSA key in the first layer, and then the AES key is used to decrypt the cipher text and get the plaintext. As RSA decryption is used, the encrypted cipher text c is decrypted and transformed, and the plain text m is obtained by the following calculation [32].

$$m = cd \bmod n \tag{1}$$

Here, d is calculated by the key generation algorithm, and n is the product of the large prime numbers p and q

In the decryption process of the AES algorithm, Sub Bytes, Shift Rows, and Mix-Columns are the inverse operations of the encryption process. Still, in Add Round Key, the inverse operation is the same as the forward transformation because the X-OR operation is its own inverse.

3.6 Details of Model in Encryption Process

The details of the model encryption process can be divided into three parts.

Ensuring the Confidentiality: Figure 7 shows P as our plaintext representation. Assuming that the plaintext will be encrypted using the AES-128 technique, the EA stands for the AES encryption algorithm, and the K for the AES secret key. The attacker cannot access the plaintext without knowing the secret key of the encryption technique, as shown in Figure 3.4, where CP is the cipher text of the original plaintext P [29].

Transfer the Secret Key: Sending the secret key via the internet will make it vulnerable to cracking. Therefore, we advise employing the RSA technique to encrypt the secret key in our suggested architecture.

Ensuring Integrity and Message Authentication: We stated in Section B earlier that we will provide the CK and CP via the Internet channel to clarify the secrecy. Additionally, as we want to guarantee the authenticity and integrity of the message, we propose using the HMAC technique to generate an M1 value, attach it to the end of the cipher text CP, and send the entire message to the cloud server. The SHA-256 algorithm is used by the embedded hash function [33].

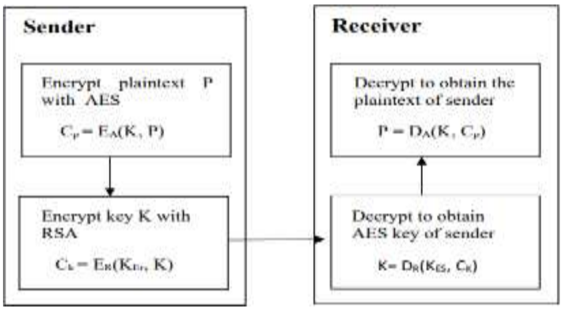


Fig. 7: Encryption and decryption process of the proposed model

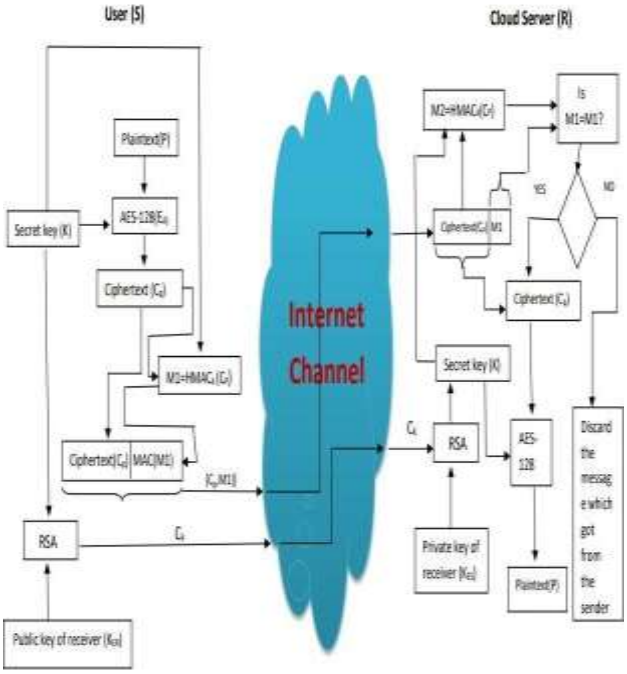


Fig. 8: Flowchart of the proposed model.

3.7 Details of Model in Decryption Process

When the cloud server receives the message, it will first use its own RSA private key to gain the AES algorithm secret key K. Then it will retrieve the new value M2 of HMAC using the secret key and cipher text CP to verify the authenticity and integrity of the message. If they are equal, the plaintext is integrated verified, and must be processed by the cloud server. Figure 7 explains the processes for encrypting plaintext and the secret key and decrypting the secret key and cipher text.

3.8 Flowchart of Proposed Framework

Figure 8 outlines the entire encryption and decryption procedure in our suggested paradigm.

4 Results

This section provides the implementation of Rivest, Shamir, and Adleman (RSA), Advanced Encryption Standard (AES), and Hybrid encryption technique algorithm according to the proposed structure, and simulation results are discussed in detail. All the algorithms have been programmed with Wolfram language in the Mathematica platform. The experiment was done using an HP laptop, which has Windows 10 as the operating system. The proposed model is implemented on the different sizes of data ranging from 64 bytes to 288 bytes. We calculated the encryption and decryption time throughput for all three algorithms and compared theresults.

4.1 RSA Encryption and Decryption Time

Table 1 and Figure 9 below show the required time for the encryption and decryption process for the RSA Algorithm.

Table 1. RSA encryption and decryption time

Data Size (Byte)	Time required for encryption (s)	Time required for decryption (s)
64	1.074	1.08057
96	1.07541	1.07648
144	1.07015	1.08404
176	1.06584	1.08666
208	1.06945	1.09343
240	1.08034	1.09673
288	1.08249	1.08561

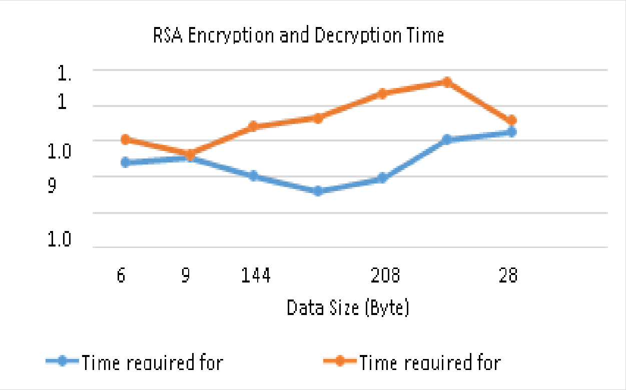


Fig. 9: Encryption and decryption time consumption of RSA

4.2 AES Encryption and Decryption Time

The required encryption and decryption time for AES Algorithm is shown in Table 2 and Figure 10.

Table 2. AES encryption and decryption time

Data Size (Byte)	Time required for encryption (s)	Time required for decryption (s)
64	0.00025241	0.00032401
96	0.00023034	0.00033865
144	0.00020102	0.00031522
176	0.00024265	0.00030787
208	0.00019955	0.00054922
240	0.00025144	0.00027889
288	0.00021165	0.00029941

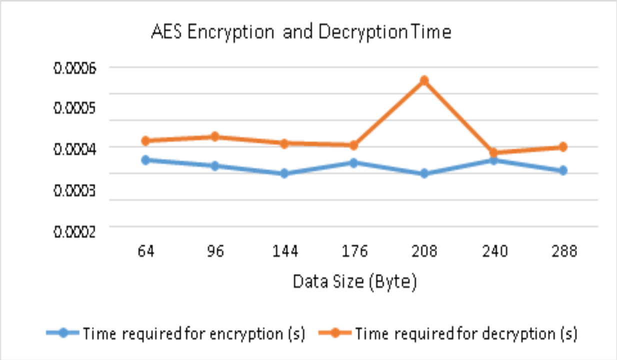


Fig. 10: Encryption and decryption time consumption of AES

4.3 Encryption and Decryption Time for Proposed Hybrid Algorithm

The required time for the encryption and decryption process for the proposed Hybrid Algorithm is shown in Table 3 and Figure 11 below.

Table 3. Proposed Hybrid algorithm's encryption and decryption time

Data Size (Byte)	Time required for encryption (s)	Time required for decryption (s)
64	1.04707	0.0540557
96	1.04708	0.0540354
144	1.0471	0.0539762
176	1.04707	0.0539808
208	1.04709	0.0539886
240	1.04707	0.0539728
288	1.04706	0.0539677

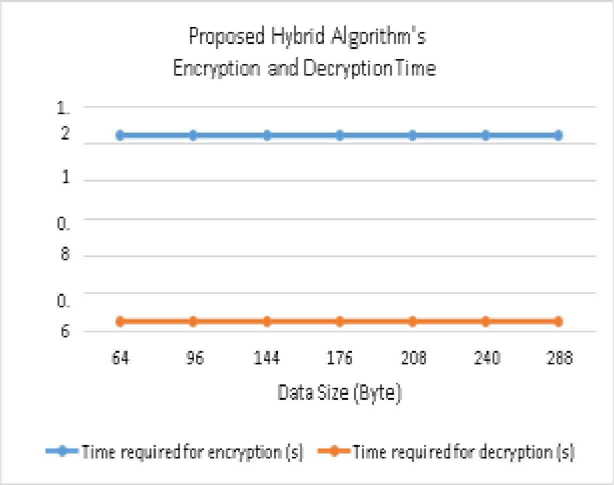


Fig. 11: Encryption and decryption time consumption of the proposed Hybrid algorithm

Table 4. The throughput value of the three algorithms

RSA Throughput	AES Throughput	Hybrid Throughput
562.92	2126.53	1104.38

Table 5. Time is taken for each algorithm in the second

Data size (Byte)	RSA encryption	RSA decryption	AES encryption	AES decryption	Hybrid encryption	Hybrid decryption
64	1.074	1.08057	0.0002524	0.0003240	1.04707	0.054055
96	1.0754	1.07648	0.0002303	0.0003386	1.04708	0.054035
144	1.0701	1.08404	0.0002010	0.0003152	1.0471	0.053976
176	1.0658	1.08666	0.0002426	0.0003078	1.04707	0.053980
208	1.0694	1.09343	0.0001995	0.0005492	1.04709	0.053988
240	1.0803	1.09673	0.0002514	0.0002788	1.04707	0.053972
288	1.0824	1.08561	0.0002116	0.00029941	1.04706	0.0539677

The proposed hybrid scheme allows the user to encrypt data with hybrid algorithms that use two robust encryption algorithms without taking more time for both encryption and decryption for various message lengths.

Table 6. The total time for each algorithm in the second

Data Size (Byte)	RSA Total Time	AES Total Time	Hybrid Total Time
64	2.15457	0.00057642	1.1011257
96	2.15189	0.00056899	1.1011154
144	2.15419	0.00051624	1.1010762
176	2.1525	0.00055051	1.1010508
208	2.16288	0.00074877	1.1010786
240	2.17707	0.00053033	1.1010428
288	2.1681	0.00051106	1.1010277

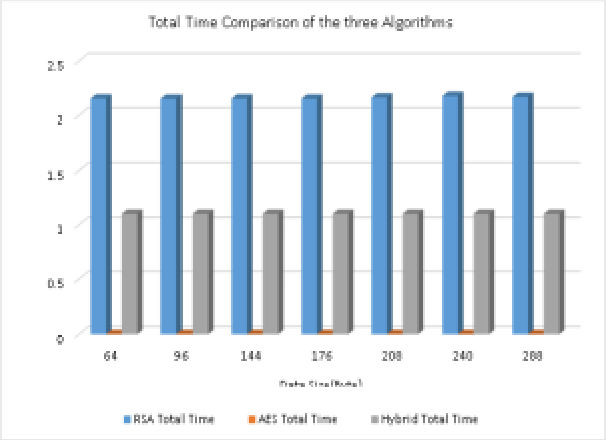


Fig. 12: Comparative analysis of the three algorithms' total time encryption and decryption.

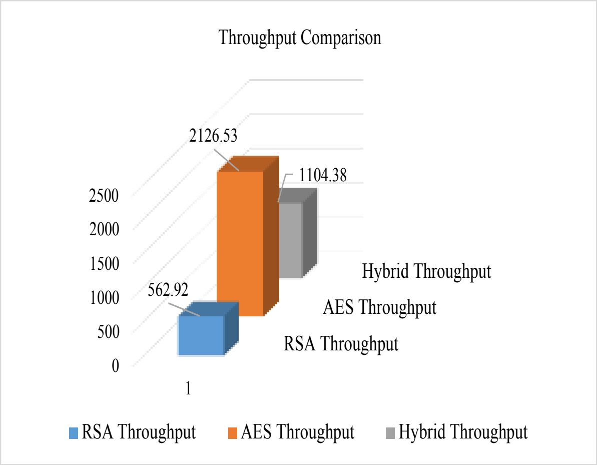
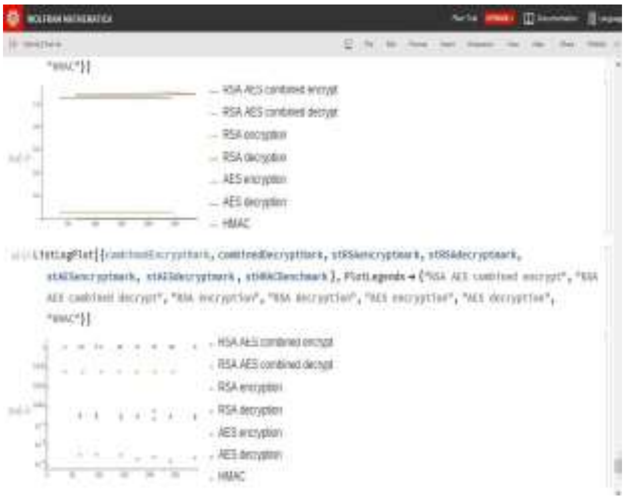


Fig. 13: Throughput value of the three algorithms

Throughput: Throughput is the amount of data that passes via a network system. It is a result of dividing all data sent in bytes by the average time required to send all data in seconds. The throughput value in (B/Sec) for each algorithm is shown in Table 4.

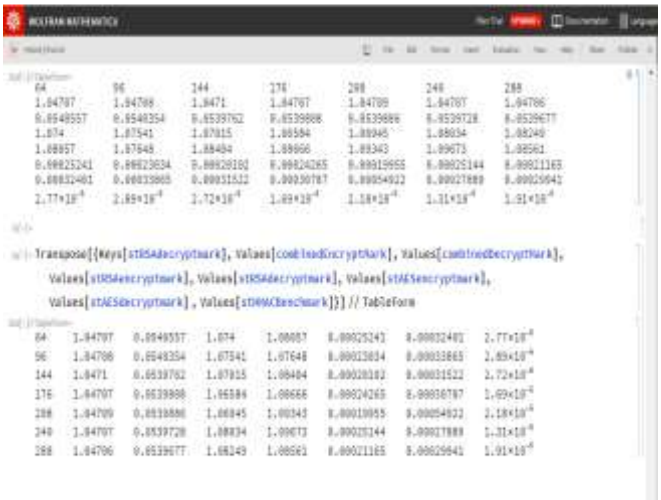
Comparative Analysis of the Results



```
"HMAC"}]
```

```
ListLogPlot[{combinedEncryptMark, combinedDecryptMark, stRSAencryptmark, stRSAdecryptmark,
  stAESencryptmark, stAESdecryptmark, stHMACBenchmark}, PlotLegends → {"RSA AES combined encrypt", "RSA
  AES combined decrypt", "RSA encryption", "RSA decryption", "AES encryption", "AES decryption",
  "HMAC"}]
```

Fig. 14: The encryption-decryption time of the three algorithms in Wolfram Mathematica



```
64          96          144         176         208         240         288
1.84787     1.84788     1.8471      1.84787     1.84789     1.84787     1.84786
0.8548557   0.8548354   0.8539762   0.8539808   0.8539886   0.8539728   0.8539677
1.874       1.87541     1.87815     1.86584     1.88945     1.88034     1.88249
1.88857     1.87648     1.88484     1.88666     1.89343     1.89673     1.88561
0.00025241  0.00023834  0.00028182  0.00024265  0.00019955  0.00025144  0.00021165
0.00032481  0.00033865  0.00031522  0.00030787  0.00054922  0.00027889  0.00029641
2.77×10^-4  2.89×10^-4  2.72×10^-4  1.89×10^-4  1.18×10^-4  1.31×10^-4  1.91×10^-4
```

```
Transpose[{Keys[stRSAdecryptmark], Values[combinedEncryptMark], Values[combinedDecryptMark],
  Values[stRSAencryptmark], Values[stRSAdecryptmark], Values[stAESencryptmark],
  Values[stAESdecryptmark], Values[stHMACBenchmark]}] // TableForm
```

```
64   1.84787  0.8548557  1.874    1.88857  0.00025241  0.00032481  2.77×10^-4
96   1.84788  0.8548354  1.87541  1.87648  0.00023834  0.00033865  2.89×10^-4
144  1.8471   0.8539762  1.87815  1.88484  0.00028182  0.00031522  2.72×10^-4
176  1.84787  0.8539808  1.86584  1.88666  0.00024265  0.00030787  1.89×10^-4
208  1.84789  0.8539886  1.88945  1.89343  0.00019955  0.00054922  1.18×10^-4
240  1.84787  0.8539728  1.88034  1.89673  0.00025144  0.00027889  1.31×10^-4
288  1.84786  0.8539677  1.88249  1.88561  0.00021165  0.00029641  1.91×10^-4
```

Fig. 15: The encryption-decryption time value of the three algorithms in a tabular form in Wolfram Mathematica

This part shows a comparative analysis based on metrics such as encryption time, decryption time, total time, throughput, and data size to measure the performances of the selected algorithms. The encryption-decryption schedule of the three is shown in Table 5 with different data sizes.

Three algorithms are used in this experiment to encrypt and decrypt the same data size. The encryption-decryption schedule of the three is shown in Table 5 with different data sizes. Table 6 shows the total processing time in seconds. According to the results shown in Table 6, it is clear that the hybrid algorithm is better than the other algorithms (AES and RSA) after testing the three algorithms and calculating the time required to complete the processing of several data of different sizes. Results show that the best algorithm is the hybrid algorithm, which provides the reliability and the highest security for the data sent; when the RSA, AES, and hybrid algorithms are compared, the encryption and decryption time differences are evaluated in Figure 12. Throughput analysis is shown in Figure 13. Figures 14 and 15 present the three algorithms' encryption and decryption time values in the Wolfram Mathematica platform. The hybrid encryption algorithm provides the highest level of data security than other algorithms, and its speed is much faster than RSA and slightly slower than AES algorithms.

5 Discussions

According to the experiments applied in this paper, the decryption time of the RSA algorithm and the AES algorithm increases with increased data size. The RSA algorithm has increased dramatically, almost linear development, and the AES algorithm has increased marginally. The decryption time of the hybrid encryption algorithm is stable close to a specific value, close to the AES algorithm. Compared to the RSA algorithm, the improvement in decryption performance has a noticeable impact on large files. Through contrasting encryption and decryption above, the hybrid algorithm significantly increases encryption performance relative to the RSA algorithm while encrypting and decrypting broad data. Owing to the use of dual-layer encryption, the decryption complexity is intensified as the data is decrypted, and the hybrid algorithm optimizes the dilemma that the AES algorithm key is leaked and the authentication is ineffective. The functionalities of the algorithm determine the level of data security. The table below describes the nature of the algorithm, security level, key management, and time parameters for AES, RSA, and Hybrid. The table gives the summary of functionalities enhanced regarding values assigned to hybrid.

Table 7. Summary of the functionalities of the algorithms AES, RSA, and Hybrid

FACTORS	**AES**	**RSA**	**HYBRID**
NATURE			
Type of algorithm	Symmetric	Asymmetric	Hybrid
Data size	Big	Small	Big

Block size	128,192, 256 bits	Minimum 512 bits	128 bits
Power consumption	Low	High	Low
Rounds	10,12,14	1	AES-14, RSA-1
Memory space	Less	More	More
TIME			
Encryption/ Decryption	Fast	Slow	Fast
Speed of computation	Fast	Slow	Fast
Software Implementation	Fast	Slow	Fast
Hardware Implementation	Fast	Slow	Fast
SECURITY			
Confidentiality	Moderate	High	High
Integrity	None	High	High
Authentication	None	Moderate	High
Non-repudiation	None	None	High
Digital signatures	None	Possible	Available
Hash function	None	Possible	Available
KEY			
Key generation	Yes	Yes	Yes
Key storage	No	Yes	Yes
Multiple keys	No	Yes	Yes
Secret key	Yes	Yes	Yes
Public key	No	Yes	Yes
Shared key	Yes	No	No
Distribution public key	No	Yes	Yes
Distribution of secret key	Yes	No	No
Pair keys	No	Yes	Yes
Inverse keys	Yes	No	Yes

This hybrid technique combines the features of both asymmetric cryptography and symmetric cryptography—a proposed schema based on two levels of data encryption and key encryption. The technique provides a higher level of security and efficiency level. It is better than either of the techniques used separately.

The AES-128 algorithm achieves data security in this hybrid to confirm confidentiality. Data integrity is a process that is difficult to meet with only symmetric keys. The combination of RSA guaranteed this security goal to encrypt the AES secret key. Authentication of the sender and non-repudiation of data is ensured using the HMAC function. Furthermore, they must be archived under time-based management to be available for retrieving. The combination of different cryptography algorithms provide maximized efficiency, correcting or compensating. This approach offers a solution for various weaknesses that must be faced in a security cryptosystem, including. The results showed that the hybrid encryption is 67.47% faster than the RSA algorithm and 32.39% slower than the AES algorithm. That's why the hybrid encryption algorithm can be used in software applications, system design, and other fields required to exchange data security, which can effectively protect the data, in addition to the performance and fast execution time.

6 Conclusion

Cloud computing is the latest trend in IT. But security is the biggest challenge in this area. So, researchers mainly concentrate on this area. Encryption is the best security method; now, different kinds of encryption techniques apply in cloud computing environments, and hacking can be prevented. In this paper, we have suggested a mechanism of hybrid encryption and decryption based on the AES-128-bit algorithm to encrypt the original plaintext and then encrypt the secret key of AES by the RSA algorithm. Furthermore, we used the value produced by the HMAC algorithm and attached to it the end of the encrypted plaintext to check the integrity and authenticity of the message. The experiment results show the time required for encryption and decryption of different data sizes started from 64 bytes up to 288 bytes. Moreover, the throughput value has been measured for the three algorithms. According to the experiments applied in this paper, the hybrid encryption algorithm can be used in software applications, system design, and other fields required to exchange data security, which can effectively protect the data, in addition to the performance and fast execution time.

In future studies, to provide complete cloud computing security from several aspects, we want to add more parameters to this secure suite's privacy framework and validate the marks on the keys and records that are unquestionably shared.

Acknowledgement:

We acknowledge the persons working in the Information and Communication Engineering (ICE) Department laboratory at Noakhali Science and Technology University, who have always helped us complete this research work successfully. Also, we are very thankful to the Research Cell, Noakhali Science and Technology University, for financial support.

References:

[1] Abdelrazek, Mohamed, John Grundy, and I. Mueller. "An analysis of the cloud computing security problem," 2010.

[2] Oleiwi, Zahraa Ch, Wasan A. Alawsi, Wisam Ch Alisawi, Ali S. Alfoudi, and Liwa H. Alfarhani. "Overview and Performance Analysis of Encryption Algorithms." In *Journal of Physics: conference series*, Vol. 1664, No. 1, p. 012051. IOP Publishing, 2020.

[3] Chinnasamy, P., Padmavathi, S., Swathy, R. and Rakesh, S. "*Efficient data security using hybrid cryptography on cloud computing*." Vol. 145, No. September, pp. 537– 547, Lect. Notes Networks Syst., 2021. doi: 10.1007/978-981-15-7345-3_46.

[4] Banasode, P. and Padmannavar, S. "*Protecting and Securing Sensitive Data in a Big Data Using Encryption.*" Vol. 0, No. 0, p. 163991, EAI Endorsed Trans. Smart Cities, 2018.

[5] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud-def-v15.pdf, Accessed April 2010.

[6] Kumar, Saurabh, and Rajkumar Buyya. "Green cloud computing and environmental sustainability." *Harnessing green IT: principles and practices* (2012): 315-339.

[7] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma, "*Towards Analyzing Data Security Risks in Cloud Computing Environments*," Springer-Verlag Berlin Heidelberg 2010, pp. 255- 265.

[8] Jinan, Umme Afifa, and Ashikur Rahman Khan Given. "Fog assisted and IoT based real-time health monitoring system implementation." *International Journal of Applied Mathematics, Computational Science and Systems Engineering* 2, 2020.

[9] Majda Omer Elbasheer and Dr.Taring Mohammed, "*Signing and verifying certificates by NTRU and RSA algorithm*" International Conference on Cloud Computing (ICCC), pp. 1-4. IEEE.2015.

[10] PreetiGarg and Dr.Vineet Sharma, "*An efficient and secure data storage in mobile cloud computing through RSA and hash function*" International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 334-339. IEEE. 2014.

[11] Vishwanath S Mahalle and Aniket K Shahade, "*Enhancing the data security in the cloud by implementing hybrid(RSA & AES) encryption algorithm*", International Conference on Power, Automation and Communication (INPAC), pp. 146-149. IEEE. 2014.

[12] Mr. Prashant Rewagad and Ms. Yogita Pawar, "*Use of digital signature with Diffie Hellman key exchange and AES encryption algorithm to enhance security in cloud computing*," International Conference on Communication Systems and Network Technologies(CSNT), pp. 437-439. IEEE.2013.

[13] D. Chen and H. Zhao, "*Data security and privacy protection issues in cloud computing*," Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 1, no. 973, pp. 647- 651, 2012.

[14] Cases, Cloud Computing Use. "A white paper produced by the Cloud Computing Use Case Discussion Group." 2010.

[15] ENISA, "*Cloud computing: benefits, risks, and recommendations for information security*," 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk- assessment, Accessed July 2010.

[16] Cloud Security Alliance (CSA), (2010). Available: http://www.cloudsecurityalliance.org.

[17] B. K. Dewangan, A. Agarwal, & A. Pasricha, "*Credential and security issues of cloud service models*," 2nd International Conference on Next Generation Computing Technologies (NGCT), (pp. 888-892), IEEE 2016.

[18] Khan, Md Ashikur Rahman, and M. M. Rahman. "Mathematical Expression for Machining Performance." *International Journal of Mathematical and Computational Sciences* 12, no. 11 (2018): 208-213.

[19] V. S. Mahalle and A. K. Shahade, "*Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm*," 2014 Int. Conf. Power, Autom. Commun. INPAC 2014, no. I, pp. 146–149, 2014, doi: 10.1109/INPAC.2014.6981152.

[20] R. Kiruthika, S. Keerthana, and R. Jeena, "*Enhancing Cloud Computing Security using AES Algorithm*," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 3, pp. 630–635, Mar. 2015.

[21] V. K. Soman and V. Natarajan, "*An enhanced hybrid data security algorithm for cloud*,"Int.

125 Conf. Networks Adv. Comput. Technol. NetACT 2017, pp. 416–419, Jul. 2017, doi: 10.1109/NETACT.2017.8076807.

[22] B. Bindu, L. Kamboj, and P. Luthra, "*Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm*," Int. J. Adv. Res. Comput. Sci., vol. 9, no. 2, pp. 773–776, 2018, doi: 10.26483/ijarcs.v9i2.5916.

[23] Hasan, M.A., Khan, M.A.R., Ahammad, I., Uddin, M. and Zaman, T.,"Digital Technique for Allowance Estimation," International Journal of Recent Technology and Engineering, vol-08, 2277-3878, 2020.

[24] M. Batra, P. Dixit, L. Rawat, and R. Khalkar, "*Secure File Storage In Cloud Computing Using Hybrid Encryption Algorithm*," Int. J. Comput. Eng. Appl., vol. XII, no. VI, pp. 30–36,Jun. 2018.

[25] Ahammad, Ishtiaq, Md Ashikur Rahman Khan, and Zayed Us Salehin. "QoS performance enhancement policy through combining fog and SDN." *Simulation Modelling Practice and Theory* 109: 102292, 2021.

[26] L. Kumar and N. Badal, "*A Review on Hybrid Encryption in Cloud Computing*," Proc. - 2019 4th Int. Conf. Internet Things Smart Innov. Usages, IoT-SIU 2019, pp. 1–6, 2019, doi: 10.1109/IoT-SIU.2019.8777503.

[27] F. Zhang, Y. Chen, W. Meng, and Q. Wu, "*Hybrid Encryption Algorithms for Medical Data Storage Security in Cloud Database*," Int. J. Database Manag. Syst., vol. 11, no. 01, pp. 57–73, 2019, doi: 10.5121/ijdms.2019.11104.

[28] Ahammad, Ishtiaq, Ashikur Rahman Khan, and Zayed Us Salehin. "A review on cloud, fog, roof, and dew computing: IoT perspective." *International Journal of Cloud Applications and Computing (IJCAC)* 11.4, 14-41, 2021.

[29] Rege, Komal, et al. "*Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA*," International Journal of Computer Applications 71.22, 2013.

[30] Chandra, Sourabh, et al. "*A comparative survey of symmetric and asymmetric key cryptography*," Electronics, Communication and Computational Engineering (ICECCE), 2014 International Conference. IEEE, 2014.

[31] Crocker, Paul, and Pedro Querido. "*Two Factor Encryption in Cloud Storage Providers Using Hardware Tokens*," 2015 IEEE Globecom Workshops (GC Wkshps). IEEE, 2015.

[32] Wan, Z.: "*Public key encryption scheme based on QI hyperchaos and its FPGA implementation*," Tianjin Polytechnic University, 2018.

[33] Xue-Zhou, Chang. "Network data encryption strategy for cloud computing." In *2015 Seventh International Conference on Measuring Technology and Mechatronics Automation*, pp. 693-697. IEEE, 2015.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Rima Akter has contributed to the work simulation, optimization, and paper writing.

Md. Ashikur Rahman Khan has given the idea and supervised this research work. Moreover, he has contributed to the model development, accomplishing paper revision and paper submission.

Fardowsi Rahman has played a significant role in writing the paper, revising it, and preparing it for the journal article.

Sultana Jahan Soheli and Nusrat Jahan Suha have played an efficient role in the paper's revision and submission.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

This work is fully funded by Research Cell, Noakhali Science and Technology University.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.