Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/82

Enhancing Network Security with A Hybrid Cryptography Method

Durgaprasad Gangodkar[1], Vrince Vimal[2]

[1]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002
[2]Department of Computer Science & Engineering,Graphic Era Deemed to be University, Dehradun, Uttarakhand India, 248002

ABSTRACT

Network and data security is of paramount importance to ISPs and other service providers. In order to ensure the safety of the information being transmitted, cryptographic methods are used throughout the exchange of this information. However, the standard cryptographic methods are well-known to both attackers and defenders, and the answer to these problems is public knowledge. This calls for a fresh approach to cryptography that can boost the safety and complexity of data cypher. In this work, we propose and report on the implementation of a hybrid cryptographic technique for bolstering data security through network transmission. The proposed cryptographic method, which makes use of RSA, DES, and SHA1, is said to be a very secure method of generating cyphers. A JAVA-based implementation of the suggested method is provided, and its performance in terms of space and time complexity is estimated and compared to that of conventional RSA cryptography. While comparing the performance of many cypher texts, the proposed cryptographic method discovered the most effective and superior one.

Keywords: Climate, Climate Change, Transportation, Precipitation, Green House Gases

INTRODUCTION

The process of making information unintelligible to humans by encoding it into a format they can't decode, or cipher text. The only people who can read the message in its plain form are the ones who have the secret key to understand it. Even though modern cryptography techniques are nearly unbreakable, encrypted messages can sometimes be broken using cryptanalysis, also termed code-breaking. Due to the proliferation of the Internet and other means of electronic communication, safeguarding information transmitted online is of paramount importance. Emails, credit card numbers, and sensitive business information can all be encrypted with the use of cryptography. Pretty Good Privacy is widely used as a cryptographic system for the Internet due to its efficiency and freedom of use. Symmetric-key systems employ a single key that is known to both the sender and the recipient, while public-key systems utilize two keys, one that is publicly known and one that is known only to the recipient of messages. Numerous apps exist now that allow for the transmission of private and sensitive data over an unsecure network. Data is typically sent from a user's trusted network to another user's trusted network. The network is secure within the source host's sphere of influence, but not between the source and target hosts. Consequently, cryptographic techniques are used by the vast majority of applications to ensure the safety and privacy of user information.

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/82

Herein this work is presented

Ultimately, we're looking for the best possible way to encrypt colour images securely. The optimization of the solution, which includes changing the cryptographic technique to use a hybrid approach and checking it for integrity, is motivated by a concern for efficiency in terms of minimizing the computational resources. Thus, the ideal cryptographic system would have to be faster and use less memory. There has to be a focus on using lightweight cryptographic standards and straightforward mathematical methods in order to create such an approach.

The proposed work seeks to create, by fusing together various cipher creation methods, a method that is both efficient and sophisticated. The following procedures are a part of the research design and are necessary for the achievement of the objective.

RELATED STUDY

As the volume of data transferred across networks continues to grow rapidly, it is more important than ever to implement robust security protocols. A thorough review of the current security mechanism is required to create a safe setting for data transmission across a network. Recent years have seen an increase in the usage of compression-based mechanisms in conjunction with RSA algorithm in current systems [1], with the goal of making these systems suitable for lightweight devices like mobile phones and personal digital assistants. This method ensures that your communications on the internet are safe [2]. This system first encrypts the message using the RSA algorithm, but only after it has been compressed using a special technique. To encrypt data, the RSA algorithm employs the asymmetric Public Key Encryption technique. Space and time complexity are barriers that prevent widespread adoption of asymmetric cryptography. An additional name for this setup is the Hybrid Compression Encryption system (HCE). A second approach sends sensitive health data via encrypted compressed files. In order to achieve its goals, it makes use of Sequitur and other compression technologies are used to minimise the transmitted data size. Confidentiality in transit is ensured via the McEliece public-key cryptosystem and compression [3]. The more data you feed into this system, the less efficient it becomes. The suggested system employs symmetric key cryptography, which makes it more efficient than asymmetric key cryptography, and a compression mechanism to minimize the size of the cypher text.

PROPOSED SYSTEM

With the help of the internet and other forms of modern communication, the field of information technology is rapidly expanding. Since the internet is such a robust medium for exchanging information, a great many programmers and their end users are taking advantage of its infrastructure. The network is protected in numerous ways, including the use of a firewall and other anti-virus measures. However, the data between the two private networks must pass through the public network, which has its own security flaws and is vulnerable to a variety of assaults. This is why cryptographic methods are used to safeguard information when it is being transmitted over open networks.

Meanwhile, hackers are familiar with and able to circumvent the various traditional cryptographic solutions used for data transmission via networks. As a result, research and development into novel methods for bolstering network data security are urgently needed. This paper presents a hybrid

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/82

technique that combines two distinct cryptography strategies. Security at both ends of a network can be guaranteed by modifying these methods to enhance key generation and integrity checks.

The proposed methods can protect information while transmission over insecure public networks. And it's determined whether or not data transmission was tampered with during various forms of external attacks. In situations where the two users are conversing across an entrusted network, the provided method provides an efficient and necessary measure for protecting sensitive data.

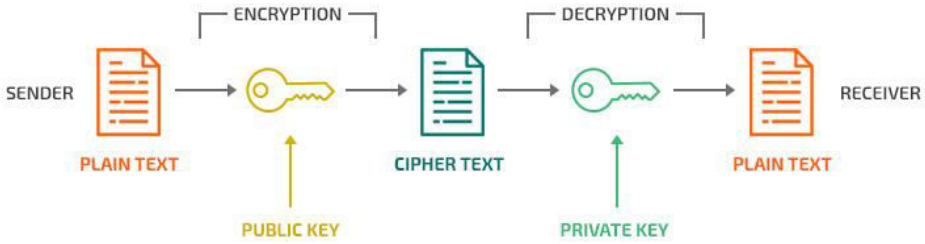

Fig 1: Encryption and Decryption of proposed system

Figures 1 depict the suggested data cryptography hybrid paradigm in action. When encrypting a file, the user must first encrypt the file using the hybrid cryptographic model, and these results in an input file being generated for the system. First, a 128-bit hash code is generated from the input file using the SHA1 hash generating technique.

The generated 128-bit hash key undergoes a process of bit discarding, during which the hash code is broken down into 16 chunks of 8-bit information. The initial bit of data in each block is extracted and stored separately. Thus, the 128-bit hash code is reduced to 112 bits, followed by 16 bits of separated code. A 128-bit key is generated by feeding 112 bits and 16 bits of data into a key generator, then splitting the 16-bit data into two 8-bit blocks and the 112-bit data into 14 blocks. The key is encrypted using the DES algorithm for added security, yielding the cipher 1 that serves as the encrypted key during decoding. By contrast, the key generator creates a 128-bit key to decrypt the input original data using the RSA method. The cipher 2 is produced by this method. The two cypher texts, 1 and 2, are then concatenated in the following procedures to get the message ready for transmission.

In this context, "received text" refers to the text that an end user actually sees after it has been broadcast to a network. The first step involves splitting the incoming text into two distinct cyphers, cypher 1 (the result of the key data) and cypher 2 (the encrypted data). In order to generate the key for data recovery, the cypher 1 is processed first, resulting in the cypher text 1, which is then fed into the DES algorithm in order to get the original key, with which the data is decrypted. The RSA algorithm requires a key, which is generated from the recovered key using the deciphered second cypher text. The original text is deciphered by the RSA algorithm, and it is compatible with any other application where authentication of recovered data is required.

Data is subjected to an integrity check at the receiving end. Therefore, the SHA1 hash key and 128 bits of retrieved data are processed first. After that, a comparer is constructed, which serves a dual

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/82

purpose: first, it can use the original key that was used for encryption to recreate itself using SHA1 (128 bits). This means that the 128-bit key is produced using the same method as the network-obtained key, and then the two keys are compared. Additionally, if the two keys are comparable, the system accepts the data.

RESULTS AND DISCUSSION

We compute the experimental evaluation and performance and compare it to the RSA algorithm. In order to make a comparison, we use a number of efficiency indicators. Here, we'll talk about the findings that were uncovered. The phrase "encryption time" is used to refer to how long a certain cryptographic system takes to encrypt a given amount of data. Both the RSA algorithm and the suggested method's encrypting time are displayed in figures 3 and 4 below.

Experiments are carried out using data with varying file sizes, which are represented in the X-axis of the diagram. Time, expressed in milliseconds, is plotted along the Y axis. Proposed method performance is represented by the blue line, whereas RSA algorithm performance is represented by the red line. The outcomes demonstrate the suggested approach is more efficient than the RSA algorithm in terms of time spent. The duration is information-dependent. Figure 4 shows the median performance of different algorithms, which can be used to make rough comparisons. Based on average performance, the proposed method is faster than the RSA algorithm while using fewer resources.

File size	Proposed system	Existing system
15	0.96	2.36
25	3047	5.36
100	8026	44.58
500	32.58	37.25
1500	62.14	68.57
2000	154.32	157.25
2500	168.23	198.45

Table1: Encryption

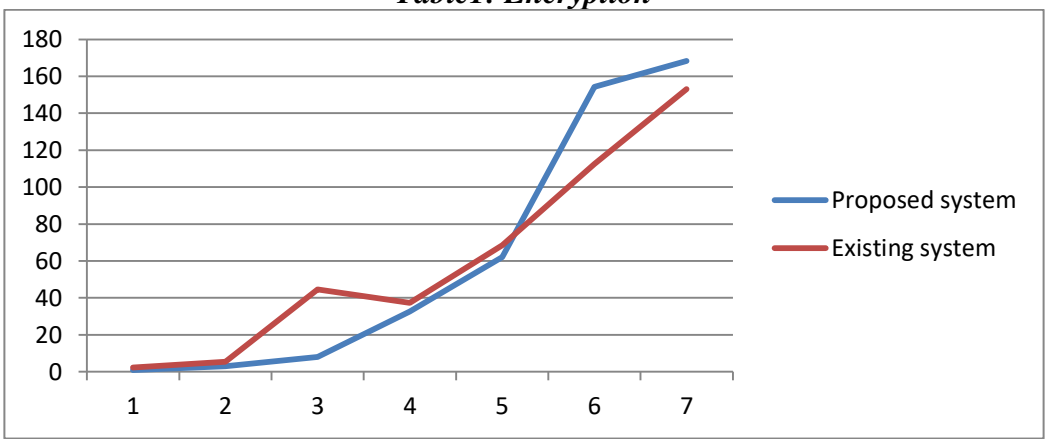

Fig 2: Encryption

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/82

Decryption time is the amount of time it takes to reverse a cypher and reveal the original data. The results of the proposed technique and RSA are compared in Figure 5. This graph displays the time needed to complete an experiment as a function of file size on the X axis and a variety of file sizes on the Y axis. When compared to the RSA algorithm, the suggested approach's decryption time is far more manageable.

As can be shown in Figure 5, the proposed method is more effective than the RSA algorithm. Figure 6 also provides an estimate of the mean decryption time for each to help with the comparison. Outcomes demonstrate that the proposed method is superior to the RSA algorithm. As a result, the suggested method is 6-10 times faster than the RSA algorithm.

File size	Proposed system	Existing system
15	0.96	2.36
25	3047	5.36
100	8026	44.58
500	32.58	37.25
1500	62.14	68.57
2000	124.32	147.25

Table 2: Decryption

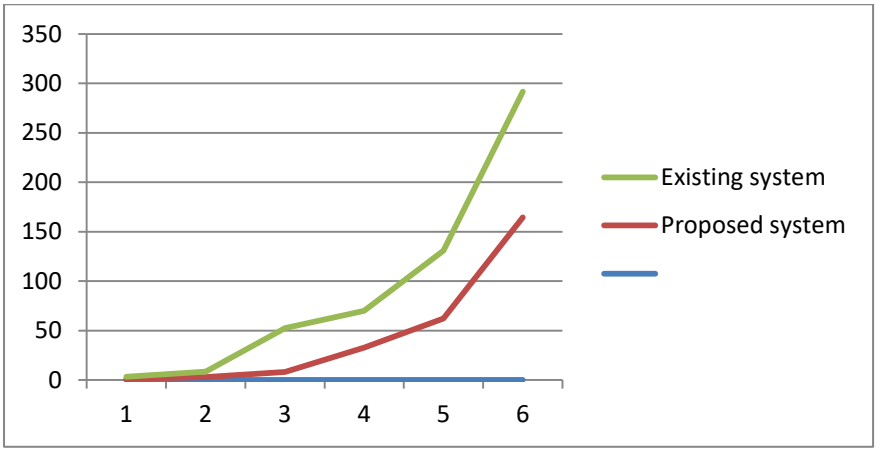

Fig 2: Decryption

CONCLUSION

The efficiency of the proposed cryptographic approach is demonstrated by the experiments. A summary of the suggested method's performance in comparison to existing methods is provided in Table 7. A robust encryption technique is crucial to the proposed work and to this paper. That can efficiently process many data types and generate sophisticated encryption text. Because of this, we have produced a hybrid cryptographic method based on RSA, DES, and SHA1. A bit-discarding procedure is also implemented to improve encryption and safe key creation. This method improves the difficulty of key generation while decreasing key size. JAVA was used to create an operational version of the proposed hybrid encryption method. The space complexity, encryption time, and

Webology, Volume 18, Number 5, 2021
ISSN: 1735-188X
DOI: 10.29121/WEB/V18I5/82

decryption time are also calculated to determine their overall performance. In addition, the proposed cryptographic solution is evaluated in terms of its performance relative to the time-tested RSA algorithm for files of comparable size.

The collected findings show that the proposed method may effectively generate complicated cyphers while consuming fewer resources. Implementing the technique for security using cloud security and other sensitive areas of information security will be further refined in the near future.

REFERENCES

1. Mykola Karpinskyy, Yaroslav Kinakh, "RELIABILITY OF RSA ALGORITHM AND ITS COMPUTATIONAL COMPLEXITY", Computing, 2003, Vol. 2, Issue 3, 119-122
2. Ashita Sharma, Navroz Kaur, "Implementation of DES (Data Encryption Standard) Algorithm", International Journal for MultiDisciplinary Engineering and Business Management, Volume-2, Issue-3, July-September, 2014
3. Hybrid Compression Encryption Technique for Securing SMS Tarek M Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed & Ahmed M Mahfouz
4. HexiMcEliece Public Key Cryptosystem K. Ilanthenral∗ and K. S. Easwarakumar Department of Computer Science and Engineering, Anna University, Chennai 600 025, India
5. Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 21, April 2015 34.
6. Sonal Modh, DR. M. K. Rawat, "Mobile Data Security using TPA Initiated Token Based Cryptography", IJSETR, Vol.05,Issue.06, March-2016, Pages:1140-1146