International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-12 Issue-1, October 2022

Hybrid Cryptosystem Ensuring CIA Triad

P Swapna, S Fazila, K Hanumanthu Naik, G Amrutha Vani, B Reddaiah

Abstract*: *Any untoward incident occurs while transmitting data digitally may lead to threats whenever the data is transmitted to malicious destination unknowingly, there arises a question of data integrity. In this scenario cryptography plays a crucial role in ensuring the users both confidentiality and integrity while transmitting of data over various network platform, supporting with the algorithms like AES, hashing etc., to ensure end user safety. In this paper, an improved hybrid cryptography system which is a combination of message digest and symmetric key algorithm is being incorporated. This proposed system provides confidentiality as well as integrity.

Keywords*: *Hash Functions, RSA Algorithm, Integrity, three fish algorithm, SHA-256.

I. INTRODUCTION

In this electronic era, we come across some of the socioeconomic issues like digital money laundering, password management, fake calls for verification of user credentials and many online transactions (Banking) leading to insecure accessibility of users over digital platforms. There comes the necessity of integrity and confidentiality. cryptography provides a triad of CIA (Confidentiality, Integrity and Availability) for the above said insecurities. It is described in the figure 1.

Fig.1. CIA Triad

If the stated three key terms are satisfied by any organization, then eventually, we are providing security to the system which includes both hardware and software.

A. Confidentiality

Data Confidentiality is intended to prevent data that is being transmitted from unauthorized access. One way to provide confidentiality is performing encryption. Encryption is the process of scrambling data. It is the process of converting the actual data in to unreadable form. Cryptography is also intended [8] for confidentiality.

B. Integrity

Data integrity is proposed to prevent data from being modified by any third party [2]. Integrity ensures that the data is transmitted without any changes. It means, the receiver receives data which is actually sent by the sender. In Cryptography, Hash functions can assure that transactions are reliable and data has not been altered.

The principal objective of hash function is data integrity. A hash function can be pertained to any sized message. It generates fixed length output. It is very difficult to perform decryption to return actual message.

C. Availability

Availability is one of the key terms of CIA Triad. In Availability, we ensure the timely and reliable access to the system. It means, the information must be accessible to the end user. Information is worthless if it is not available.

The proposed approach uses a mixture of symmetric, asymmetric and hashing technique to make the system more efficient. In this paper, RSA Algorithm is adapted for securing our key which is symmetric. The data is encrypted using Three fish Algorithm. Finally, SHA-256 for providing data integrity.

II. LITERATURE SURVEY

"Avinash Jain, V. Kapoor" in 2017, proposed and designed a public key cryptosystem which includes AES Algorithm [3] for encrypting data. Besides, RSA algorithm is given as scrambling for key. However, this proposed work is more efficient [3] than other algorithm in aspects of speed, memory utilization.

"Chitra Biswas Udayan, Das Gupta, Md. Mokammel Haque", projected both the hybrid cryptography and steganography concepts that generate a stego image. This work provides the CIA Triad [4] and also it resists the attacks in an effective way comparing to other algorithms.

"P Varaprasada Rao, S Govinda Rao, P Chandrasekhar Reddy, G R Sakthidharan, Y Manoj Kumar", reviewed various hashing algorithms[5] and proved that Secure Hashing Algorithm(SHA) as the secure one comparing with MD5. This version also considered different attack slowering techniques.

Manuscript received on 24 September 2022 | Revised Manuscript received on 28 September 2022 | Manuscript Accepted on 15 October 2022 | Manuscript published on 30 October 2022.

***** Correspondence Author (s)
P Swapna*, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: piduguwapna22@gmail.com
S Fazila, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: fazila042000@gmail.com
K Hanumanthu Naik, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email:hanumanthukorra@gmail.com
G Amrutha vani, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: amruthagodina@gmail.com
B Reddaiah, Assistant Professor, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: b.reddaiah@yogivemanauniversity.ac.in

"Yogini C. Kulkarni, S.D. Joshi" designed and implemented a security pattern for login system [6] using SHA-384 algorithm. The proposed work concludes that applying changes to the SHA-384 algorithm provides two level security. However, the work is assessed upon different cracking tools. In [7], watermarking algorithms, cryptography and hashing techniques were applied for providing effective security. It concludes that the proposed work is efficient upon different attacks. A Comparative Study of different hashing algorithm is shown in[7], by considering various boundaries it is resolved that SHA is efficient than MD5 Algorithm. While in contrast MD5 is faster than SHA [7] on 32-bit machine.

III. BACKGROUND

There may be some scenarios where we may not even need securing data but instead providing assurance of data. Cryptography helps get rid out of such cases through "integrity". Integrity can be achieved by different ways. One such way of achieving integrity is the use of hash functions. Hashing is a one-way function[1] that accepts any size of message and produce a certain length output as hash code. In general, hash functions are irreversible[1]. It is impractical to reproduce the actual message if only hash value is revealed. There are many cryptographic hashing algorithms such as MD5, SHA-1, SHA-256, SHA-512 and others. These hash functions can be used for attaining integrity. Cryptographic hash functions generates a compressed value of our message. The formed output is termed as "message digest". It is depicted in figure 2.

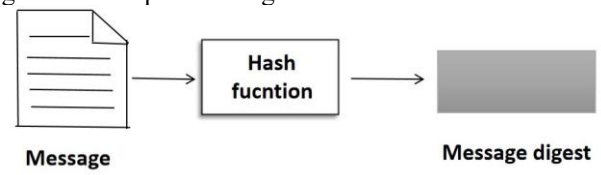

Fig.2. Message and digest

Let us consider a scenario of online transaction applications. We perform a transaction of 5000. Here, two cases exist. There may be a chance of sending 50000 instead. The second one, it may be transferred to some others account without sender's knowledge. This happens due to attacker. They may change the destination address. A security mechanism needs to be implemented to prevent such difficulties. There comes the concept of integrity. Now, let us see how it is known that data is sent actually as it was.

A. Checking Integrity

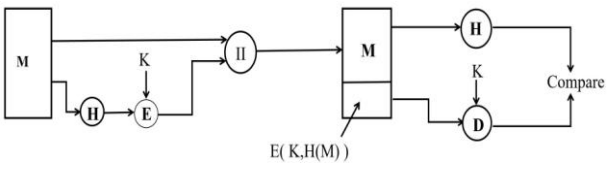

Fig.3. Checking Integrity

To verify the data integrity, we apply the hash function again and match the new digest with the preceding one. If they are similar, it is ensured that the actual data has not been altered. Figure 3 describes the idea. In this paper, SHA-256 is applied as hash function which is considered as more secured [9] one referred to SHA-2 Family.

IV. PROPOSED METHOD

The proposed version includes implementing a combination of symmetric, asymmetric and message digest. This will in turn provides two things. It is securely transmits data. It also provides reliability. Conclusively, a hybrid cryptosystem is implemented. The primitive of the proposed technique is to provide efficient system. Hybrid Encryption uses both symmetric and public keys to enhance the security of the system. This version is more efficient compared with other algorithms. In this paper, a symmetric key algorithm "Three fish" is encrypted using a symmetric key. The message digest of actual data is obtained using SHA-256. This message digest is transmitted along with the encrypted data to the receiver. However, the symmetric key applied is further encrypted using RSA Algorithm. This will accomplish confidentiality as well as integrity concept.

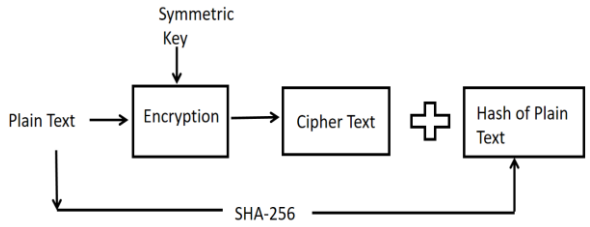

Fig.4. Encryption Process at sender end

A. Encryption Process

The encryption process is done at sender end. The steps involved in this process is described as follows:

1: Secret Key is generated using symmetric algorithm

2: Now, calculate the message digest of the plain text.

3: Then encrypt the message using Threefish algorithm with symmetric key say, S_k.

4: The symmetric key Sk is further encrypted with public key cryptography, RSA algorithm.

5: Firstly, it is encrypted using receiver's public key, say pu_b.

6: The encrypted symmetric key (ESk) is again encrypted using sender's private key, say pr_a.

7: The obtained output generates double encrypted symmetric key (DESk). It is shown in the figure 5.

8: Finally, the cipher text, message digest H1and DESk is transmitted to the receiver. Figure 4 depicts the encryption process of sender.

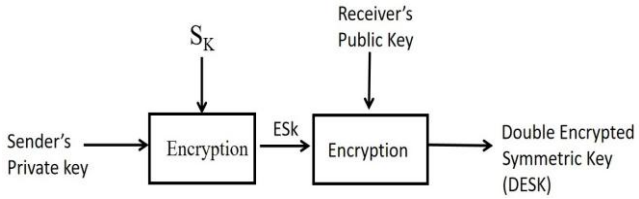

Fig.5. Encryption of Symmetric Key

B. Encryption Process

The decryption process is done at receiver's end. The receiver has the following as inputs, DESk, message digest and C.T. The task that is performed by receiver is described below:

Retrieval Number: 100.1/ijeat.A38411012122
DOI: 10.35940/ijeat.A3841.1012122
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

1: To perform decryption of obtained cipher text user B requires key. Hence, decryption of DESk is done to obtain the actual symmetric key, Sk. From figure 6 it is clearly viewed the decryption process of DESk.

2: Now receiver can decrypt the cipher text (C.T) applying Sk and three fish algorithm to produce plain text. It is seen in figure 7.

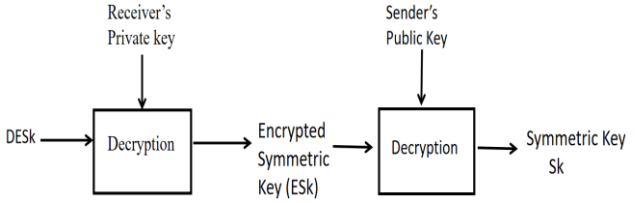

Fig.6. Decryption of Symmetric Key

3: After that the main theme of the proposed technique is performed. The message digest of the newly obtained data of receiver is calculated. Let us assume it as H2.

4: Now, the receiver compares the value of H2 with H1. If both the values are same then we are done. It concludes that there is no change in the data that has been sent by the sender.

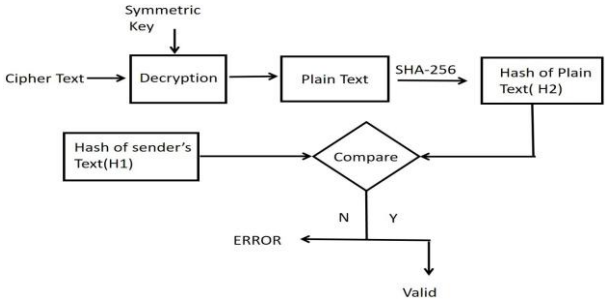

Fig.7. Decryption Process at Receiver's end

V. RESULTS

This paper is successfully completed by implementing CIA concept. The proposed version provides more efficiency than the traditional algorithms. The proposed work is evaluated based on the specific parameters such as Time and Space. Moreover, it is verified using Hash Tool where encrypted data or file is uploaded for checking the integrity. Figure 9, 10 clearly depicts the working of hash tool.

Table 1. Size of Text

Plain Text Size	Cipher Text Size
952	795
736	661
648	632
684	585

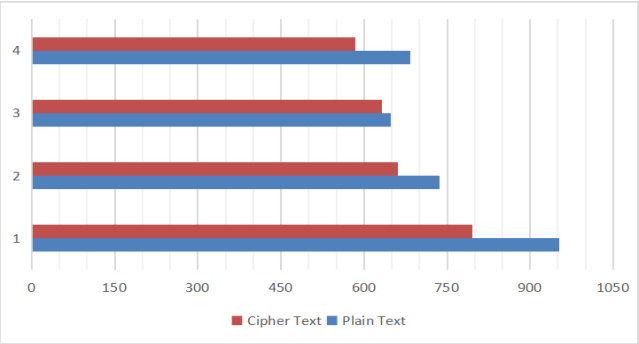

Fig.8. Size of Cipher Text against Plain Text

Table 1 shows the different sizes of plain text taken and the formed cipher texts. Further, the obtained data is depicted graphically as in the figure 8.

The actual theme of the proposed version is described in figure 9, 10. The encrypted file is verified by comparing the hash obtained. It displays the message of the uploaded files after comparing the hashes.

The message success states that there is no change in the data that is received.

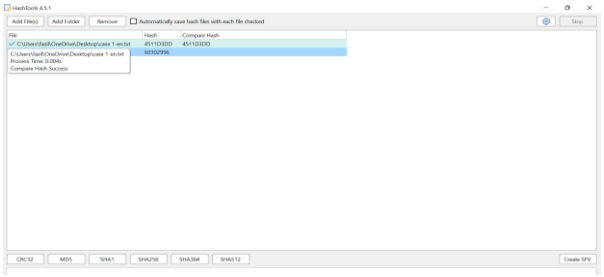

Fig.9. Hash Tool

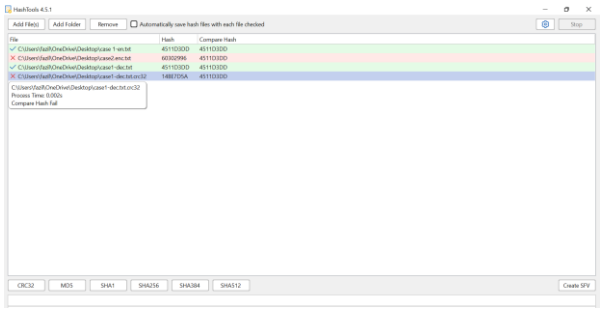

Fig.10. Hash Tool

VI. CONCLUSION

In this paper, a hybrid Cryptosystem has been developed and implemented using a hash tool. It is practically proven that the proposed version has more efficiency compared to actual algorithms. In this paper, a combination of both symmetric and asymmetric is applied which in turn provides more security. However, secret key is encrypted using RSA Algorithm. Ultimately, this version provides integrity as well by applying Hash Tool.

REFERENCES

1. Mark N.Wegman and J.Lawrence Carter, "New Hash Functions and their use in authentication and set equality", Journal of Computer and System Sciences 22, 265-279(1981). [CrossRef]
2. William Stallings, " Cryptography and Network Security" , 3rd Edition, Prentice-Hall Inc., 2005.
3. Avinash Jain and V. Kapoor, "Novel Hybrid Cryptography for Confidentiality, Integrity, Authentication", International Journal of Computer Applications (0975 – 8887) Volume 171 – No. 8, August 2017. [CrossRef]
4. Chitra Biswas Udayan Das Gupta, Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 7-9 February, 2019. [CrossRef]
5. P Varaprasada Rao, S Govinda Rao , P Chandrasekhar Reddy, G R Sakthidharan , Y Manoj Kumar, "Improve the Integrity of Data Using Hashing Algorithms", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-7, May, 2019.

6. Yogini C.Kulkarni, S.D. Joshi, “Security Design Pattern for Login System through Authentication using Modified Sha-384 Algorithm”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075 (Online), Volume-10 Issue-8, June 2021. [CrossRef]
7. Saleh Suleman Saraireh, “PROVIDING CONFIDENTIALITY, DATA INTEGRITY AND AUTHENTICATION OF TRANSMITTED INFORMATION”, VOL. 14, NO. 1, JANUARY 2019 ISSN 1819-6608, ARPN Journal of Engineering and Applied Sciences.
8. S Fazila, B Reddaiah, S Sai Ramya, B J Job Karuna Sagar, C Swetha, “Enhancing AES with Key Dependent S-Box and Transpose MDS Matrix”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075 (Online), Volume-11 Issue-9, August 2022. [CrossRef]
9. S Shajarin, P Leelavathi, B Reddaiah, G Amrutha Vani, C Swetha, “Three Fish Algorithm: T-Mix Cipher using SHA-256”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075 (Online), Volume-11 Issue-10, September 2022. [CrossRef]

AUTHORS PROFILE

P Swapna is pursuing MSc Computer Science from department of Computer Science and Technology in Yogi Vemana University, Kadapa. Areas of interest are Cyber Security and Software Engineering. I am a hard worker and punctual towards my work. I am interested to do research in the field of cyber security.

S Fazila is pursuing M.Sc Computer Science from department of Computer Science and Technology in Yogi Vemana University, Kadapa. Areas of interest are Cyber Security and Web Development. Secured Rank-1 in PGCET-2020. I am a Self-learner and passionate to explore new things. I am interested to do research in the field of cyber security.

K Hanumanthu Naik working as Academic Consultant, Department of Computer Science & Technology, Yogi Vemana University, Kadapa. His Ph.D. Degree awarded at Department of CST, Sri Krishna devaraya University in the year 2016. Number of research publications: 8 reputed international journals. My research interests span both Computer networks, Mobile sensor network, AI and Machine Learning. He received the UGC- RGNF (Rajiv Gandhi National Fellowship) award in 2011. He qualified the APSET-2020 in Computer Science and Application subject conducted December 2020.

G Amrutha Vani has 8 years of experience in teaching. Area of Interest is Software Engineering. My core research area is Network Security. I published 4 papers in various international journals.

B Reddaiah is working as Assistant Professor in department of computer science and technology, Yogi Vemana University, Kadapa, driven to inspire students to pursue academic and personal excellence. Areas of research and interest is in Network Security and Software Engineering. I published 35 papers in various international journals and published 15 papers in different international conferences.