National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(6th and 7th March 2020)
International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

Data Encryption Algorithm – A Comparative Study

Srishti Bangera[1], Pallavi Billava[2], Anush Amin[3], Sunita Naik[4]

[1]Department of Computer Engineering, Mumbai University, MUMBAI
Email: bangerasrishti@gmail.com
[2]Department of Computer Engineering, Mumbai University, MUMBAI
Email: billavapallavi@gmail.com
[3]Department of Computer Engineering, Mumbai University, MUMBAI
Email: anush856@gmail.com
[4]Department of Computer Engineering, Mumbai University, MUMBAI
Email: Sunitanaik@viva-technology.org

Abstract— *Data security is one of the important aspects of today's developing world as a huge amount of data is being digitally transmitted every day. It refers to the process of protecting data from unauthorized access and alteration of data throughout its lifecycle. Threats on the digital data are increasing day by day out of which data confidentiality is most affected among all security goals. Various encryption algorithms are available for securing data authentication and providing better data confidentiality. These algorithms can be combined with each other for better results. In this paper, a comparative study of various encryption algorithms is discussed to get better data authentication and data confidentiality. A comparison of different computational and statistical parameters of the encryption algorithms is studied.*

Keywords — Algorithm, Authentication, Confidentiality, Data, Digital Transmission, Encryption.

I. INTRODUCTION

In today's world with fast-growing technology, almost every work has been digitized[2]. There are various electronic systems that carry out these works online, and all of them deal with a large amount of data[13]. Data is considered valuable, and people are often quite sensitive to how their personal information is being handled. Due to the value of data and the impact it has on people, there is a massive demand for data security.

Data security, also known as information security are protective cyber privacy mechanisims that are used to prevent computers, databases and websites were there are large number of crucial data from unauthorized users[14]. The system can be made much more difficult target for attackers by increasing the security measures that protect the assets, which in turn, will reduce the chances of a system becoming a victim[15]. In this paper, various techniques were studied and compared which are used for providing better data security in digital communication.

II. LITERATURE SURVEY

W.Yin, et.al [1] have proposed a design and implemented the honey encryption mechanisms and have demonstrated its different applications. It also includes evaluation of the performance of the proposed mechanism, design and implementation which address some of the drawbacks of the proposed mechanism. The paper showed a graph (figure 1) for the encryption and decryption required by RSA and symmetric key from which it was observed that the time required for encryption for RSA is four times higher than that required for the symmetric key encryption mechanism whereas the decryption time required by symmetric key encryption mechanism is 46 microseconds while that of RSA is 0.045s. An enhancement is introduced to address the overhead issue faced in Honey Encryption.

s

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

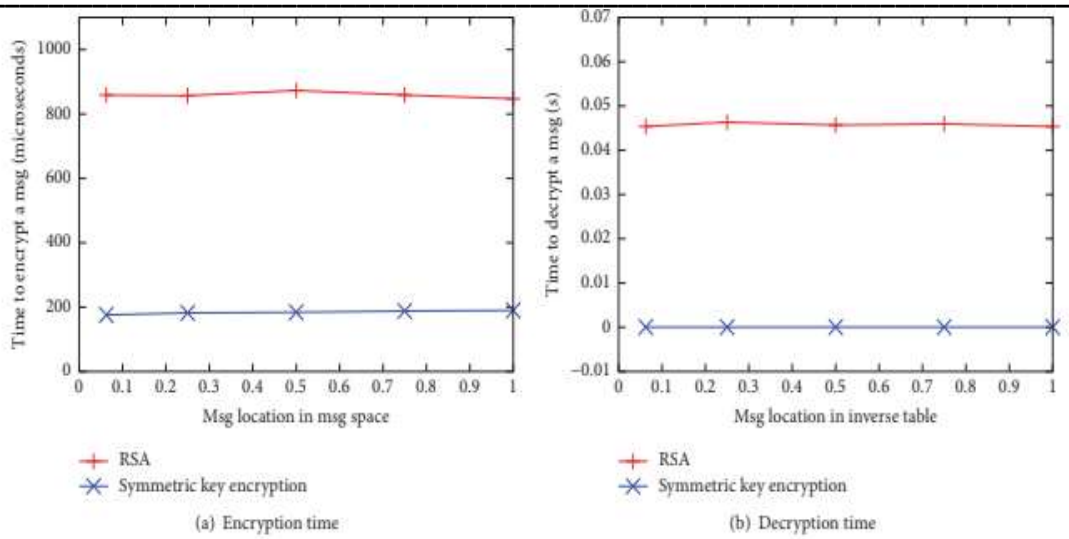

FIGURE 1: Time to encrypt and decrypt a message[1]

A. M. Abdullah [2] has provided an overview of the AES algorithm and explained some of its important features such as security, cost and implementation characteristics. The Advanced Encryption Standard (AES) algorithm is one of the powerful symmetric block cipher algorithms that has its own structure for encrypting and decrypting sensitive data. The paper also includes the demonstration of some previous researches that have been done on AES and comparison of it to other algorithms, where the results obtained from researches show that AES has the ability to provide better data security compared to DES, 3DES, Blowfish, etc.

K.S.M. Moe, et.al[3] has proposed an innovative honeyword generation approach that decreases the storage problem, typo safety problem and also reduces the other drawbacks of existing honeyword generation techniques such as old password management problems. The important aspect of the proposed technique was less time complexity, which was determined in the paper using a table (table 1) and graph. The paper showed that the honey generation method is an effective way for encryption and decryption and has time complexity much less than AES.

TABLE 1
TIME COMPLEXITY FOR LENGTH OF PASSWORD[3]

Length of password(in characters)	Time complexity(second)
7	3.050004
8	3.100004
9	3.140004
10	3.18005

R. Chatterjee, et.al [4] have proposed Natural Language Encoder (NLE) which ia a new type ofsecure encoding scheme. The proposed system helpsconstruct vaults which when decrypted using a wrong password will generate plausible looking decoy passwords. Existing tools from natural language processing were used for constructing NLEs. The paper demonstrated an attack and supporting analysis to show that the existing conventional password-based encryption (PBE) methods are vulnerable to various attacks, thus introduced NLE to overcome these drawbacks of traditional PBE.

E. Mok, et.al [5] has proposed a scheme by appending an additional security mechanism to the encrypted data called as extended Honey Encryption (XHE). The Honey encryption algorithm generates similar bogus data, in which the attack difficult to determine whether the guessed is correct or not. Therefore, this helps to increase the password guessing complexity and cracking attacks.

M. Zhao, et.al [6] haveshown a comparison between four single homomorphic encryption algorithms in the cloud environment. The paper also showed the performance evaluation of fully homomorphic encryption and 5 kinds of fully homomorphic

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

encryption algorithms encapsulate the research situation and its application in a cloud environment.

Piyush [7] has researched a paper that concentrates on honey encryption, the proposed technique that converts its defensive action into both detections (tracing the hacker) and deflection action by generating aspecial type of fake key. It will also show how the victims will be notified about the attack along with other users who also have the probability of being attacked. The paper has successfully explained the basic concepts of honey encryption and how it can be made more powerful and effective. It also showed some real-world applications their proposed system along with its complete working.

B. Patel, et.al [8] have proposed a ranked based voiting system that focuses on ballot casting and tallying using Paillier homomorphic and Elgamal homomorphic encryption schemes and also have compared the results of both the encryption schemes.

N. Patel, et.al [9] have proposed a homomorphic cryptosystemswhich is used for preservingdata security, their properties, and categories.The paper also includes applications of proposed system in the field of could computing, private information retrieval, and data aggregation in a wireless sensor network for privacy preservation.

E. O. Abiodun, et.al [10] the prupose of the research was todiscourage the eavesdroppers by using the decoy based decryption model to strengthenthe current encryption measures, from stealing encrypted message by confounding his resources and time. The proposed model is leveraged from decoys, deception, and artificial intelligence.The proposed work concept was well supported by implementing an instant messaging application. The result showed that the following model will help reduce brute-force attacks on encrypted data andstrengthens state-of-the-art encryption schemes.

Jyun-Neng.Ji, et.al [11] proposed an approach on fully homomorphic encryption (FHE) that allows tp perform mathematical computations directly on encrypted data for ensuring the security of cloud computing. The paper explored and well explained the concept of aggregate plaintext for reducing the computational complexity of encrypted data while showing that how existing systems lack by using bit-level encryption for encryption, and also the paper proposes an efficient scheme, commonly used for sorting and searchingin cloud computing to handle the comparison and swap operation. Experimental results showed that the size of required FHE data can be reduced by using this proposed scheme. For 32-bit data comparison, the proposed one can operate 2.3 times faster and achieve about 52 times a reduction in the required FHE data size as well as the transmission bandwidth to the cloud in comparison to the related.

MS. Akshatha, et.al [12] have proposed that an efficient search method needs to be used in order to search data over the encrypted cloud. While having a large number of data users, and documents on the cloud, it is essential to give multi-keywords in the search query to get documents only relevant to these keywords in a ranked order.

1.1 ANALYSIS

The following table is a summary of various research papers on data security using various encryption techniques.

TABLE 2
ANALYSIS TABLE

Sr.No	Title of paper	Techniques used	Computational and Statistical performance
1.	Protecting private data by honey encryption.[1]	DTE method is used	181microseconds
2.	Advanced Encryption Standards (AES) Algorithm to Encrypt and Decrypt Data. [2]	Advanced Encryption Standards (AES) is used.	4 secs
3.	Improved Hashing and Honey-Based Stronger Password Prevention Against Brute Force Attack.[3]	Honeyword generation technique is used	3 secs
4.	Cracking-Resistant Password Vaults using Natural Language Encoders.[4]	Natural Language Encoder (NLE) is used.	Around 1 sec for large vaults.
5.	Implementing the Honey Encryption	Extended Honey Encryption (XHE)	NA

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

	for Securing Public Cloud Data Storage.[5]	technique is used.	
6.	Homomorphic Encryption Technology for Cloud Computing.[6]	Homomorphic encryption is used.	NA
7.	Advanced Honey Encryption: An escapeless trap for intruders.[7]	The techniques that convert its defensive action into both detection (tracing the hacker) and deflection action with the help of the generation of a special type of fake key.	2 secs
8.	Efficient Ballot Casting in ranked Based Voting System Using Homomorphic Encryption.[8]	Paillier homomorphic and Elgamal homomorphic encryption is used.	Paillier cryptosystem takes less time for an increased number of votes.
9.	Homomorphic Cryptography and Its Application in Various Domains.[9]	Fully homomorphic and partially homomorphic encryption is used.	FHE preserves more privacy than PHE.
10.	Fully Homomorphic Encryption for Ring LWE and Security for Key Dependent Message.[10]	Ring LWE technique is used.	NA
11.	Efficient Comparison and Swap of Fully Homomorphic Encrypted Data.[11]	The FHE method is used.	0.59 secs.
12.	Cloud Data Encryption Using RSA, Enabling Multi-Keyword Ranked Search and Achieving Privacy Requirements.[12]	RSA algorithm is used.	NA

NA- Not Available

III. CONCLUSION

Due to the fast-growing internet world, data security becomes the most important aspect. There are various algorithms that are used to provide data security by using high data confidentiality and enhanced user authentication techniques. In this paper, various techniques used for data security have been studied and analyzed such as the AES encryption algorithm, RSA encryption algorithm, Honey encryption algorithm, and Homomorphic encryption algorithm. The Honey encryption algorithm and Homomorphic encryption algorithm are found efficient for data security. Two or more such encryption techniques can be combined to obtain much higher data security.

ACKNOWLEDGEMENTS

We would like to express a deep sense of gratitude towards our Department of Computer Engineering, for their constant encouragement and valuable suggestions. The work that we have been able to present is possible because of timely guidance and support.

REFERENCES

[1] Wei Yin, Jadwiga Indulska, Hongjian Zhou, "Protecting private data by honey encryption", 2017, https://doi.org/10.1155/2017/6760532.

[2] Ako Muhamad Abdullah, "Advanced Encryption Standards (AES) Algorithm to Encrypt and Decrypt Data", ResearchGate, 2017.

[3] Khin SuMyat Moe, "Improved Hashing and Honey-Based Stronger Password Prevention Against Brute Force Attack", International Symposium on Electronics and Smart Devices, 2017, 978-1-5386-2778-5/17//$31.00.

[4] Rahul Chatterjee, Joseph Bonneau, Ari Juels, Thomas Ristenpart, "Cracking-Resistant Password Vaults using Natural Language Encoders", IEEE Symposium on Security and Privacy, 2015

[5] Edwin Mok, Azman Samsudin, Soo-Fun Tan, "Implementing the Honey Encryption for Securing Public Cloud Data Storage", First EAI International Conference on Computer Science and Engineering, 2017,10.4108/eai.27-2-2017.152270.

[6] Min Zhao, Yang Geng, "Homomorphic Encryption Technology for Cloud Computing", ICICT, 1877-0509.

[7] Piyush, "Advanced Honey Encryption: An escapeless trap for intruders", IEEE, 2018, 918-1-5386-6947-1/18/$31.00.

International Journal of Engineering Research & Science (IJOER)
ISBN:[978-93-5391-287-1] ISSN: [2395-6992] [Vol-6, Issue-3, March-2020]

[8] Bhumika Patel, Purvi Tandel, Slesha Sanghavi, "Efficient Ballot Casting in ranked Based Voting System Using Homomorphic Encryption", Springer, 2019, pp 565-576.

[9] Namrata Patel, Parita Oza, Smita Agarwal, "Homomorphic Cryptography and Its Application in Various Domains", Springer Nature Singapore Pte Ltd, 2019

[10] Zvika Brakerski, Vinod Vaikuntanathan, "Fully Homomorphic Encryption for Ring LWE and Security for Key Dependent Message", Springer, 2011, pp 505-524.

[11] Jyun-Neng Ji, Ming-Der Shieh," Efficient Comparison and Swap of Fully Homomorphic Encrypted Data", IEEE, 2018, 978-1-5386-6947-1/18/$31.00.

[12] Akshatha MS1, Renita Tellis, "Cloud Data Encryption Using RSA, Enabling Multi-Keyword Ranked Search and Achieving Privacy Requirements", IJARCCE, 2018, DOI 10.17148/IJARCCE.2016.5587.

[13] Data security, https://www.quora.com/What-is-the-importance-of-data-security last accessed on 5-Jan-2020.

[14] Data security need, https://www.techopedia.com/definition/26464/data-security last accessed on 5-Jan-2020.

[15] Basic concept of information security, https://www.prolifics.com/blog/basic-concepts-security last accessed on 5-Jan-2020