An Efficient Steganographic Approach for Securing Text Transmission Using S-Box in Cloud

*Humaira Ashraf
department of computer science and software engineering
International Islamic university
Islamabad, Pakistan
humaira.ashraf@iiu.edu.pk

Javeria Malik
department of computer science and software engineering
International Islamic university
Islamabad
Islamabad, Pakistan

Uswa Ihsan
department of computer science and software engineering
International Islamic university
Islamabad, Pakistan
Uswaihsan.mscs1075@iiu.edu.pk

Fatima Al-Quayed
Department of Computer Science, College of Computer and Information Sciences, Jouf University
Sakakah, Saudi Arabia;
ffalquayed@ju.edu.sa

Mamoona Humayun
department of Information Systems, College of Computer and Information Sciences, Jouf University
Sakakah, Saudi Arabia;
mahumayun@ju.edu.sa

NZ Jhanjhi
School of Computer Science and Engineering (SCE), Taylor's University, Malaysia;
NoorZaman.Jhanjhi@taylors.edu.my
Applied Science Research Center, Applied Science Private University, Amman 11937, Jordan
h_gaftim@asrc.asu.edu.jo

2023 International Conference on Business Analytics for Technology and Security (ICBATS) | 979-8-3503-3564-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICBATS57792.2023.10111339

***Abstract*— In era of modern world and technology where everything is digitalized. Cloud computing emerged as one of the fastest growing parts of digital industry. With the Succor of cloud computing models, business accomplishes their objectives with least exertion when contrasted with traditional processing environment. In spite of these compensations, yet security of the information in cloud database is the significant fear in endorsement of cloud. Although several techniques have been proposed such as cryptographic and steganographic approaches, but all of these have some loopholes. Therefore, in this paper new data protection technique based on steganographic encryption is proposed which has less computational time and secure against known plain text and Man-In-Middle Attack.**

Keywords—Cloud Security, Cryptography, Steganography, known plaintext attack, text security in cloud, Man-In-Middle attack.

I. INTRODUCTION

Cloud computing is on request delivery of various administrations on the web, from software to secure storage everything is delivered via internet to the client. Cloud provides the reduction of cost, independence of location, easier maintenance, multitenancy, better performance productivity with security. In the distributed computing framework, the front end alludes to the customer component. In order to advance to the distributed computing phases, it consists of the interfaces and applications. While The Back End comprises to the cloud itself. It consists of the considerable number of assets required to give distributed computing administrations. It contains gigantic information stockpiling, virtual machines, security system, administrations, sending models, workers, and so forth as shown in figure 1.

Though cloud is widely used, there are major issues that need to be resolved, such as data security, storage protection, authentication, uncertain interfaces and API'S, information misfortune and spillage of equipment's. Now everything is done on internet from form submission to large scale business transactions, these transitions are sent on unsecured medium, where attackers can attack and steal the confidential data. For fortifying the private or delicate data manifold cryptography techniques combined with steganography has been proposed. Steganography is strategy of concealing a coded message inside a customary message. The motivation behind steganography is to hold the data under spreads while both the sender and the collector share the data as shown in figure 2. Steganography and cryptography are solidly related; cryptography dissipates the message with the goal that it can't be comprehended while steganography conceals the presence of the message.

Voluminous approaches have been proposed over the past years like AES with LSB, RSA, Random bit generation combined with LSB. This paper proposes an efficient encryption algorithm combined with steganographic technique for securing the text transfer. Presented technique has less computational time as compared to literature and secure against known plaintext and Man-In-Middle Attack. The proposed methodology is based on S-Box, Random key Generation and LSB method. This scheme proposed a new substitution method which is less complex and efficient. The efficient steganographic algorithm takes plain-text and convert it into binary values. Binary values are further divided and substituted with S-box values.

Generated cipher text is further processed with key and embed in image using least significant Method. The complete procedure of proposed scheme in described in section III.

The paper assembled as follows. Segment I describes the Introduction, Segment II discuss the Literature of the cryptographic and Steganographic approaches, Segment III describes the proposed Methodology, Segment IV and V discusses the results and conclusion.

979-8-3503-3564-4/23/$31.00 ©2023 IEEE