DOI: https://doi.org/10.24113/ijoscience.v3i5.51

Data Security through Encryption Technique

Suruchi Karnani
Department of Computer Science and Engineering
SR Group of Institution
Jhansi, Uttar Pradesh., India
suruchi012@yahoo.com

Mr. C.P. Singh
Assistant Professor
Department of Computer Science and Engineering
SR Group of Institution
Jhansi, Uttar Pradesh., India
cp.singh1984@gmail.com

***Abstract*:- Secure computing is one of the fastest growing internet based technology that facilitates users, to utilize services by making use of large number of resources without installation of any software. Adoption of this technology is increasing rapidly because of many advantages including reduction of cost and IT load. Now a days, data security is not only issue but the need of communication speed and size of content is also a measurable problem. in the current paper a scheme has been proposed to which uses the concept of data encryption and compression. In current time the focus has been made specially on cryptography and data compression. In the next phase we have emphasized on compression cryptosystem. Finally, proposed technique has been discussed which used the concept of data compression and encryption. In this first data is compressed to reduce the size of the data and increase the data transfer rate. Thereafter compress data is encrypted to provide security and safety.**

Keywords: Encryption, Security, Confidentiality, Authentication, Integrity.

I. INTRODUCTION

The security of data transmission is the biggest problem in data exchange and data communication networks. The communication system is very faithful whenever it provides security. Normally, users share personal sensitive information or important data. In this case; authenticity, confidentiality, integrity, and security, of the exchanged data should be provided over the transmission methods or mediums. In these days, internet multimedia is very easy to access, user-friendly and popular; a Hugh amount of data is exchanged every second over a non secured channel, which may not be safe. it is very important to protect the data from attackers.For protecting information and data; cryptography and steganography techniques can be used. Cryptography is the technique to keep data transfer safe and secure. This technique provides data encryption for secure communication [1]. The encryption process is applied before transmission, and the decryption process is applied after receiving the encrypted data. Steganography is the technique for writing hidden messages inside a multimedia content; it conveys thedata by concealing it in other medium such as image or audio which is called the cover object. The information hiding technique is should be apply before transmission of the data and the extraction technique should be applicable after receiving the data or information. Encryption is indeed a secure coding technique and data compression is also a coding technique, the main purpose of this technique is to reduce both the space requirements for data storage and the time for data transmission. In this technique data security using private key encryption system encoded string is produced by a model from an input string of symbols and based on arithmetic coding that can be used to achieve the present network scenario for exchange of information with more security and compression [2]. cloud computing can be defined as a technique of computing that delivered IT facilities ‘as a service’ to end users through internet. Foreign large companies such as Google, IBM, Amazon, Microsoft and Yahoo are leading the way in cloud computing. Many other companieslike Myspace, Facebook, Salesforce and YouTube, also make an achievement in cloud computing [3].

The main models of the cloud computing are categories in three parts: (1.1) IaaS (Infrastructure as a service), it completely distracted the hardware working behind it and allowed users to consume infrastructure as a service without any inconvenience about the underlying complexities. (2.1) PaaS (platform as a service), it is developed upon IaaS and provides clients with access to operating software and optional services to develop and use software applications without software installation. (3.1) SaaS (software as a service) enables the user to access online applications and software that are hosted by the service providers. The deployment model of cloud computing include (1.1) Public cloud, which is owned by service provider and its resources are rented or sold to the public. (2.1) Private cloud, owned or rented by an organization. (3.1) Community cloud, similar to private cloud but cloud resources is shared among number of closed community. (4.1) Hybrid cloud, exhibits the property of two or more deployment models [4]. According to survey conducted by International Data

Group (IDG) enterprise, the top three challenges to implementing a successful cloud strategy in enterprise vary significantly between IT and line- of-business (LOB). For IT, concerns regarding security is 66% and 42% of cloud-based projects are eventually brought back in-house, with security concerns 65%. Many vendors declared that adoption of this technology can bring many benefits to the users such as cost reduction, convenience and continuous availability, scalability and performance, easy to deployment and helpful in integration, yet some organization are still not feeling comfortable in adoption of this technology due to concerns of trust and security e.g., data security is one of them.

II. CRYPTOGRAPHY

Cryptography or cryptology is the same word

Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages, in the current time it is very important to provide communication and exchange the information should be safe and secure for the society, and the global economy, the value and quantity of data is intensifying demands to storage on the systems. cryptography is heavily based on mathematical theory and computer science practice; The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export, in data and telecommunications, cryptography is necessary when communicating over any untrusted unsecure medium. In the few previous years however, the trend has been taken placing cryptography into a sound mathematical framework. This modern focus has initiated the evolution of the field from an art in to a science, which includes just about any network, particularly the internet. This evolution comes with new techniques of modern cryptography (MC) really begins with Claude Shannon arguably the father of mathematical cryptography. In addition to his other works on information and communication theory established a solid theoretical basis for cryptography and for cryptanalysis. And with that, cryptography more or less disappeared into secret government communications organizations such as the NSA and equivalents elsewhere. The earliest forms of secret writing required little more than writing implements since most people could not read. Now in these days cryptographic techniques have become the very effective solution to protect information and data against untrusted parties. The cryptography techniques required that data and information should be encrypted with some sort of mathematical algorithm where only the party that shares the information could possible decrypt to use the information.

The main requirements for the specific security are as following: -

Authentication: - is the act of confirming the truth of an attribute of a single piece of data claimed true by an entity.

Confidentiality: - The ethical principle or legal right that a physician or other health professional will hold secret all information relating to a patient, unless the patient gives consent permitting disclosure.

Integrity: - Having integrity means doing the right thing in a reliable way. It's a personality trait that we admire, since it means a person has a moral compass that doesn't waver.

III. LITERATURE REVIEW

The literature review introduces and defines concepts relating to cryptography, issues relating to cryptography need for parallel approach in the cryptography and the development of software frameworks.

The use of parallel processing enhances the speed of system when compared to the traditional crypto systems. In this approach they have divided a file into two slices and have applied a single algorithm with different key for each slice and the processing of the algorithm is done in a parallel environment. Especially nowadays multi-core computers are commonly available. Since the security level provided by most cryptographic algorithms depends on the difficulty of solving some computational problems, the developments in computer systems manufacturing will threaten people’s security. Thus, it is very important to cope with this development and increase the security level by using stronger cryptographic algorithms with longer keys which in return will take longer to encrypt and decrypt data but also a much longer time to hack the cipher text. The literature review summarizes the need for fast and efficient crypto algorithm for present applications. Due to present need it is necessary to have fast algorithm which performs the crypto process in time efficient and secure manner, for this the best method is performing the crypto operation in parallel using available hardware technology. Some of the techniques of cryptography generally are in the use discussed here.

2.1 Cryptography

Plain Text: Any communication in the language that we speak- that is the human language, takes the form of plain text. It is understood by the sender, the recipient and also by anyone who gets an access to that message.

Cipher Text: Cipher means a code or a secret message. When a plain text is codified using any suitable scheme the resulting message is called as cipher text.

Encryption: The process of encoding plain text messages into cipher text messages is called encryption.

Decryption: The reverse process of transforming cipher text messages back to plain text is called as decryption.

Key: An important aspect of performing encryption and decryption is the key. It is the key used for encryption and decryption that makes the process of cryptography secure.

2.1 Purpose of Cryptography

Cryptography serves following purposes:

Confidentiality:- The principle of confidentiality specifies that only the sender and the intended recipient should be able to access the contents of a message.

Authentication:- Authentication mechanisms help to establish proof of identities. This process ensures that the origin of the message is correctly identified.

Integrity:- The integrity mechanism ensures that the contents of the message remain the same when it reaches the intended recipient as sent by the sender.

Non Repudiation:- Non-repudiation does not allow the sender of a message to refute the claim of not sending the message.

Access Control:- Access Control specifies and controls who can access what.

Availability:- The principle of availability states that resources should be available to authorized parties all the times.

2.1 Types of Cryptography

Two types of cryptography is studied:

Symmetric Key Cryptography:- When the same key is used for both encryption and decryption, then that mechanism is known as symmetric key cryptography. The project works efficiently for small size while it consumes time for large size of files. At a instant only one file can be encrypted and transmitted. As a future work multiple file encryption and decryption can be possible. It has broad development prospects.

Asymmetric Key Cryptography:- When two different keys are used, that is one key for encryption and another key for decryption, then that mechanism is known as asymmetric key cryptography.

IV. MOTIVATION

In [5] the secure data security is assured by utilizing the RSA algorithm in which data and Bilinear Diffie-Hellman encrypted while keeping the keys exchanged. The technique which used is the addition of message header in the front of every data packet. When a cloud server receives a request for data storage from a user then it uniquely generates the user public and private key with user identification in certain server (SID) for user. After that it sends the secret key to the uer and unique identification to user for the server. Before a user sends the file to cloud two tasks are performed at user end. Firstly, a message header is added to the data and secondly, data is encrypted including message header by use of secret key. When a user can make a request for data to secure server then it will pick the SID information and also will check the message header of received data. In [6] two important encryption techniques play fair and vigenere incorporated with the structural elements of SDES and DES. In which a fixed block sized 64 bit plain text is considered and converted into two parts by the means of black box. The right part contains 2 bits while left part contains 6 bits, then for the further divisions of these 6 bits they are injected into “superior function” block where they divided in two parts in which first two bits express the rows and last four bits express the column. The corresponding value can be selected by recognizing the rows and columns. Then this function is implemented to all 8 octets vigenere block output and the resultant of black box is again of 64 bits. Four new octants are created by the further division of these bits and similarly right 4 bits are combined for the formulation of right parts. Lastly, left and right parts are XOR-ed to get the left half of this arrangement. Three times this process is repeated. In a technique for ensuring the availability, confidentiality and integrity of data cloud data is introduced in which SSL 128 bit encryption is used which can be then increased to 256 bit encryption. To access the encrypted data a user is required to provide valid user identity and password. A three layered based data security model is proposed in where every single layer perform different task to secure data in cloud. First layer performs the task of authentication, second layer is responsible for data encryption and third layer perform the task of data recovery. Additionally, at cloud end software is implemented with two aspect authentication. One characteristic of this software is that it compares the eight recent encryption algorithms and to get the fastest and highest security algorithm which is based on cloud infrastructure. In RC5 an algorithm is implemented for the sake of secure data security in which encrypted data is transmitted even if the data is stolen because there will be no relevant key to decrypt this data. In Role Base

Encryption (RBE) technique is suggested for secure data security and role base access control (RBAC) cloud architecture for organizations in which they can store data securely in public cloud, whereas information about the organization's structure is maintained in private cloud. In [7] four authorities (data owner, data consumer, cloud server and N attribute authorities) are explained and attribute authorities sets were divided into N disjoint sets according to their category. The data owner will get the public key from any one of the authority and will encrypt the data before sending it to the cloud server. When data will be requested then the private key will be created by authorities and delivered to data consumer after that the consumer will be able to download the file if and only if he or she satisfies the related authority tree and approved by cloud server In two secured cloud computing types are suggested in which one type needed a trusted third party but the other does not. These types use Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing to ensure the data security in cloud environment. For the protection of cloud data confidentiality, a technique proposed in which digital signature and Diffie Hellman key exchange are used with Advanced Encryption Standard encryption algorithm. This scheme provides data security, verification and authentication simultaneously therefore known as three way approach. In [8] a method that was based on location encryption proposed for secure data security in which geographical position and user location were used. In that method a geo encryption algorithm was applied on the cloud and user computer and then a label which identify the person or company was used on data. So, when the data will be required then the same label will be searched and retrieved and the information related to label will be retrieved from the cloud. After that data will encrypt by using Geo- Encryption algorithm along with information that was retrieved from cloud and then data will be delivered to user.

A. Short Group Signature

In the paper [9] author had construct short group signature scheme this means that the computation time taken to complete the task is very less. Group signature is a method for allowing a member of a group to anonymously sign a message on behalf of the group. Group manager has the ability to reveal the original signer in the event of disputes. These group signature are a generalization of credential/membership authentication schemes, in which one person prove that he belong to certain group. Security of a group signature is based on strong deffie-hellman assumption. In bilinear groups there is a new assumption called decision linear assumption. Random oracle model is used to provide security. Short group signature scheme length is below 200 bytes and it provide approximately same security to that of RSA signature length. Strong deffie hellman was constructed without random oracle. In this they had also make use of zero- knowledge proof of knowledge protocol to provide solution to strong deffie-hellman problem. With the help of Fiat-shamir heuristic algorithm signature scheme will be secure under random oracle model. There are three properties that a group signature scheme must satisfy

1. Correctness
2. Full-anonymity
3. Full-traceability

Correctness ensure that the signature generated must be verified and trace correctly. Full-anonymity ensure that the signature do not reveal their signer's identity. And full traceability ensures that all signatures, even those created by the collusion of multiple users and the group manager, trace to a member of the forging coalition. Using these properties they had proves the security of group signature. Revocation mechanism has been used for a group signature. In this revocation list is given to all user in the group. Revocation list contain private keys of all revoked user. It is used to update the group public keys which is used to verify signatures.

B. Broadcast Encryption

In this paper author had introduce new theoretical measures for broadcast transmission. They had designed qualitative and quantitative assessment of encryption scheme. In this paper they had present several scheme which allow center to broadcast secret key to any subset of privileged user which does not come in the universe of size n so that coalitions of K users which is not in the privilege set cannot learn the secret key.

V. CONCLUSON

This validation area needs the attention of the research community to gain the trust and confidence of cloud computing users. This paper provides implementation of encryption and decryption algorithm for text file using different cryptographic method using python as programming language. The encryption and decryption are implemented for Caesar cipher and subdivision algorithm. In this wireless world nowadays, the security for the data has become highly important since the selling and buying of products over the open network k occur very frequently. Main feature of this method is that it satisfies the properties of Confusion and diffusion and also has a perfect guess of encryption key makes decryption impossible. In this paper discussed about cryptography, authentication, confidentialities, integrity, non repudiation, access control, and availabilities.

REFERENCE

[1] Ajna Madanan and Dr. S. Poorna chandra,"Comparative Study on Watermarking & Image Encryption for Secure Communication," International Journal For Trends In Engineering & Technology Volume 5 Issue 1 – May 2015 - ISSN: 2349 –9303.

[2] Bobby Jasuja, Abhishek Pandya, "Crypto-Compression System: An Integrated Approach using Stream Cipher Cryptography and Entropy Encoding", International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 21, April2015.

[3] Mrs. Snehal A. Narale, Dr. P.K. Butey, "Employing Security Techniques In The Current World Of Cloud Computing Environment: A Study", Ijcsmc, Vol. 4, Issue. 4, April 2015, pg.796 –801.

[4] Sonali Ghodke,"An Overview of Application Security in the Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 12, December 2015 ISSN: 2277128X.

[5] Richa Dubey, Apurva Saxena and Sunita Gond,"An Innovative Data Security Techniques Using Cryptography and Steganographic Techniques", Richa Dubey et al,/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2175-2182.

[6] Aized Amin Soofi, M.Irfan Khan, and Fazal-e-Amin," Encryption Techniques for Cloud Data Confidentiality", International Journal of Grid Distribution Computing Vol.7, No.4 (2014), pp.11-20 http://dx.doi.org/10.14257/ijgdc.2014.7.4.02.

[7] Syeda Rabiya Basri, Rashmi K H, "Attribute Based Revocable Data Access Control for Multi Authority Cloud Storage ", International Journal of Advanced Research in Computer Engineering &Technology(IJARCET) Volume 4, Issue 5, May 2015.

[8] Borse Manoj V, Bhandure Harshad D, Patil Dhiraj M and Bhad Pratik B,"Location Based Encryption-Decryption Approachfor Data Security", International Journal of Computer Applications Technology and Research Volume 3– Issue 10, 610 - 611, 2014.

[9] Dan Boneh, Xavier Boyen, and Hovav Shacham," Short Group Signatures", An extended abstract of this paper is to appear in Advances in Cryptology—CRYPTO 2004,Springer-Verlag.