THEORY AND PRACTICE OF SECRET DATA IN COMMUNICATION USING CRYPTOGRAPHY

Aniket Kumar Singh[1], Prince Kumar Sah[2], Anirban Bhar[3], Shambhu Nath Saha[4]

[1,2] *B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*
[3]*Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*
[4]*Associate Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*

ABSTRACT

Securing the information is becoming a key consideration when communicating across a network in the modern world of communication. Users frequently trade sensitive information and documents when communicating. Security is therefore a key factor in communication. Communication and security go hand in hand. It is commonly acknowledged that the architecture of future IT systems will be heavily influenced by data security. Numerous of these IT applications will be implemented as embedded systems that largely rely on security measures. Examples include copy protection systems for audio/video consumer items, wireless computing, pay-TV, wireless phone security, and digital theatres. Keep in mind that a sizable portion of those embedded applications will be wireless, making the communication channel particularly weak.

Cryptography is the study of secure communication techniques that allow only the sender and intended recipient of a message to view the content. It is a type of a rule or a technique by which private or sensitive information is secured from the public or other members. It focuses on the confidential data, authentication, data integrity etc. It is a field of computer science and mathematics which focuses on techniques for secure connection between two parties while a third party is present. It is based on methods like encryption, decryption, signing, etc.

Keyword: - *Cryptography, Cipher, Encryption, Network Security.*

1. INTRODUCTION

It is commonly acknowledged that the architecture of future IT systems will be heavily influenced by data security. The PC had been the main engine of the digital economy up until a few years ago. The focus has now shifted toward IT applications implemented as embedded systems. Security for wireless phones, faxes, wireless computing, pay-TV, copy protection techniques for audio/video consumer products, and digital theatres are just a few of the applications that largely rely on security measures. It's important to keep in mind that a sizable portion of those embedded apps will be wireless, making the communication route more insecure and the requirement for security much more critical.

Data processing in real time is necessary for this fusion of communication and compute capabilities, and DSPs have shown to be effective in a variety of applications. The design and optimization of digital signal processors allows them to carry out some arithmetic operations at extremely fast rates. DSPs are crucial components of many communications devices that we use and will continue to utilize on a daily basis, whether directly or indirectly. Cellular phones, fax machines, pagers, and Internet-based tools like modems, multi-service networks that enable the use of IP telephony, Digital Subscriber Line (DSL) technologies, and some electronic commerce devices are just a few examples of such uses [1]. The rapid expansion of digital communications also creates new security challenges outside of embedded devices. Every day, millions of transactions are done electronically, and the explosive expansion of eCommerce has made security a top concern for many customers. Megabytes of private data will be transmitted around the world over insecure communication channels in the future when important commercial prospects are realized online. Therefore, it is crucial that all these transactions be carried out in a secure manner in order for modern organizations to succeed. Particularly, it is important to prevent unwanted access to information, protect privacy, and confirm the validity of electronic documents. We can address these issues thanks to cryptography, which combines art and science to safeguard messages. We think that implementing cryptographic engines on DSPs is a potential way to secure eCommerce systems [2].

Computer data is transferred from one device to another, protecting the physical environment. When the data is out of control, it might be changed or faked for amusement or the benefit of those with bad intentions. Our data can be formatted and turned using cryptography to make the transfer between computers safer. Our data are fiercely protected by the technology, which is based on secret codes that have been strengthened by contemporary mathematics.

- **Computer security** – It is a term used to refer to tools used to protect data and stop hackers. Data protection measures for networks during transmission Network safety.
- **Internet Security** - Data collecting from connected sources combined with data protection measures Attacks, Services, and Mechanisms for Security A structured way to establish security requirements and characterize approaches to meeting them is necessary for the security manager in charge of an organization's safety needs to successfully assess their level of safety.

2. RELATED WORK

Numerous defense approaches were proposed for tackling cloud threats and vulnerabilities after research on cloud storage systems. In their draught of cloud computing overview and recommendations, NIST covered cloud security risks and challenges [3]. The Cloud Security Alliance has offered comprehensive advice for the cloud emphasis areas stated in [4]. They covered a number of security topics, including identity management, encryption and key management, and application-level security for data protection. Out of these, researchers frequently focus on encryption and identity management.

The majority of cloud storage research focuses on single cloud environments, which store all data in one location and are therefore vulnerable to attacks from system administrators, problems with data integrity, and data losses caused by vendor lock-in issues. As a result, a multi-cloud environment was developed, as mentioned in [6], where performance is enhanced by sharing trust and security among various clouds. They covered a variety of multi-cloud-based systems, including RACS, DepSky, and HAIL, along with their benefits and drawbacks. All of these systems employ distributed file systems (DFS) to share and store user files across a dispersed network. Popular DFS has been discussed by authors in [7] and [8]. In [9], Paval Bozh proposed improving DFS's reliability and performance by distributing the file's data and metadata independently on the server. The RACS system, which is explained in [10], is centered on building a redundant cloud storage array that is primarily concerned with data and economic failures. Parameters for maintaining security and privacy will be integrated in the DepSky model [12], which works to ensure availability and integrity while HAIL system [11] works to preserve confidentiality and integrity in the cloud. In [16] and [17], authors examined multi-cloud systems with a focus on cost efficiency and failure management.

3. SECURITY ISSUES

The following is a list of some trends that have a big impact on cyber security.

Web hosts: Web application attacks that seek to steal data or spread malicious code remain dangerous. Cybercriminals spread their harmful malware by infiltrating legitimate web servers. Attacks that steal data, however, nevertheless constitute a serious concern and are constantly in the news. Now, we must concentrate more on protecting web servers and web applications. Web servers are particularly effective platforms for these thieves to steal data. One must always use a safer browser, especially while doing crucial transactions, to prevent falling victim to these frauds.

The cloud and its services: All small, medium, and large enterprises are now steadily implementing cloud services. In other words, the clouds are progressively becoming encircled by the ground. This most recent trend poses a serious threat to cyber security since communications can avoid traditional ports of inspection. As there are more apps available in the cloud, policy controls for web applications and cloud services will also need to alter in order to prevent the loss of crucial data. Security issues continue to be a top priority despite the fact that cloud providers are developing their own models. Although the cloud may have many advantages, it is crucial to keep in mind that as the cloud grows, security issues also arise.

APTs and targeted attacks: A new type of malicious malware known as a "APT" (Advanced Persistent Threat). For years, detecting such targeted assaults has relied heavily on network security techniques like web filtering and intrusion prevention systems (IPS) (mostly after the initial compromise). Network security needs to integrate with other security services to identify attacks as they happen since attackers are becoming more daring and using shadier methods. To prevent future risk emergence, we must therefore strengthen our security mechanisms.

Mobile Networks: We are able to communicate with anyone, wherever in the world, thanks to current technology. However, security is a major concern for these mobile networks. As more people use gadgets like tablets, phones, PCs, and other similar ones—all of which require additional security measures in addition to those found in the programmes being used—firewalls and other security measures are becoming more permeable nowadays. Always take into account how secure these mobile networks are. Furthermore, these cybercrimes are quite susceptible to mobile networks, thus utmost caution must be utilized in the event of any security issues.

IPv6: New Internet Protocol: The new Internet protocol, IPv6, will eventually replace IPv4 (the old protocol), which served as the basic skeleton of the Internet and our networks. To defend IPv6, more is required than only moving IPv4 capabilities. Although IPv6 completely replaces IPv4 in terms of increasing the number of IP addresses available, security policy still needs to account for certain fairly fundamental changes to the protocol. To reduce the risks connected with cybercrime, it is therefore always desirable to switch to IPv6 as soon as is practical.

Encryption is the practice of encrypting communications (or other information) so that snoopers or hackers cannot read them. An encryption approach converts the message or information into an unreadable cypher text using an encryption algorithm. Usually, this is done using an encryption key, which specifies how the message will be encoded. At its most fundamental level, encryption protects the confidentiality and integrity of data. Additionally, data sent across networks (including the Internet and e-commerce), mobile devices, wireless microphones, wireless intercoms, etc. is protected by encryption. Therefore, one can ascertain whether there has been any information leaking by encrypting the code.

4. CRYPTOSYSTEM TYPES

4.1 Asymmetric cryptosystems

The messages are sent and received using two distinct keys. Another key is used for forward encryption, and it uses the public key for encryption. When two users A and B need to communicate, A encrypts the message using B's public key. B decodes the text using a private key. Other names for it include public key cryptosystems. Public and private keys are generated during a Diffie-Hellman key exchange.

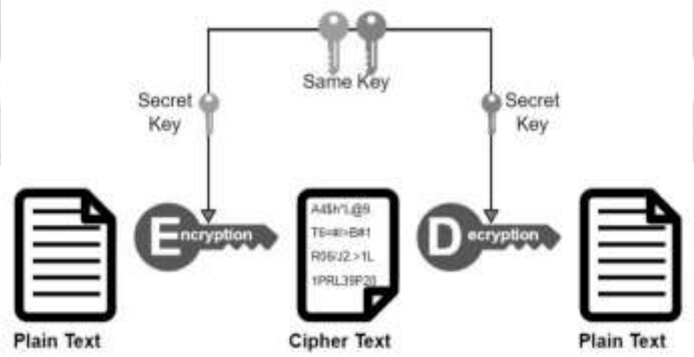

Fig -1: Asymmetric cryptosystem

4.2 Symmetric cryptosystems

Enciphering and deciphering keys in symmetric cryptosystems are either identical or occasionally closely linked to one another. If the key is not held more securely, secure communication will be impossible in the future. Keys should be shared between users over a secure channel, and they should be more secure. One illustration of a symmetric cryptosystem is the Data Encryption Standard (DES).

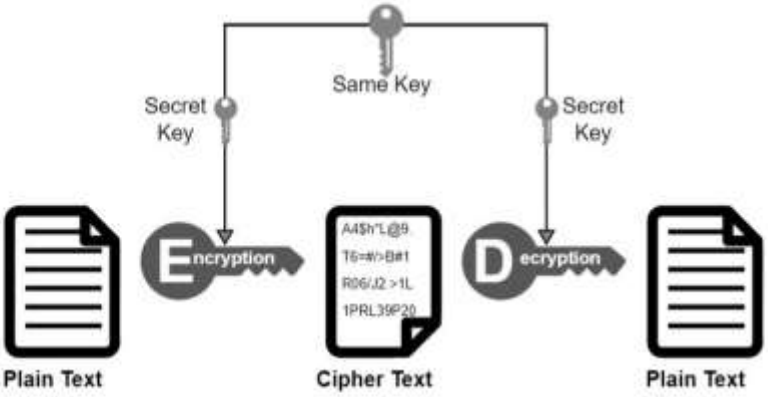

Fig -2: Symmetric cryptosystem

5. METHODOLOGY

The primary goal of the proposed approach is to provide a reliable and secure mechanism for information concealment. Cryptography algorithms were utilized to meet the requirements for security, robustness, and capacity.
The RSA technique is used to encrypt the message before it is inserted using the suggested manner. At the receiver, the information is extracted from the side. In order to do this, the concealed information file had to be selected first. Following file selection, advance LSB is used to erase the information that has been scrambled before RSA is used to scramble it again.
Below is a presentation of the suggested information extraction process.

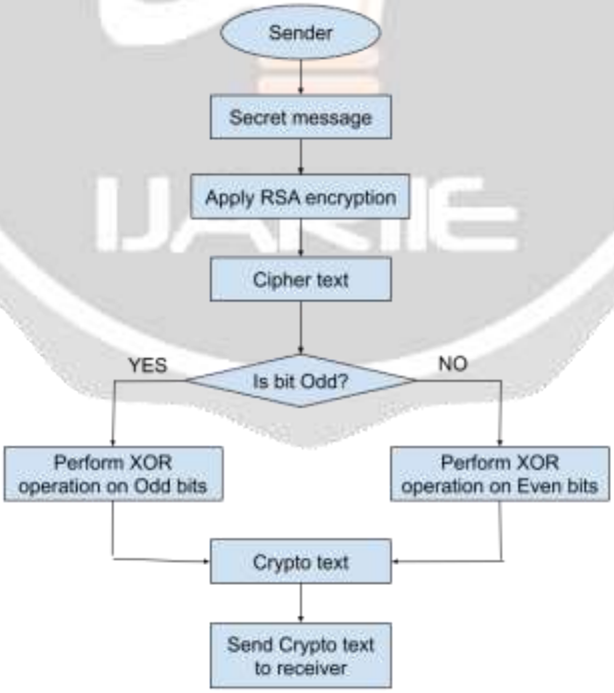
Sender
Secret message
Apply RSA encryption
Cipher text
YES
Is bit Odd?
NO
Perform XOR operation on Odd bits
Perform XOR operation on Even bits
Crypto text
Send Crypto text to receiver

Fig -3: Proposed flowchart

There are of course a wide range of cryptographic algorithms in use. The following are amongst the most well-known:

1) DES: This is the 'Data Encryption Standard'. This is a cipher at operates on 64-bit blocks of data, using a 56-bit key. It is a 'private key' system.
2) RSA: RSA is a public-key system designed by Rivest, Shamir, and Adleman.
3) HASH:A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is sometimes known as a 'message digest', or a 'fingerprint'.
4) MD5:MD5isa128 bit message digest function. It was developed by Ron Rivest.
5) AES: This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST.
6) SHA-1:SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160bits(20bytes).Because of the large digest size, it is less likely that two different messages will have the same SHA-1 message digest. For this reasonSHA-1 is recommended in preference to MD5.
7) HMAC: HMAC is a hashing method that uses a key in conjunction with an algorithm such asMD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1.

6. CONCLUSIONS

Any firm whose internal private network is connected to the Internet must now consider network and data security due to the Internet's fast expansion. Data security has grown to be of utmost importance. The privacy of user data is a key concern with cloud computing. Cryptographic techniques are becoming more adaptable with more mathematical tools, and frequently use many keys for a single application. the numerous cryptographic techniques employed for network security. A fundamental step in achieving high security in the cloud is to encrypt messages using a strongly secure key that is only known by the sending and receiving ends. A crucial aspect is the safe key transfer between sender and receiver. Key management protects confidential information from being accessed by unauthorized parties. In order to confirm the message's legitimacy, it can also check the message's integrity. Cryptographic algorithms used in network protocols and network applications fall under the category of network security. This essay focuses on the dangers to computer network security while briefly introducing the idea of computer security. Future research can focus on the best encryption algorithm and key management techniques for cloud data security.
Secure communication in the presence of outside parties is practiced through the use of cryptography. Its goal is to make it challenging for an observer to comprehend the communication. Numerous applications, such as email, file sharing, and secure messaging, require cryptography. Cryptography is a strong instrument for secure communication, but it is not flawless, according to the research. A cryptographic system can be attacked in a variety of ways, and fresh methods are consistently being found. Although cryptography is a crucial component of security, it is not the only thing to take into account.

7. REFERENCES

[1] Tom Engibous. The Communications Age - It's Real Time. Presentation given at the Dow Jones/Wall Street Journal Europe CEO Summit, June 22nd 1999. At http://www.ti.com/corp/docs/investor/speeches/wsj99/.
[2] B. Schneier. Applied Cryptography. Wiley & Sons, 2nd edition, 1996.
[3] Lee Badger, Tim Grance, Robert Patt-Corner, Jeff Voas DRAFT Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146, May 2011.
[4] Cloud Security Alliance (CSA). “Security Guidance for Critical Areas of Focus in Cloud Computing V2.1,” (Released December 17, 2009).
[5] Zhifeng Xiao and Yang Xiao, “Security and Privacy in Cloud Computing”, IEEE Communications Surveys & Tutorials, March 2012.
[6] MohammedA. AlZain, Eric Pardede, Ben Soh, James A. Thom, “Cloud Computing Security: From Single to Multi-Clouds”, IEEE 45th Hawaii International Conference on System Sciences, 2012.
[7] Tran Doan Thanh, Subaji Mohan, EunmiChoil, SangBum Kim, Pilsung Kim “A Taxonomy and Survey on Distributed File Systems,” IEEE Fourth International Conference on Networked Computing and Advanced Information Management, 2008.
[8] Satyanarayanan, M., "A Survey of Distributed FileSystems," Technical Report CMU- CS-89- 116, Departmentof Computer Science, CarnegieMellonUniversity, 1989.
[9] PavalBzoch, Jiri Safarik, “Security and reliability of distributed file systems,” 6th IEEE international con. on intelligent data acquisition and advanced computing systems, Sep 2011.

[10] Hussam Abu-Libdeh, Lonnie Princehouse, Hakim Weatherspoon, " RACS: A Case for Cloud Storage Diversity", International conference for Internet technology and Secured Transaction, December 2012.
[11] Kevin D. Bowers, Ari Juels, Alina Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage", 16th ACM conference on Computer and communications security, November 2009.
[12] Alysson Bessani Miguel Correia Bruno Quaresma Fernando Andre Paulo Sousa, " DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds", ACM Transaction on Storage, Vol. 9,No. 4, Article 12. November 2013.
[13] DaliborPeric, Thomas Bocek, Fabio Victora Hecht, David Hausheer, Burkhard Stiller, " The design and evaluation of a distributed reliable file system," Int. Conference of parallel and distributed computing, application and technologies, 2009.
[14] Hung-Chang Haiao, Hsueh –Yi Chung, HaiyingShen, Yu-Chang Chao, "Load rebalancing for distributed file systems in clouds," IEEE transactions on parallel and distributed systems, Vol. 24, No. 5, May 2013.
[15] KhengKok Mar, "Secured virtual diffused file systemfor the cloud," 6th International.
[16] IEEE conference on internet technology and secured transactions, UAE, December 2011.
[17] Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, Yafei Dai, " CHARM: A Costefficient multi cloud data hosting scheme with high availability," IEEE Transactions on Cloud Computing, Vol. 3, Issue 3, July-September 2015.