Volume 3, No. 11, November 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

APPLICATION OF FUZZY ERROR CORRECTION IN SOLVING SECURITY ISSUES IN ONLINE COMMUNICATION

Akshay Kumar Tyagi
Research Scholar Mewar University, Chittorgarh, Rajasthan
akshaytyagi@airtelmail.in

***Abstract*:** The paper will discuss the applications of fuzzy error correction in the field of information and communication security. It is clear that cryptography has become an interesting field in computer science. There are many methods that have been devised in cryptography that are used to secure applications. Currently, cryptography is used to secure communications and network systems. This paper will look at the application of fuzzy error correction in solving security issues in communication.

INTRODUCTION

It is evident that cryptography is becoming a very important field in computer security. With the use of this method, it becomes more difficult to generate, store and undertake the retrieval of strings in such an environment. Under such settings, strings, whose behavior is neither random nor can be reproduced constantly, are seen to be abundant. Two common examples are the scan of the retina and looking from common person thumbprint. These two measurements are not imitated every time they are taken for measurement. Currently, there is the emergence of networks and communication channels that are making business support and corporate processes easy to be managed. Although this is the case, the emergence of threats regarding information security and privacy is becoming real every day, and management of information security faces a lot of dangers.

There are various methods that have been devised for managing information security and privacy. The purpose of this paper is to provide ways of managing information security with the use of fuzzy error correction.

FUZZY CRYPTOGRAPHY

Professionals like to try much cryptographic equipment to come up with security methods. These are normally found to be noisy and not exact. In the same case, fuzzy secrets can be assessed in biometric characteristics that are hidden in a scan of the retina instead of a thumbprint. An example is a long password that has been persistently stored in memory, or it could be one's reaction, which is seen to be impulsive in response to personal questions. If it were be possible, a technician would be in search of a method to change the above into keys that can be used in cryptography. This is one reason as to why there is some emergence of techniques to be used in security management.

The use of fuzzy cryptography gives a perfect way in which potential network errors can be corrected, and the security of the network is enhanced. It is evident that the use of next generation security mechanisms is far much better than what have been used so far. The current mechanisms have improved network security and enhanced communication networks in terms of privacy.

PROBLEM DEFINITION

With the emergence of new ways of communications, like mobile devices, the issue of security and privacy has increased. The current communication trends have brought more security threats. The main purpose of this paper is to apply the technique of fuzzy cryptography in enhancing and achieving better security and giving unobtrusive networks.

Context-based pairing of device in fuzzy cryptography:

One area in which fuzzy cryptography can be applied is in mobile device pairing. The proposed solution is the use of fuzzy cryptography in securing mobile communication networks. It is aimed at security pair of mobile devices. The use of cryptography to secure communication networks is becoming common.

Cryptography concept:

Cryptography is the study and practice of the techniques that are used in securing communication and data especially in the presence of potential unauthorized third parties or adversaries. Third parties influence the security of data and information in a communication channel; these influences are mainly concerned with several principles of data security which include: authentication, confidentiality, non-repudiation and data integrity(Bellare and Rogaway 10).

Techniques in cryptography:

According to Brauer (51), there are three techniques of cryptography. These techniques are essentially based on the mode of data encryption which is used by the sender and the recipient of the information. These techniques include:
i)Symmetric key cryptography

This is a type of cryptography where the sender of the information and the recipient use a single key for encryption and decryption of information respectively. It is sometimes referred to as secret key cryptography. The encryption key is also the decryption key; therefore, the sender encrypts the information or message and sends the cipher text to the receiver. The recipient then decrypts the message and retrieves the information using the cipher text. This technique, however, has a major challenge of communicating and distributing the secret key. The symmetric encryption schemes can be classified into two

categories, namely, block ciphers and stream ciphers(Bauer 51).

A stream cipher encrypts one byte (single bit) at a time and creates some feedback mechanism where the secret key is constantly changed. This scheme is of two types the self-synchronizing stream ciphers and the synchronous stream ciphers. On the other hand, a block cipher encrypts a block of data at a time with the same secret key for each block. Block ciphers can operate in several modes, among these are: electronic Codebook (ECB) mode, Cipher Block Chaining (CBC) mode, output feedback (OFB) mode and Cipher feedback (CFB) mode(Bauer 52).

In addition to these schemes, the technique has several algorithms that are used in the modern age: Data Encryption Standards (DES), Advanced Encryption Standard (AES), CAST-128/256, and the international Data Encryption Algorithm (IDEA) among others.

ii)Asymmetrical cryptography

This technique does not utilize the secret key; the communication can ,however, be done through a public platform without privacy or security issues. This is made possible by the use of two different keys. This technique employs two keys that are mathematically related but unique. One key is termed the public key and the other the private key. One is used to encrypt the message and the other is used to decrypt the cipher text; both of these keys are needed to ensure the communication is complete (Denning 25).

The public key may be advertised and made public, but the private key, as the name suggests, is not revealed to any other party. This technique ensures there is non-repudiation in the communication network. This is due to the ability to know the sender of a message. The public key used by the sender can be used to decrypt the message. This is achieved using the sender's private key. Asymmetric cryptography has several algorithms that are used in the modern age for digital signatures and key exchange(Bauer 52). These algorithms include:

RSA developed at MIT, D-H (Deffie and Hellman) Algorithm, Digital signature Algorithm, key Exchange Algorithm (KEA) and LUC algorithm among others.

iii)Hash Functions

Hash functions are also referred to as one way encryption or message digests. These techniques use no key for communication and transmission; instead, fixed length hash value is always computed based on the length of the message or data to be transmitted. The hash value makes it impossible to know the length or the contents of the message (Bellare and Rogaway 45).

The hash technique, basically, provides a digital finger print of a file's contents, the finger print ensures that the file is not altered through a virus or unauthorized access. This technique provides the measure of data integrity. The hash algorithms that are currently in use include: message digest (MD) algorithms, Secure Hash algorithm (SHA), HAVAL (*Hash of Variable Length)* algorithm among others(Gary 15).

These variety techniques and algorithms in cryptography provide various users with the necessary data and communication security. Each of these techniques has been optimized for a specific application(s). The symmetrical key cryptography, for instance, is used to encrypt messages thus ensuring privacy and confidentiality, the sender generates a secret key that is used for a particular session the recipient will use the same key to decrypt the message(Bauer 55). On the other hand, hash functions ensure data integrity due to the fact that any change can result in the recipient calculating a wrong hash value different from the one embedded in the transmission by the sender. There is no possibility of two different messages yielding the same hash value, therefore, data integrity is guaranteed (Gary 15). Finally, asymmetrical key cryptography fosters non-repudiation and user authentication, it could also be used in the encryption of messages just as the symmetrical key cryptography ,but the latter is faster than asymmetrical cryptography(Gary 15).

REFERENCES

[1]. Bauer, Francis. Decrypted secrets: Methods and maxims of cryptology. New York: Springer, 2002.

[2]. Bellare, Mihir and Phillip Rogaway. Introduction to mordern Cryptography. New York: Cengage Learning, 2005.

[3]. Denning, David. Cryptography and Data security. New York: Addison - Wesley, 2002.

[4]. Gary, Kessler. An overview of Cryptography. New York: Cengage Learning, 2012.

Short Bio Data for the Author

Akshay Kumar Tyagi, PersuingPh.D from Mewar University, Chittorgarh, Rajsthan, INDIA. He has more than fifteen year experience in IT & Academics Worked As HOD IT at Graduate School of Business & Administration, Greater Noida, U.P. Sr.S/W Engineer CCE Punjab Engineering College Chandigarh Punjab, INDIA. The current research area is Cryptography& fuzzy commitment scheme.

