ISSN: 0976-3104
ISSUE: COMPUTER SCIENCE

ARTICLE

NETWORK SECURITY USING LATTICE BASED CRYPTOGRAPHY

Sonal Singhla*, Shailja Yadav, Rohit Tanwar

Department of CSE, Manav Rachna Universitry,Faridabad, INDIA

ABSTRACT

In today's world, due to advancement of internet, our society becomes an information society and today era becomes an information era. Today's technology offered us variety of services with the spread of network, which comes with various threats to our confidential information, databases and website domains from cyber-attacks. So network security has become an issue which requires major attention. Lattice based cryptography has been a very active research area and still work is being done to design various cryptosystems that are efficient, easy to use and provide us with high degree of security This paper is an attempt to explain the network security and challenges and various techniques such as Lattice based cryptography through which network security can be enhanced.

KEY WORDS
Internet, Security, Cryptography, Encryption, Decryption, lattice.

Received: 27 Mar 2019
Accepted: 11 May 2019
Published: 10 June 2019

INTRODUCTION

Gestures and facial expressions can be used to communicate with the computers which require the computer system to understand and analyze the signals to perform a particular movement [1]. Recently the designing of special input devices proved to facilitate the interaction between humans and computers. Gesture recognition has been applied in a large range of application areas such as recognizing sign language, human computer interaction (HCI), robot control, smart surveillance, lie detection, visual environments manipulating, etc. Now a days different techniques and tools have been used for handling gesture recognition that vary between mathematical models like Hidden Markov Model (HMM) and Finite State Machine (FSM) to approaches based on software computing methods such as fuzzy clustering, Genetic Algorithms (GAs) and Artificial Neural Network (ANN). Since human hand is a complex articulated object which is controlled by 35 muscles and requires 27 degrees of freedom to be versatile in all the movements, it is a thrust area of research [2]. In today' digital field implementing gesture recognition system requires different type of devices such as cameras, instrumented gloves and colored markers.

Network is a group of two or more systems linked to each other to share resources such as files and information. A node is a point of connection within a network. It can be a computer or other devices such as scanner, printer, modem, etc. [3]. As the number of internet users is increasing rapidly, network security has become a challenge for network administrators to protect it from intruder's attack. These intruders attempt to obtain, alter or affect the original data at target machine. This results in undesired outputs and behavior. So the importance of network security becomes more significant.

Network security refers to the policies adopted for securing system resources from malicious programmers. All internet users, from an ordinary surfer to large enterprises require network security against the intruders [1]. Cryptography refers to the technique used to secure communication in the presence of third party using a public key i.e. hiding information by converting it into mystery code or cipher text. It is the branch of both mathematics and computer science. It includes encryption and decryption processes [4]. It is important to understand and learn the concept of network security for the following reasons. Following are the goals of network security [4].

- It maintains the privacy of an individual by denying the unauthorized access.
- It maintains the integrity i.e. assuring the consistency in data worldwide.
- It gives high availability.

CLASSIFICATION OF ATTACKS

Unethical practices in the field of IT have resulted into many problematic areas we need to tackle, such as different forms of attacks through which the intruder tries to affect the target machine.

We can classify the attacks as [1]-

Passive attacks

In this kind of attack, the attackers try to fetch the user's personal information without his permission. These are further of two types-

***Corresponding Author**
Email:
sonalsinghal1010@gmail.com

IIOAB JOURNAL
ISSN: 0976-3104

Traffic analysis

In this method, without the consent of the sender and the user, the third party (stalker) can view the hided information.

Release of message content

It is an easy approach to fetch the sender's and receiver's information.

Active attacks

It affects the system resources by altering the original data. It is classified as-

Modification of messages

Some messages are altered in order to produce an unauthorized effect.

Denial of services (DoS)

These services are a menace to the society as they require only some fundamental knowledge.

Distributed denial of services (DDoS)

Multiple affected systems are used to damage a single system.

Relay attack

In this kind of attack, intruder fetches the user's information such as credit card details via fake calls or doing some tricks.

Masquerade attack

The attacker gets the user's information such as login id and password by acting as some authorized party and then uses that information against them.

Insider attack

In such kind of attacks, an insider i.e. someone who belongs to authorized party invades the system resources in malicious ways and then damage the data on target machine.

Close-in attack

By applying some tricks, the hackers attack the target and fetch the information.

Phishing

The malicious hackers obtain the confidential information by fake calls or duplicate websites or mails pretending to be an authorized person.

Exploit attack

Intruders take the advantage of the system vulnerabilities.

Password attack

Intruders try to fetch user's password and get the confidential information.

Appearance based approaches

In this type of approach, visual appearance of input hand image is modelled using the feature extracted from stored image. Appearance based approaches are simpler and easier than 3D model based approaches due to the easier extraction of features in a 2D image. The common method used in this approach is to detect the skin colored regions in the image; however this method is affected by changing illumination conditions and other background objects with skin like color.

NETWORK SECURITY THREATS

These threats are increasing day-by-day rapidly and so the concern for this issue is increasing. Network security threats are classified into four categories as shown in [Fig. 1].

ISSN: 0976-3104

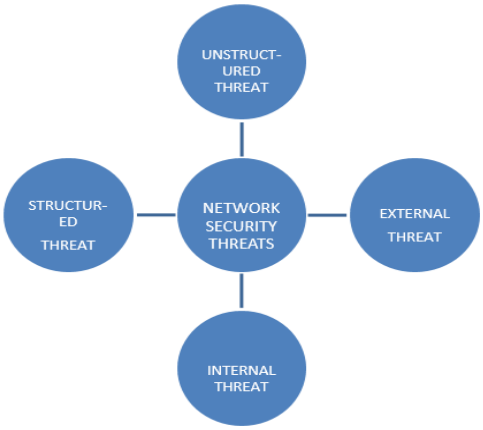

Fig. 1: Network Security Threats.

Unstructured threat

Unskilled individuals try to attack the target machine using some hacking tools in leisure time to do something challenging.

Structured threat

Malicious hackers who are technically skilled and are masters in this field generally hired by industries and organizations.

External threat

Threats from outsiders who do not belong to organization and attacks and steal the original data at target machine.

Internal threat

Threats from insiders who basically belong to the organization and still try to manipulate the original data by creating false streams resulting in false output.

TYPES OF NETWORK SECURITY

Network security threats can be classified in the following form as discussed in the [Fig. 2].

IMPLEMENTATION TOOLS

A lot of implementation, hardware and software tools have been used for recognizing gestures depending on the application fields they are used.

TEXANOMY

The taxonomy of the system can be analyzed using three factors: of the hand gesture application areas are mentioned below-

Encryption

It is a method of converting simple information (called plain text) into unintelligent (called cipher text).

Decryption

It is the reverse of the encryption which means cipher text into ordinary one.

Cryptosystem

It is a method of converting simple information (called plain text) into unintelligent (called cipher text). It is an organized list of attributes which contain all the finite possible planed and cypher texts. It also includes encryption and decryption algorithms [4].

IIOAB JOURNAL
ISSN: 0976-3104

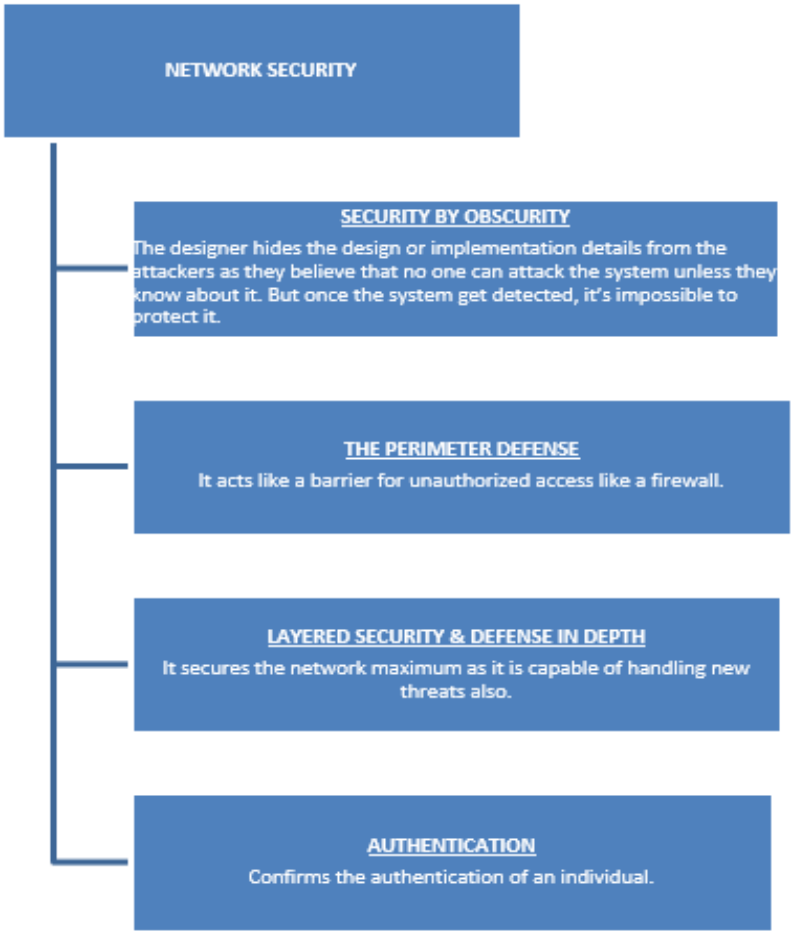

Fig. 2: Types of Network Security

SECURITY TECHNIQUES

The taxonomy of the system can be analyzed using three factors: of the hand gesture application areas are mentioned below- With the increase in internet users and technology, network security is more concerned. To enhance the network security, following techniques are used [3].

Hashing

A hash value is a number generated by a string of a text, also known as a message digest. The length of the hash value is generally less than the length of the input message. And it is practically impossible to create a duplicate text of the same hash value.

Symmetric key cryptography

It is also known as secret key cryptography. It uses the concept of a single key for both processes, i.e. encryption for plain text and decryption of unintelligible text.

Diffie-hellman key exchange (DH)

This technique was launched by Diffie and Martin Hellman in 1976. It allows the two parties to secretly create a secret key which can be used to communicate over insecure channel. Problem associated with it was that it was not practically possible.

Public key cryptography

It is a technique which includes two keys- public key and private key. The public key is known by both the parties while the private key is only recognized by the recipient. Public keys are used for the encryption of the information, and it can be decrypted only with the private key. But practically it was difficult to make the two keys to work simultaneously.

IIOAB JOURNAL
ISSN: 0976-3104

Elliptical curve cryptography

It uses smaller Abelian (finite) group i.e. subset of a lattice but its operations were costly.

Lattice based cryptography

It is widely used and details about this technique are discussed in brief.

LATTICE BASED CRYPTOGRAPHY

History of Lattice Based Cryptography [5-9]- In 1982, first time lattice was used in cryptanalysis. In 1995, Ajtai & Dwork described lattice based cryptography theoretically but they were unable to explain it practically. In 1996, Goldreich, Goldwasser & Halevi (GGH) introduced crypto schemes based on hard lattices, but it requires megabyte size public keys to secure the system. Later on smaller keys were used which helps in faster encryption. In 2009, encryption techniques based on lattices.

Lattice is a fundamental algebraic structure which consists of regular array of points in space. Lattice based cryptography is an efficient and easy implementation. It is the best way to secure quantum computers i.e.it provides security proofs based on worst conditions. When we talk about, lattice based cryptographic constructions, in terms of security; we divide it into two types.

- The first type focus on its practical aspects, but often lack security.
- The second type ensures a great proof of security, but only few are efficient and easy to use for practice.

A lattice is a discrete subgroup of R^n, or the set L (b_1, b_2... b_d) of all linear combinations $\sum x_i b_i$ where $x_i \in Z$, and the b_i's are linearly independent [5]. Now, if we talk about lattice crypto, it uses finite Abelian group. The Gaussian Heuristic theorem says that for full rank lattices L and uncountable sets C we have:

$$C \text{ and } (LC) = vol(C)/vol(L) \quad (1)$$

It basically measures the density of lattice. Hermite's Constant (1850): It is considered to be the worst case for short lattice vectors. From the last 20-25 years, lattices tend to be very trendy in case of complexity. It can be either classical or quantum.

Lattice based cryptography is highly in use in network security because of its primitives that are associated with problems such as CVP (closest vector problem) and SVP (shortest vector problem). In CVP, challenge is to find a closest point P. But it is difficult to find solution in higher dimension such as 500 [5]. In Lattice based cryptography, we come across various problems based on the presumed hardness. If we talk about SVP, there is no specifically an efficient algorithm to approximate SVP [6].

Let us suppose g=n^c in the worst case where, (n is the dimension of the lattice and c is the arbitrary constant independent of n), one can build knapsack-like cryptographic (one-way) functions that are almost certainly hard to break (when the key is chosen at random). Quantum computers can't even solve these problems [6].

Now, we will talk about its advantages like how it helps us other than lattice.

- More efficiency,
- It has security properties based on worst case assumptions e.g. quantum computers.
- Easy to design
- It has cheaper operations

CONCLUSION

As the internet is expanding with tremendous speed, the concern for security has been increased. It became the most attractive hunting ground for malicious hackers. These threats and outdated policies are one of the issues for major concern. And the hackers are finding more and more ways to penetrate the system resources and doing the malicious activities. So, in present scenario, there is a need for regular testing for network security [10]. Lattice based cryptography has been a very active research area and still work is being done to design various cryptosystems that are efficient, easy to use and provide us with high degree of security.

CONFLICT OF INTEREST
None

ACKNOWLEDGEMENTS
We would like to express our sincere gratitude to Accendere Knowledge Management Services., for providing us platform and opportunity to pursue the research.

ISSN: 0976-3104

FINANCIAL DISCLOSURE
None.

REFERENCES

[1] Sumathi R, Sundarraja R. [2008] An Efficient Operator based Unicode cryptography Algorithm for Text, Audio and Video Files, 7(2): 1-14.
[2] Muley MN. [2015] Analysis for Exploring the Scope of Network Security Techniques in Different Era: A Study, IJACEN, 3(12): 33-36.
[3] Singh H. [2016] Network Security, a Challenge, IJARCCE, 5(3): 57-61.
[4] Kumar SN. [2014] Technique for security of multimedia using neutral network, Paper id- IJRETM-2014-02-05-020, IJRETM. 02(05):1-7.
[5] Peikert C. [2016] A Decade of Lattice Cryptography. Foundation and trends in Theoretical Computer Science, 10(4): 283-424.
[6] Micciancio D. [2003] Lattice Based Cryptography, Springer, 10(3): 147-191.
[7] Gama N, Nguyen PQ. [2008] Predicting lattice reduction. In Advances in Cryptology – Proc.Eurocrypt '08, Lecture Notes in Computer Science, Springer, 1-21.
[8] Silva R, Antonio C, de A, Campello JR, Dahab R. [2011] LWE-based identification schemes. In Information Theory Workshop (ITW). IEEE, 292–296. doi: 10.1109/ITW.2011.6089439
[9] Yao Y, et al. [2011] a Sub-0.5V Lattice-Based Public-Key Encryption Scheme for RFID Platforms in 130nm CMOS: 2-19. doi: 10.3233/978-1-60750-722-2-96.
[10] Lyubashevsky V. [2008] Lattice-Based Identification Schemes Secure Under Active Attacks. In Ronald Cramer, editor, Public Key Cryptography – PKC, number 4939 in Lecture Notes in Computer Science, Springer, 162–179. doi: 10.1007/978-3-540-78440-1_10.