[[1]](#footnote-1)

CRYPTOGRAPHY IN NETWORKING AND NETWORK SECURITY

First A. Author, *Fellow, IEEE*, Second B. Author, and Third C. Author, Jr., *Member, IEEE*

***Abstract*—** **Due to the emergence of the Internet and the expansion of e-commerce platforms and social media platforms,**

***Index Terms*— encryption, decryption, cryptography, network security**

# I. INTRODUCTION

A

s the Internet is becoming more widely used, an unauthorized individual who gains access to it may not only spy on us but also quickly disrupt our life. A idea High security is supported by the Model for Cryptosystem Using Neural Network [1]. Towards the field of internet

The following sections make up this paper: The second section discusses the many sorts of cloud security assaults. Security services are discussed in Section 3. The network security paradigm is explained in Section 4. The different cryptographic mechanisms are described in Section 5. Section 6 carries the paper to the end and indicates regions for additional exploration.

# II. Types of Security Attacks

## Passive Attacks

Observation or surveillance of communication are examples:

1. **Traffic Analysis:** The communication flow seems to be.
2. **Release of Message Contents:** Deliver the data through the source to the recipient.

## Active Attacks

An effective assault attempts to modify the organization's:

1. **Message Modifications:** A legitimate communication.
2. **Denial of Service:** All communications intended to a.
3. **Replay:** It comprises silently collecting and resending.
4. **Masquerade:** It occurs when one entity assumes the.

# III. Security Services

This is a service provided through a network level of.

## Data Integrity

This could be extended to a flow of information, a particular.

## Data Confidentiality

Maintaining permissible restrictions on information.

## Authenticity

Offer authentication to ground locations and all edges in.

# IV. Model of Network Security

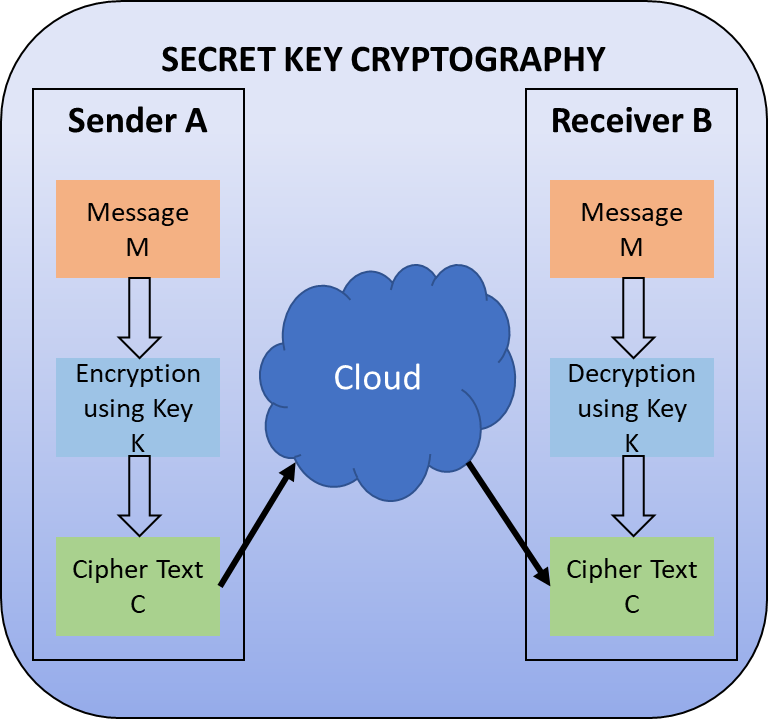
Whenever a message is to be conveyed via the Online:

* On the information to be transferred, a safety associated.
* A secret key that is utilized in coordination with the.

## Key Management Need in Cloud

Encryption provides data protection while key management.

* **Secure key stores:** Malicious users must be prevented.
* **Key stores access:** Accessibility to key storage must.

**Fig 1**. Secret Key Cryptography

# V. Cryptography Mechanism

Cryptography is a method of preserving and transmitting.

1. *Secret Key Cryptography*

In symmetric key encryption, a same key is utilised both:

1. The secret key is utilized to secure the plaintext unit.
2. The **CBC (Cipher Block Chaining)** mode augments.
3. **Cipher Feedback (CFB)** mode is a self-synchronizing.

The following are examples of secret key cryptography algorithms that are currently in use:

* **DES (Data Encryption Standard):** DES is an.
* **AES (Advanced Encryption Standard):** Block.
* **Blowfish:** Designed by Bruce Schneier [2], a.
* **Twofish:** [3] A 128-bit block cypher with keys of

TABLE I

PKI Applications

|  |  |  |  |
| --- | --- | --- | --- |
| **Algorithm** | **Key Exchange** | **Digital Signature** | **Encryption/ Decryption** |
| **DSS** | Close outline | Checkmark outline | Close outline |
| **Elliptic Curve** | Checkmark outline | Checkmark outline | Checkmark outline |
| **Diffie-Hellman** | Checkmark outline | Close outline | Close outline |
| **RSA** | Checkmark outline | Checkmark outline | Checkmark outline |

**Fig 2:** Public Key Cryptography

1. *Public-Key Cryptography*

Encryption and decryption are performed by utilizing two:

1. **RSA**

The earliest and largest frequently utilized variant of.

1. **DH (Diffie-Hellman) Key Exchange**

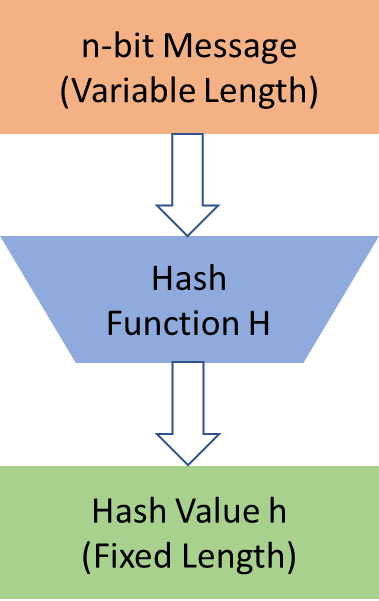
DH key transfer has been a basic public-key algorithm.

1. **Elliptic Curve Cryptography (ECC)**

It's similar to the Key Exchange protocol using DH.

1. **Digital Signature Standard (DSS)**

The secure hash algorithm is used in the DSS, which is.



**Fig 3:** Block Diagram of Hash Function

1. *Hash Functions*

Hashing algorithms, sometimes referred to as one way.

# VI. Conclusion

Because of the Internet's fast expansion, security of.

# References

|  |  |
| --- | --- |
| [1] | S. N. Kumar, "Technique for Security of Multimedia using Neural Network," *Paper id-IJRETM-2014-02-05-020, IJRETM,* vol. 02, no. 05, pp. 1-7, 2014. |
| [2] | B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," in *Fast Software Encryption, Cambridge Security Workshop Proceedings*, 1993. |
| [3] | B. Schneier, "Twofish Cryptanalysis Rumors," *Schneier on Security,* 2005. |
| [4] | A. Simmonds, P. Sandilands and L. v. Ekert, "An Ontology for Network Security Attacks," in *Asian applied computing conference*, Springer, 2004, p. 317–323. |
| [5] | A. Menezes, P. V. Oorschot and S. Vanstone, Handbook of applied cryptography, CRC press, 2018. |
| [6] | R. Davis, "The data encryption standard in perspective," *IEEE Communications Society Magazine,* vol. 16, no. 6, pp. 5-9, 1978. |
| [7] | N. S. P. 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, 2004. |
| [8] | J. Daemen and V. Rijmen, "The Advanced Encryption Standard Process," in *The Design of Rijndael*, Springer, 2002, pp. 1-8. |
| [9] | M. Matsui and T. Tokita, "MISTY , KASUMI and Camellia Cipher Algorithm Development," *Mitsibishi Electric Advance (Mitsibishi Electric corp.),* 2002. |
| [10] | "General Report on the Design, Speification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms," *3GPP,* 2009. |
| [11] | O. Dunkelman, N. Keller and A. Shamir, "A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony," *Journal of Cryptology,* vol. 27, p. 824–849, 2014. |
| [12] | R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communication of the ACM,* vol. 21, no. 2, 1978. |
| [13] | W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory,* vol. 22, no. 6, pp. 644-654, 1976. |
| [14] | N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation,* vol. 48, no. 177, pp. 203-209, 1987. |
| [15] | F. 180, "Secure Hash Standard, Federal Information Processing Standard (FIPS), Publication 180," *NIST, U.S. Dept. of Commerce,* 1993. |
| [16] | M. Lamberger, F. Mendel, C. Rechberger, V. Rijmen and M. Schläffer, "Rebound Distinguishers: Results on the Full Whirlpool Compression Function," *Advances in Cryptology – ASIACRYPT,* 2009. |

1. [↑](#footnote-ref-1)