IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Key Management Framework for Data Centric Networking

Mr. G. R. Deshpande[1], Mr. Pavan Bidwai[2], Miss. Jayshri Bhise[3], Miss. Swati Bhaye[4], Mr. Chaitanya Taware[5].
Assistant professor [1], Student[1], Student[2], Student[3], Student[4].
Computer Engineering
Gramin Technical And Management Campus, Nanded, India.

Abstract:
The framework utilizes public key cryptography to provide required security services to enable exchange of keying material, and information about security policy and cipher suites. As the internet has evolved from host-to-host communication to content distribution, data centric networking is poised to improve networking efficiency. As cloud computing the internet of thing, The fifth generation networking become popular, there is that data is to be distributed or some potentially untrusted middle boxes.

I. KEYWORDS

Encoding-Decoding, Message Privacy, Analysis.

II. INTRODUCTION

Increasingly more traffic on the internet requires fast, scalable, and efficient data delivery. One of the possible solutions is to deliver data not form a data origin but from a closer client. Data center networking is the integration of constellation of networking resources. To faciliate the storage and processing of applications and data.

III. CLIENT-SERVER

In the information technology, client-server is a system architecture model consisting of two parts, client systems, and server systems, both communicating over a computer network. A client-server application is a category of a distributed system made up of both client and server software. The client server application provides an enhanced way to share the workload.

IV. PUBLIC KEY

A public key is a large numerical value that is used to encrypt data. The key can be generated by a software program, but more often , it is provided by a trusted , designed authority and made available to everyone through publicity accessible repository or directory. In public key cryptography, every public key matches to only one private key together they are used due to encrypt and decrypt message .If you encode and a message using a person’s public key they can only decode it using their matching private key. The public key is made available through the public accessible directory. Example; A encrypts sensitive information using B’s public key and send it across. B can only access that information and decrypt it using there corresponding private key. In a digital signature system, a sender can use a private key together with a message to create a signature. Anyone with the corresponding public key can verify whether the signature matches the message, but a forger who does not know the private key cannot find any message/signature pair that will pass verification with the public key.

V. SYMMETRIC KEY

In cryptography, a symmetric key is one that is used both to encrypt and decrypt information. This means that to decrypt information, one must have the same key that was used to encrypt it. The keys, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. Symmetric-key cryptography is called a shared-key, secret-key, single-key, one-key and eventually private-key cryptography. With this form of cryptography, it is clear that the key should be known to both the sender and the receiver that the shared. The complexity with this approach is the distribution of the key. Symmetric key cryptography schemes are usually categorized such as stream ciphers or block ciphers. Stream ciphers work on a single bit (byte or computer word) at a time and execute some form of feedback structure so that the key is repeatedly changing. A block cipher is so-called because the scheme encrypts one block of information at a time utilizing the same key on each block. In general, the same plaintext block will continually encrypt to the same cipher text when using the similar key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher. The database master key is a symmetric key that is used to protect the private keys of certificates and asymmetric keys that are present in the database. It can also be used to encrypt data, but it has length limitations that make it less practical for data than using an asymmetric key. To enable the automatic decryption of the database master key, a copy of the key is encrypted by using the SMK. It is stored in both the database where it is used and in the master system database.

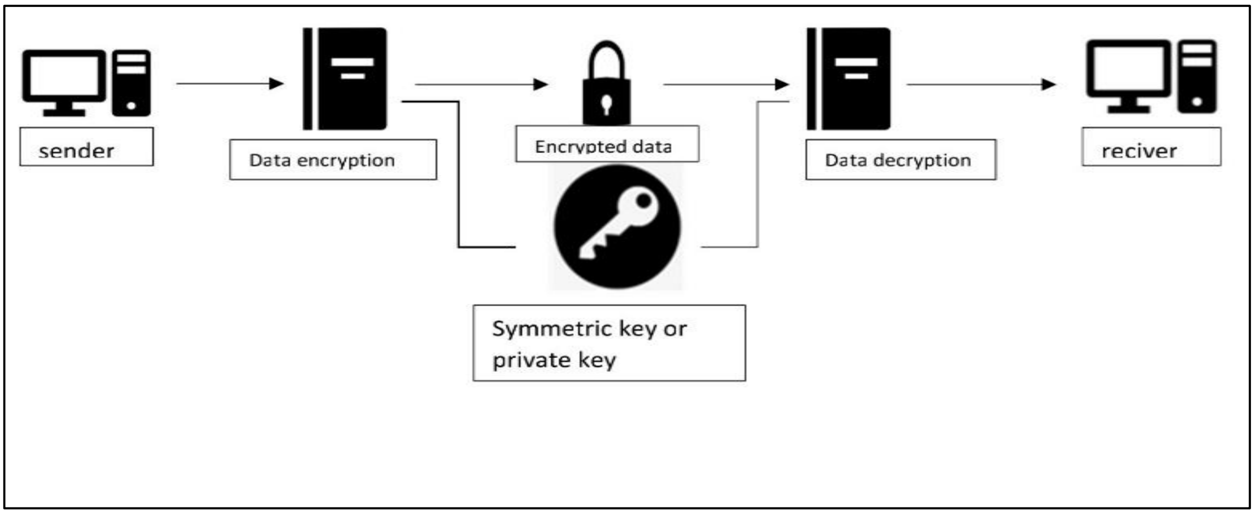

Fig 1 : Symmetric Key Or Private key

VI. ASYMMETRIC KEY

Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys one public key and one private key to encrypt and decrypt a message and protect it from unauthorized access or use. When someone wants to send an encrypted message, they can pull the intended recipient's public key from a public directory. Use it to encrypt the message before sending it. The recipient of the message using their related private key. The encryption process is also used in software connection over an insecure network, such as browsers over the internet, or that need to validate a digital signature. Asymmetric encryption is used in key exchange, email security, Web security, and other encryption systems that require key exchange over the public network. Two keys (public and private), private key cannot be derived for the public, so the public key can be freely distributed without confidentially being compromised.

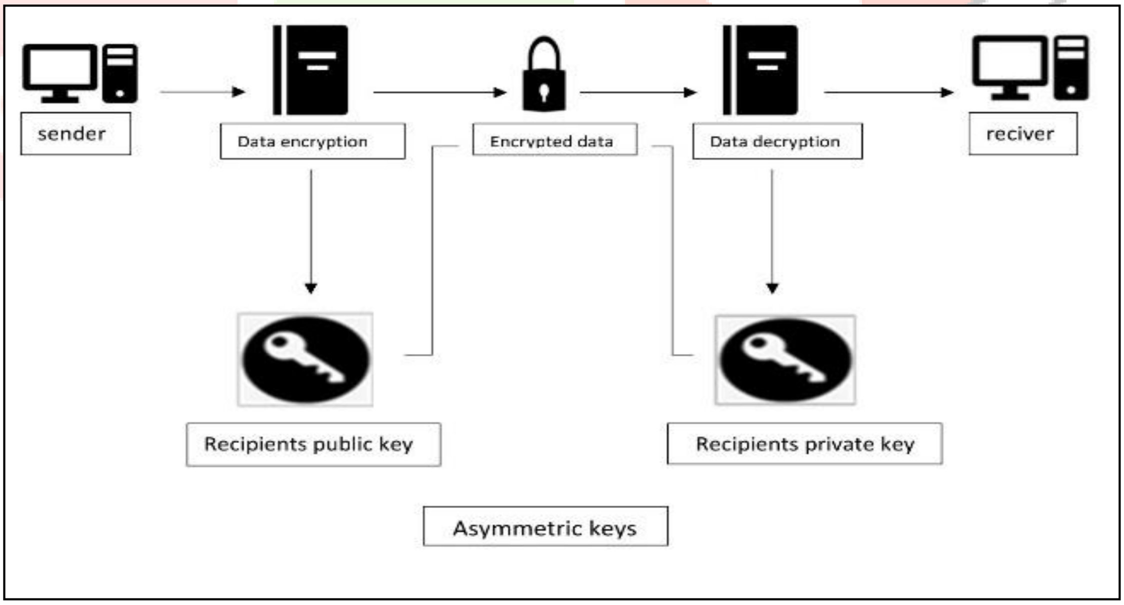

Fig 2 : Asymmetric Key

VII. JDBC

JDBC is the Java API which is used for database connectivity. The JDBC API consists of a set of interfaces and classes written in the Java programming language. This API allows Java programs to access database management system. It is part of the Java Standard Edition platform, from Oracle Corporation.

There are four types:-

- JDBC-ODBC Bridge Driver,
- Native Driver,
- Network Protocol Driver,
- Thin Driver.

VIII. EXPERIMENT

we need total 3 system two client one server. There are two clients. one A and another B and third server client A saved XYZ file in server and want to access that file but client B need some specific key which set by client A to access this file. The file saved by client A protected in the server with the help of using encryption and decryption technology and that's why client B need that key. When client A send that key to client B, then client B can access that file with the help of key to open that file or folder.

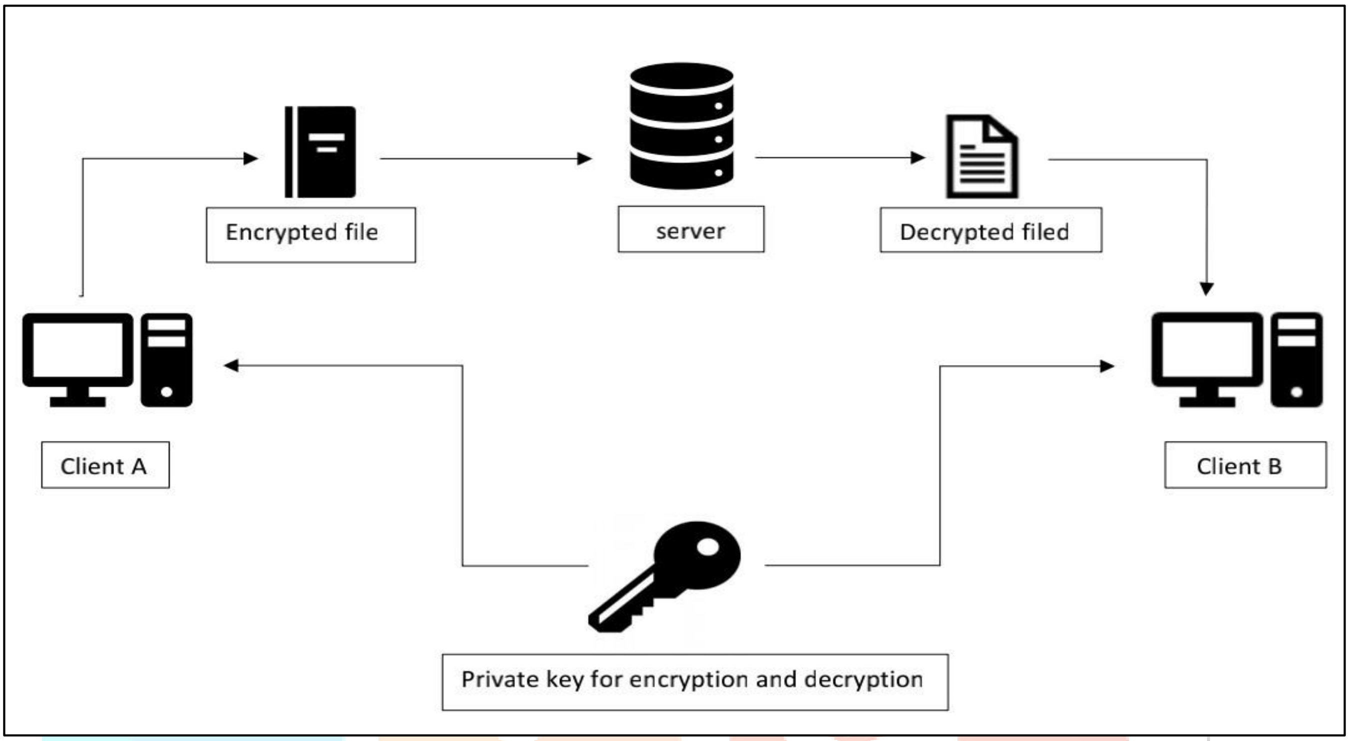

Fig 3 : Experimental diagram.

IX. CONCLUSION

The above paper is regarding text and message privacy providing user a secure platform to communicate and share data via particular network. it uses Key concepts and that is explained.

X. REFERENCES

1. R. Shirey (August 2007). Internet Security Glossary, Version
2. Network Working Group. doi:10.17487/RFC4949. RFC 4949. Informational.
3. Kartit, Zaid (February 2016). "Applying Encryption Algorithms for Data Security in Cloud Storage, Kartit, et al". Advances in Ubiquitous Networking: Proceedings of UNet15: 147. ISBN 9789812879905.
4. Delfs, Hans; Knebl, Helmut (2007). "Symmetric-key encryption". Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436.
5. Hirsch, Frederick J. "SSL/TLS Strong Encryption: An Introduction". Apache HTTP Server. Retrieved 17 April 2013.. The first two sections contain a very good introduction to public-key cryptography.
6. Christof Paar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online cryptography course that covers public-key cryptography), Springer, 2009.
7. Wikipedia. (2018). Client-Server [Online]. Available: https://simple.wikipedia.org/wiki/Client-server.
8. https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/sql-server-and-database-encryption-keys-database-engine?view=sql-server-ver16 (5).
9. Bernstein, Daniel J. (1 May 2008). "Protecting communications against forgery". Algorithmic Number Theory (PDF). Vol. 44. MSRI Publications. §5: Public-key signatures, pp. 543-545. Retrieved 8 October 2022.