



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: VII Month of publication: July 2022

DOI: <https://doi.org/10.22214/ijraset.2022.45926>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

²Assistant Professor, *Information Science and EngineeringRV College of Engineering Bengaluru, India*

4080

II. AES AND ITS USAGE

A. Comparison of AES with Other Algorithms

Due to the small key size in DES and 3DES (Triple DES), it was soon breakable and insecure. AES was used as an alternative in place of DES and 3DES that offers better security and larger key sizes. AES comes with key sizes 128-bit, 192-bit and 256-bit with 10, 12, 14 rounds performed during the encryption process respectively with the AES256-bit version being the most secure. AES being a symmetric key encryption algorithm provides stronger encryption than asymmetric encryptions when per bit key length is taken into consideration. One major disadvantage of AES over asymmetric encryption algorithms like RSA or ECC which uses a pair of public and private keys, is that if the key is known, it can be decrypted as the same key is used for encryption and decryption.

B. Comparison of AES in Different Modes

Based on the usage, AES algorithm can be implemented in different modes. In cases where plain text patterns must be well hidden or made random, CBC (Cipher Block Chaining) mode of the AES can be used. In this mode, the entire plain text is broken into blocks which are encrypted sequentially. While encrypting, an initialization vector, which chooses a unique value of fixed length is XORed with the first block and the output of this operation is XORed with the next block. The output of the first and second block is then XORed with the next block and so on, until all the blocks are encrypted. Due to the XOR operation at each step, the output will be such that even though they can have the same plain text as input, the encrypted text will never be the same. This way, a pattern does not exist and makes decryption harder. Another mode for AES which is better than AES-CBC is the AES-GCM (Galois Counter Mode). In cases where high speed outputs are needed with low latency and low cost, this mode is preferred. In this mode, each block can be independently encrypted, unlike CBC that depends on a sequence and if the sequence is altered during decryption, the plain text can be lost. From a computational point of view, AES-GCM is preferred in 128-bit key length. This is faster and more secure compared to a bigger key size AES-CBC that needs a minimum 256-bit key length to be secure.

III. SECURING THE NETWORK

A. Need for Network security and protocols

To safeguard sensitive data in the network, data must be safely stored and transported from one place to another in a network. This helps to prevent data theft, tampering, damage, and unauthorized access of data by third parties. There are sets of rules defined to carry out the procedure of transferring data safely through a network during the process of communication. These are the network protocols. Some network protocols used are TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol), SMTP (Simple Mail Transfer Protocol) etc.

B. Three-way Handshake for HTTPS

One of the most used protocols for secure encrypted internet communications is the TLS (Transport Layer Security) protocol. This is the successor of SSL (Secure Socket Layer), which uses encryption to secure the communication. TLS is faster and more secure when compared to the SSL. TLS makes use of certificates to protect information when transferring between two ends (end user and a website) and helps authenticate a website's identity for the end user to know that they are using legitimate websites. HTTPS is the combination of HTTP (HyperText Transfer Protocol) and the TLS.

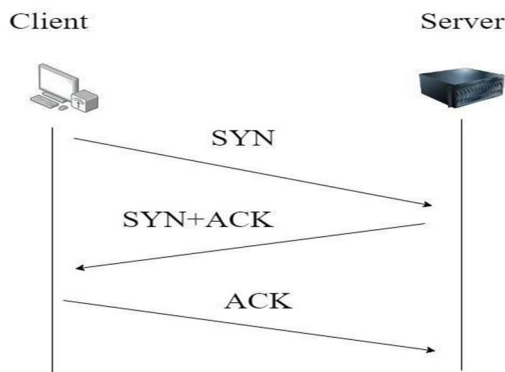


Fig 2: Three-way handshake to establish HTTPS connection

Fig 2 shown above shows the three-way handshake. The client sends a SYN packet to the server and the server replies with an acknowledgement (ACK) and sends a SYN to the client, which then replies with an ACK. If this handshake is successful and the sent SYN packet is replied with an ACK from both ends, a secured HTTP connection is established along with TLS (the handshake) between two entities in a network. This ensures trusted connection between the entities on the network to have confidential communication.

C. Concept of Hashing

Hashing is a process for converting a given input string into another format of fixed length. This process is done with the help of a hash function. Unlike encryption, hashing is a one-way process where once the string is hashed, it is irreversible. The concept of hashing can be used to store data securely and later used to validate the input data by comparing it with the hash value. It can not only help to search for data faster but also check whether the content is altered or not by a virus or an intruder. This concept can be used in networking to check if the data is tampered or not by comparing it with the stored hash values.

IV. DIGITAL CERTIFICATES AND SIGNING PROCESS.

A. Origin and use of Digital Certificates

Digital certificates are public key certificates that contain information to identify devices, organization, entity, servers or a website. They contain a public key which is cryptographically linked with the owner of the key. It helps bring secure and trusted connections between devices in a network for the devices to communicate in a confidential manner. This works with the help of PKI (Public Key Infrastructure), which is a framework that allows servers and users to securely communicate and exchange sensitive information. PKI consists of components like CA (Certification Authority), RA (Registration Authority) and certificates. CA is responsible for signing and distributing certificates to clients or entities under the assurance of RA. RA ensures that the client requesting for certificate is authentic and is delegated by a CA. This way, the certificate received by CA is then used as an authentication process between two entities in a network to exchange information.

B. Process of Signing with Encryption

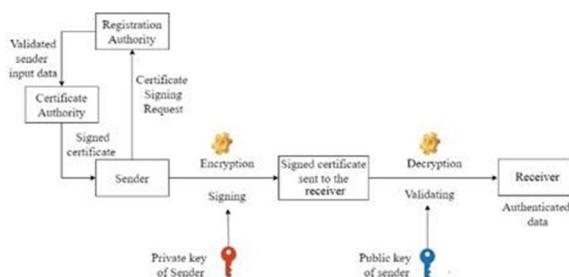


Fig 3: Process of Signing

First, an entity or a server sends a CSR (Certificate Signing Request) to a CA (Certification Authority) for obtaining a signed certificate. There are many CAs, and the entity may choose the CA of their choice. Once the CA server receives a request, the CA will delegate an RA to process the request by validating and authenticating the data provided by the entity. Once validated, the certificate is then signed using the CAs private key (not shared to the entity or elsewhere) and the certificate containing the public key and sensitive data is shared to the receiver (from the sender), who then uses the sender's public key to verify the package is valid or not. This can be used to validate sensitive data as well as the sender and ensure secure transfer of sensitive data from sender to receiver on the network. The most used certificate is the X.509.

V. CONCLUSION

With large amounts of sensitive data generated day-to-day, there is a need to securely store and transport them. This is made possible with the help of cryptography that provides keys and algorithms for securing the data. AES is one of the most robust and secure algorithms that has not been broken down yet and is used in many instances where securing sensitive data is of utmost importance. Network protocols like TCP/IP, UDP and HTTPS are used to have a standardized and secure way of transporting data safely from the sender to the receiver over an unsecure network environment. Digital certificates and the Public Key Infrastructure framework bring about another step for authenticating and validating the sender thereby making data transfer more secure and tamper proof.



REFERENCES

- [1] V. Esther Jyothi, Dr. BDCN Prasad, Dr. Ramesh Kumar Mojjada, "Analysis of Cryptography Encryption for Network Security", IOP Conference Series: Materials Science and Engineering, DOI:10.1088/1757-899X/981/2/022028, 2020.
- [2] Mariam O. Alrashidi, Maher Khemakhem, "A Framework and Cryptography Algorithm for Protecting Sensitive Data on Cloud Service Providers", Computing and Information Technology Sciences 8(2):69-92, 2019.
- [3] Santhosh Kumar R, Shashidhar R, "Design of High Speed AES System for Efficient Data Encryption and Decryption System", The IEEE Seminar on Quantum Cryptography: Secure Communications for Business (Ref. No. 2005/11310), 2019.
- [4] Hamid Nejatollahi, Nikil Dutt, Rosario Cammarota, "Trends, Challenges and Needs for Cryptography Implementations", International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), 2019.
- [5] Ye Yuan, Yijun Yang, Liji Wu, Xiangmin Zhang, "A High Performance Encryption System Based on AES Algorithm", IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC), 2018.
- [6] E. Thambiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques" International Journal of Advanced Research in Computer Science and Software Engineering, VOL. 2, Issue 7 July 2018, Page 226-233.
- [7] F. Mallouli, A. Hellal, N. Sharief Saeed and F. Abdulraheem Alzahrani, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud), Paris, France, pp. 173-176, 2017.
- [8] Dr. Sandeep Tayal et al., "A Review paper on Network Security and Cryptography", Advances in Computational Sciences and Technology, Volume 10, Number 5 (2017) pp. 763-770.
- [9] Mohit, "Performance Evaluation of Cryptographic Algorithms", International Journal of Computer Applications, Vol. 41, No. 7, 2017.
- [10] Abhishek et. al "Cryptography in Network Security", International Journal of Engineering and Technology, Volume 07 Issue: 04, Apr 2017.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)