Hybrid Cryptography Using A Super Server For Encryption And Decryption

Aparna.M

VIT University, Chennai

DOI: 10.29322/IJSRP.9.12.2019.p96102
http://dx.doi.org/10.29322/IJSRP.9.12.2019.p96102

Abstract- The world of encryption is evolving every year. Hybrid encryption is a unique technique which combines both symmetric and asymmetric encryptions. This research study focuses on using a super server to create unique private keys which is in turn used for encryption and decryption of data. It is an efficient and modified technique which makes use of 'Hybrid Cryptography'. In this technique of hybrid cryptosystem, a public-key cryptosystem (asymmetric cryptosystem) with a highly efficient symmetric key is used. The technique of using a super server provides secured data encryption which ensures user's privacy, authentication and usability. Three different algorithms are being used for the encryption and decryption processes. Here, the super server works as an intermediate generating duplicate private keys which the client makes use of for the decryption of data. This technique provides increased security as well as authentication compared to other existing hybrid algorithm and the speed is also doubled as the technique makes use of two private keys and the generation of duplicate private keys ensures that the data is less prone to hacking.

Index Terms- Symmetric Keys, Asymmetric Keys, Hybrid Cryptography, Encryption, Decryption, Cipher text, Hacking

I. INTRODUCTION

Data security has become the need of the hour in the digital world we live in. In the past decade with the phenomenal growth in Science and technology, the hacking crime rates have also accelerated at an alarming rate. Internet on a larger scale has curbed the right to privacy of data of thousands of users throughout the world. In every field we step in, today almost all the web traffic is encrypted. This is advantageous for businesses and common man, since it shields against pirating content during the data transfer from the server to the client and back again to the server. Major existing threat in cryptography is hacking. Hackers also use encryption for their attacks and it becomes difficult to spot the hackers in the encrypted traffic.

However, with the advent of new techniques in cryptography the crime rates have reduced as the human race came out with the concept of Hybrid Cryptography which allows the users to transfer data in a secured way and also the process of transferring data periodically occurs at a faster rate. This technique makes use of the combination of symmetric and asymmetric encryption processes. The drawbacks encountered in using the public key encryption which was speed and security is overcome by the technique of Hybrid Encryption. Public key encryption technique makes use of simpler algorithm and uses two different keys hence results in increased processing time and this technique is highly prone to hacking. To overcome these disadvantages, hybrid cryptosystem was introduced. But the loophole in Hybrid Cryptography lies in the fact that, the generation of symmetric keys by the client or the server can easily be introspected as there is no central control and the data can easily be altered and destroyed. Hence a technique which involves a central control like that of the super server is necessary to overcome this and the process of generating duplicate keys by the super server which is used for encryption and decryption ensures the security of data on a larger scale and this technique also results in increased speed.

II. PROPOSED TECHNIQUE

The proposed technique involves a super server placed strategically in geographical locations closer to the maximum user group to avoid delays and this helps in generating new private keys which is used by the clients or the receiver. If there is more than one client then for each client every time during the process a new private key is generated for a specific public key. Consider a scenario in which User A wants to encrypt a message and send to User B, the decryption and encryption process is as follows according to my assumptions:

III. ENCRYPTION

- The sender obtains User A's public key.
- Generates a private key (symmetric key) and sends it to the super server.
- The key sent by the User A is considered as a duplicate private key and the super server generates a new private key.
- The message is also encrypted using the symmetric key generated by the super server.
- The key encapsulation along with data encapsulation is then sent to User B.

IV. DECRYPTION

- User B uses its symmetric key to decrypt the new private key generated by the super server.
- If the private key of User B matches, User B uses the symmetric key generated by the super

server to decrypt the message thus converts the cipher text to plain text.

Hence this technique provides security and is highly reliable as only authenticated user groups can receive and send data. This technique can be adapted in implementing secure processes like **digital transactions, online trading** as the mechanism is advantageous over other techniques like Public key Infrastructure as the speed is also enhanced and the size of the data is not increased as in the case of Public Key Infrastructure. This technique outperforms in **efficiency and security** compared to its predecessors.

V. EXISTING TECHNIQUE AND MOTIVATION FOR THE RESEARCH WORK

With the focus to resolve the speed and security issues in the public key Infrastructure, Hybrid Cryptography was introduced. Hybrid Cryptography makes use of a combination of symmetric and asymmetric cryptography; hence there was an enhancement in speed. In Hybrid Cryptography technique the sender generates a symmetric key during encryption which is later used by the receiver to decrypt the data but the loophole lies in the fact that while the server generates the symmetric key, it is susceptible to hacking as the data can easily be introspected. To solve this security issue was the motivation behind my research work. In the existing technique, User A would obtain the public key of user B, generates the symmetric key and encrypts the data in the form of cipher text. The encapsulated key and data is sent to User B. User B would use its symmetric key to decrypt the newly generated private key using which it decrypts the message. In the recent times, data security has become a serious issue and the proposed technique of using a super server would resolve all the data security issues and is advantageous over other techniques as it involve simple mechanisms and can be widely used for cloud computing security.

VI. SUMMARY

Lack of privacy and data security has been a major cause for several cyber-crimes. The issue brought by **Facebook's Cassandra** has created a sense of fear in the minds of Internet users throughout the world. Cryptography provides several solutions to offer secured data transfer and communication. The proposed technique of using a super server is a modified technique of Hybrid Cryptography which is an optimized and efficient way for quicker and secured communication of data. It also helps to put an end to hacking and data theft across the globe especially in online banking transactions and in data transfer of national affairs.

REFERENCES

[1] https://pdfs.semanticscholar.org/87ff/ea85fbf52e22e4808e1fcc9e40ead4ff7738.pdf
[2] https://en.wikipedia.org/wiki/Hybrid_cryptosystem
[3] https://community.jisc.ac.uk/library/advisory-services/introduction-cryptographic-techniques

AUTHORS

First Author – Aparna.M, VIT University, Chennai