INFORMATICS INSTITUTE OF TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY
In Collaboration with
UNIVERSITY OF WESTMINSTER

Enhancing Security for End Users in Cloud Computing Environment Using Hybrid Encryption Technique.

A Project Proposal by
Mr. Kushanga Sandeepa

Supervised by
Mr. Sithira Hewaarachchi

Submitted in partial fulfillment of the requirements for the MSc in Cyber Security & Forensics at the University of Westminster.

November 2021

Abstract

Encryption provides the ability to secure data transfers with cloud and end-users insecure methods where the data should not be visible to others. So, encryption is playing a major role when it comes to cyber-attacks or data breaches. It is one of the most reliable and important components in untrusted networks such as the internet which helps to effectively reduce the number of real-world issues. Due to the development of technology nowadays, encryptions can be decrypted without any secret key easily by using supercomputers or attacks like brute force, MITM, cipher only, plaintext, etc. Also, single encryption is more vulnerable due to the lack of complexity, and if the secret key gets compromised all the data will be breached.

So, this research is based on looking for a solution to the above problems and to have a proper way to overcome these issues. After conducting surveys and interviews about this topic with the experts of the industry and having a review of previous authors' research this solution was elaborated for users who are accessing cloud computing in untrusted networks to share their sensitive data in a secure way where should cyber attackers fail to breached. So, the proposed concept solution will cover up all the gaps such as in authentication, time-consuming, security issues, etc. which have been identified in the existing encryptions. Also, the combination of symmetric and asymmetric encryptions is the most reliable way of doing hybrid encryptions where most of the existing authors are failing.

The concept is defined to get the overall understanding of the solution by using this hybrid encryption for cloud computing it is having higher security, takes time for encryption and decryption is fewer contrasted to the existing hybrid encryptions, and authentication takes place before sending the ciphertext or cipher key to the end-user, etc. This will be a prototype in future work based on this concept. This concept is mainly engaged with the AES, DES, Twofish, and DSA which are the symmetric and asymmetric combinations of hybrid encryption.

Keywords: Encryption, Hybrid Encryption, Symmetric, Asymmetric, Data Security, Authentication, AES, DES, Twofish, DSA.