ABSTRACT

The cloud computing is growing technology for IT industries. The cloud refers to a network or internet and the cloud computing refers to manipulating, configuring and accessing the software and hardware resources remotely. It provides online data storage, infrastructure and applications. Many companies such as, Amazon, Google, Microsoft are established by cloud computing system and they are enhancing their services, to be provided for a larger number of users. The cloud computing poses some advantages, such as, cost saving, reliability, manageability and strategic edge. The attack detection is used for detecting the attack in cloud computing. It is used to prevent the data and improve the security. The cloud computing is attacked by the attackers, and among those Side Channel Attacks are most harmful. This type of attack is aimed to retrieve the secret data from the cryptographic system. This type of attacks reduces the performance of cloud computing. The attacks occur due to security issues in terms of increasing the memory spaces, high power consumption, and high execution time, reduced browsing security, and increased time complexity and error tolerances. It decreases the performances of cloud computing process. To overcome the security issues, two phases are developed. The first phase developed is AES with Rijndael algorithm and the next phase is effective Enriched AES (E-AES) algorithm.

The security issues are overcome by specialized assault adjacent to the AES and it is developed in the first phase of the work. The AES with Rijndael algorithm is used for detecting the attacks in the encryption and decryption process for security purposes. The Rijndael algorithm is designed with some characteristics such as,
resistance against all known attacks, speed and code compactness on a wide range of platforms and simplicity. The algorithm contains four operation processes, such as sub bytes, mix columns, shift rows and add round key. The advantage of AES is it is easy to implement the software, it is used for lookup table process and it requires minimum space for memory. The main aim of the algorithm is to avoid the Side Channel Attack (SCA) in the data transmission process. The sender sends the data to receiver with encryption process. If the receiver need the data, they require the encryption key for decrypting the data. The AES with Rijndael algorithm is also used in the unknown plain text and cipher text.

To increase the security, modified AES with random S-box generation is proposed in next phase of the work. Data security is critical in the communication system with secure and complex cryptographic algorithms. The secret keys are used in data transmission for security purposes. The effective security is provided by secure Side Channel Attack and the effective Enriched AES (E-AES) algorithm. In this phase, the E-AES algorithm is used for both encryption and decryption processes. This algorithm is used to reduce the Side Channel Attacks. The generation of random multiple S-box is made hard, to break the text that is in the encryption process. The proposed algorithm provides some advantages, such as, reduced time complexity, and error tolerances. It is used in varies key bits, such as, 64 bits, 128 bits, and 256 bits.