Abstract

Cloud computing becomes the next-generation architecture of IT Enterprises. Cloud computing is a technology. It enables clients to use high-end services in a form of software as a service. These reside on different servers all over the world. There are many security threats in cloud computing. Data security is one of them. Data security raises client concerns. There are many issues of data security. It named maintenance of data integrity, data hiding and data safety. These threats dominate clients concerns when the issue of cloud come up. Cloud computing has a big data. Traditional encryption method is time-consuming in this environment. Cloud computing has a single security architecture. It has also many customers with different demands of security. In this case, data security is considered one of the most important issues in cloud computing.

The proposed work focused on accessing data securely in cloud and desktop environment. It depends on public key cryptosystem. Generally, Data security is an important factor for both
Public Encryption Techniques for Cloud Computing: Randomness and Performance Testing

cloud computing and traditional desktop applications. Client needs to have the highest possible level of privacy. Public key cryptosystem is a good candidate for this purpose. It plays a vital role in cloud computing security and desktop. The paper presents an evaluation for selected public key cryptosystem techniques. It named ElGamal cryptosystem, modified chaotic cryptosystem and chaotic cryptosystem. A modified chaotic cryptosystem was presented. The modification enabled the same message to have different cipher version. The experiments implemented at two independent platforms namely desktop computer and Amazon EC2 Micro Instance cloud computing environment.

In this paper, the selected algorithms compared according to randomness testing. A standardized NIST statistical testing is used in both desktop environment and cloud computing environment. The algorithms are implemented using python charm Cryptography framework. Simulation results are shown to demonstrate the effectiveness of each algorithm. NIST statistical tests are used to determine suitable technique for cloud computing environment and desktop. It also used to study the performance of the selected encryption techniques in both environment.

References


Index Terms

Computer Science  Distributed Systems

Keywords

Cloud computing, ElGamal cryptosystem, lattice based cryptosystem, chaotic cryptosystem.