Abstract

Security remains as a big challenge as there are many advancements as well as applications being proposed in the areas wireless adhoc networks and cloud computing. The modern field of cryptography is divided into two main areas based on the basic encryption mechanism as symmetric key cryptography and Public-key cryptography. Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. But in Public-Key method, two different but mathematically related keys are used—a public key and a private key. So comparatively the second method is more popular. Among various techniques in this method Identity-Based encryption scheme, certificateless encryption as well as certificateless signcryption scheme are gaining popular now-a-days. One of the major advantages of any identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. Certificateless encryption is a form of public-key encryption that is designed to eliminate the disadvantages of both traditional PKI-based public-key encryption scheme and identity-based encryption. The securitygoals associated with
signcryption are stronger than those provided by authenticated encryption, where data authenticity suffices and non-repudiation is not required. In this article we present a review on various certificateless encryption schemes proposed for wireless adhoc networks as well as cloud computing. Finally we propose an idea of how to extend identity-based encryption scheme for multi-recipient via randomness-reuse and a hybrid mechanism for providing certificateless encryption. We are also trying to achieve secured certificateless signcryption scheme.

References

A Novel Approach on Certificateless Encryption Schemes


Index Terms

Computer Science Information Sciences

Keywords

Cryptography, symmetric, cipher text, encryption, decryption, certificate, security and adhoc networks.