Elliptic curve cryptography in cloud computing security

Manu Gopinathan (manugopi92@gmail.com)
Øyvind Nygard (oyvind2302@gmail.com)
Kjetil Aune(aune.kjetil@gmail.com)

October 30th, 2015

1 Abstract

Cloud computing is a technological advancement that has been growing swiftly during the last decade. In simple terms, cloud computing is a technology that enables shared, remote, on-demand and ubiquitous access to services through the Internet. It enables consumers to access applications and services that reside on remote servers, without having to allocate large amounts of storage space on their own computer and without the need for extensive compatibility configurations. Many such cloud applications provide services that are meant to handle sensitive user data and thus the protection of this data in terms of access and integrity is of major concern. Space- and time complexity of encryption algorithms can prove to be imperative when it comes to system performance. In this paper we will present the advantages of elliptic curve cryptography (ECC) and how it can be used as an encryption solution to security related issues in cloud computing.

2 References

1. Bai, Rabara, Jerald: "Elliptic Curve Cryptography based Security Framework for Internet of Things and Cloud Computing", 2015. Web: http://www.wseas.us/e-library/conferences/2015/Seoul/ACE/ACE-10.pdf

2. Tirthani, Ganesan: "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography", 2014. Web: https://eprint.iacr.org/2014/049.pdf

3. Knight M: "The Merits of Elliptic Curve Cryptography", 2012. Web: https://www.thales-esecurity.com/blogs/2012/november/the-merits-of-elliptic-curve-cryptography