Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 7, July 2013, pg.327 – 332

RESEARCH ARTICLE

TPM as a Middleware for Enterprise Data Security

Abhishek Patel[1], Prabhat Dansena[2]
[1]M. Tech, CSE, India
[2]School of Computer and Information Sciences, UoH, India

[1] mrabhi.patel@gmail.com; [2] p.dansena23@gmail.com

Abstract— Cloud Computing is one of the emerging technologies in Computer Science. Cloud provides various types of services to us. In the Private Cloud Computing the major concern is to securing data/files and also providing privacy. Storage as a Service is generally seen as a good alternative for a small or mid-sized business that lacks the capital budget and/or technical personnel to implement and maintain their own storage. Currently, the service providers that provides cloud storage, like Dropbox provides security by server-side data encryption. Since all the encryption keys are managed by software, so such method is not secure enough. But the main issue is to maintain CIA (Confidentiality, Integrity and Authentication) to the data stored in the cloud. To achieve these we use Public Key Cryptography. For securing data we use Asymmetric key Encryption Technique. Key rings are provided by the TPM. We describe an architecture which protects enterprise data in cloud and also having authentication based on the signature. We use asymmetric keys for encrypting data. We will use the keys generated by Trusted Platform Module (TPM) for providing better security. Use of TPM is a more secure way to encrypt and decrypt data. So we have implemented a TPM as a middleware which applies the specification of Trusted Computing Group (TCG). TCG is a global industry standard, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. We use TPM to encrypt data before storing it to the cloud. And we use have to use any basic Authentication Service to avoid masquerading, replay attack and eavesdropping to the client side.

Key Terms: - Security; TPM; TCG; Network; Cloud Storage

Full Text: http://www.ijcsmc.com/docs/papers/July2013/V2I7201385.pdf