Chapter 22
A Comprehensive Survey on Techniques Based on TPM for Ensuring the Confidentiality in Cloud Data Centers

Arun Fera M.
Thiagarajar College of Engineering, India

M. Saravanapriya
Thiagarajar College of Engineering, India

J. John Shiny
Thiagarajar College of Engineering, India

ABSTRACT

Cloud computing is one of the most vital technology which becomes part and parcel of corporate life. It is considered to be one of the most emerging technology which serves for various applications. Generally these Cloud computing systems provide a various data storage services which highly reduces the complexity of users. we mainly focus on addressing in providing confidentiality to users' data. We are proposing one mechanism for addressing this issue. Since software level security has vulnerabilities in addressing the solution to our problem we are dealing with providing hardware level of security. We are focusing on Trusted Platform Module (TPM) which is a chip in computer that is used for secure storage that is mainly used to deal with authentication problem. TPM which when used provides a trustworthy environment to the users. A detailed survey on various existing TPM related security and its implementations is carried out in our research work.

INTRODUCTION

Trusted platform module is considered to be the core part of trusted computing group which provides various capabilities of cryptographic possibilities which protects PC from various threats to user's sensitive information. This paper explains about the trusted platform module features which help from preventing various threats.

DOI: 10.4018/978-1-5225-8176-5.ch022

Trusted platform module (TPM) is a microcontroller which stores the passwords, key and digital certificates. It is attached to motherboard which can be used in any devices for security purposes. We can save that TPM provides a secure place for storing all types of sensitive information which provides a secure space for key operations and protect from other security attacks.TPM is attached to motherboard of our PC and that can be used in any computing devices. TPM's overview is given in Figure 1.

SURVEY ON TRUSTED PLATFORM MODULE

A trusted platform module is used for generating secure asymmetric key. Goh W, Yeo CK (2013) describes the use of a secure key generating authority in Shamir identity-based signature scheme implementation. They proposed an idea of identity-based asymmetric cryptosystems (IBC) together with an identity-based asymmetric signature. The proposed IBS scheme in this paper has itself proven secure against forgery under chosen message attacks. This paper also proposed a new concept that assigns TPM as key generating authority and list out the various merits of implementing it.

Abbadi M, Muntaha (2012) lists out the challenges for establishing the trust in the cloud and then proposes a secure framework which helps in addressing the listed challenges. This paper is actually an extension of their previous work. In their previous work, they proposed a unique framework for establishing trust in the cloud environment. By extending their previous work, the current paper addresses those issue; it clearly covers applications data and their integration with infrastructure management data. The proposed framework by Abbadi M, Muntaha (2012) has four types of software agents, each run on trusted devices. The paper also explains about the controlled content sharing between devices.

In Huang et al (2013), security is ensured using C-code-like formal modeling at the application level. As a result of this approach, security of the protocol is ensured not only at the abstract level of protocol l, but also at the concrete level.

Figure 1. Overview of TPM