Data Security in Cloud Computing

T V Sathyanarayana
Lecturer, Nizwa College of Technology
Sultanate of Oman
tv_sathya@yahoo.co.uk

Dr. L. Mary Immaculate Sheela
Professor, Department of Computer Applications
R. M. D Engineering College, Kavaraipettai, TN, INDIA
drsheela09@gmail.com

Abstract— **Cloud computing is a blossoming and rapidly evolving model, with new features and capabilities being announced regularly. Security of cloud-based applications and data is one of the key concerns of cloud customers. Secure software and secure software life cycle management are fundamental to the protection of cloud services. The information security of cloud systems rest on the classical principles of confidentiality, availability, and integrity, but applied to distributed, virtualized, and dynamic architectures. This paper presents an analysis of data security issues in a cloud environment. Solution exist for a few. Analysis of these solutions can be used to determine the lacunae in the data security issues.**

Keywords- Cloud Computing, Data Security, Data Security Life Cycle,

I. INTRODUCTION

Cloud computing can be defined as a new flair of computing in which real time scaling and virtualized resources are provided as a services over the Internet. Cloud computing has become a noteworthy technology trend, and many IT professionals expect that cloud computing will rewrite information technology (IT) processes and the IT marketplace. With the cloud computing technology, users use a diverse range of devices, including PCs, laptops, smartphones, and PDAs to access programs, storage, and application-development platforms over the Internet, via services offered by cloud computing providers. Advantages of the cloud computing technology include cost savings, high availability, and easy scalability.

The remainder of this paper is organized into different sections in which the background is presented in section II. In section III, data security issues were discussed. In section IV, research work done in different aspects of data security are discussed. In section V, findings of various data security solutions are analyzed. In section VI, the conclusion and future work are mentioned.

II. BACKGROUND

There are various security issues for cloud computing as it comprises many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are pertinent to cloud computing.

For example, the interconnection between the systems in a cloud have to be over secure network. Furthermore, virtualization paradigm in cloud computing results in several security worries. For example, mapping from virtual machines to physical machines has to be carried out securely. Data security involves data encryption as well as enforcing appropriate data sharing policies. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds. Figure 1 illustrates the architectural view of security issues addressed in Cloud Computing environment.[1]

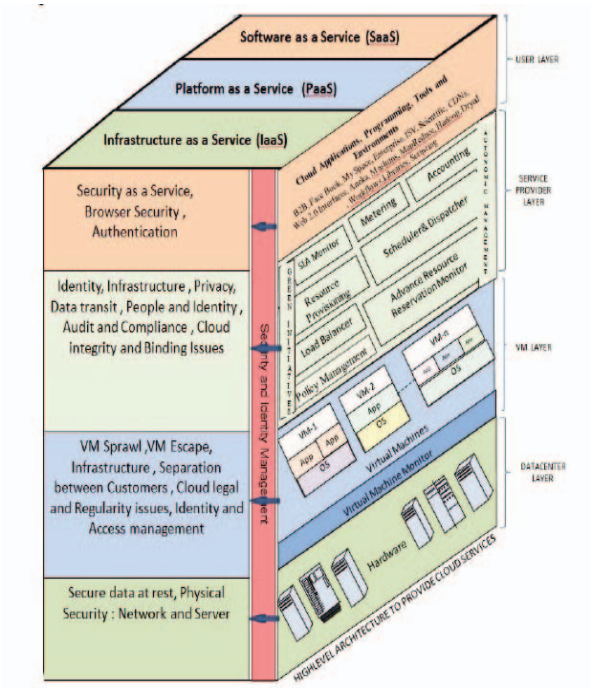

Figure 1: Security Architecture of Cloud Computing

The Cloud Security Alliance have emphasized security in 8 domains out of 14 domains [2].