International Journal of Cloud Computing and Services Science (IJ-CLOSER)
Vol.1, No.2, June 2012, pp. 53~58
ISSN: 2089-3337

World of Cloud Computing & Security

Ashish Kumar
Departement of Computer Science & Engineering, Bharatividyapeeth college of Engineering

Article Info

Article history:

Received Apr 27th, 2012
Revised May 10th, 2012
Accepted June 3th, 2012

Keyword:

Cloud computing
Security
Identity based Encryption

ABSTRACT

Cloud computing promises to increase the velocity with which application are deployed, increase innovation and lower costs, all while increasing business agility and hence envisioned as the next generation architecture of IT Enterprise. Nature of cloud computing builds an established trend for driving cost out of the delivery of services while increasing the speed and agility with which services are deployed. Cloud Computing incorporates virtualization, on demand deployment, Internet delivery of services and open source software .From another perspective, everything is new because cloud computing changes how we invent, develop, deploy, scale, update, maintain and pay for application and the infrastructure on which they run. Because of these benefits of Cloud Computing, it requires an effective and flexible dynamic security scheme to ensure the correctness of users' data in the cloud. Quality of service is an important aspect and hence, extensive cloud data security and performance is required.

Corresponding Author:

Ashish Kumar
Departement of Computer Science & Engineering,
Bharatividyapeeth college of Engineering,
A-4 Paschim vihar, Delhi-110063, India.
Email: ashish.kumar@bharatividyapeeth.edu

1. INTRODUCTION

The emerging Cloud computing field offers so many advantages to the web connected devices. To handle the massive amount of data present in cloud and the popularity that gains cloud computing over the past few years, security becomes a major concern for all who are using it and also those who want to utilize it but would not able to do so because no one can assure them in terms of security of their data on the cloud. A layered framework is required to secure the data in cloud. The storage security and the data security is must to store, manage, share, analyze and utilize the substantial amount of data. Data residing on the cloud should be secure, authenticated and encrypted so that three level securities can be provided. Cloud computing has eminent IT [1] to newer altitude by offering the market environment data storage and capacity with flexible scalable computing processing power to match the demand and supply, diminishing down the cost capital within the secure environment. The cloud system should (a) support the efficient and encrypted storage of sensitive data (b) supervise, query and save the enormous amount of data (c) support strong reliability and authentication (d) sturdily maintain integrity and confidentiality of the secret data. There are many cloud computing systems in the real world which are not suffered from security and privacy problems but based on the analysis we find that cloud systems do have security problems because the concerns provided by the companies are inadequate and accordingly causes a big barrier for the users to acclimatize themselves to the world of cloud computing. Whenever the matter of cloud computing comes up there are two facts that seem to govern the conversation. The first is that enterprises and small business would desperately like to make greater use of the explosion in new cloud services and offerings. Concerns over the security of information in cloud infrastructures, especially public cloud infrastructures, continues to stifle adoption of cloud services