Cloud Storage- Security and Privacy

Mula Aswini, Sri. P.Suresh Babu

I. Introduction

Cloud computing is an Internet based computer technology. Some of the major firms like Amazon, Microsoft and Google have implemented the cloud and have been using it to speed up their business. Cloud computing has given a new dimension to the complete outsourcing arena.

Cloud Providers offer services that can be grouped into three categories.

C. Software as a Service (SaaS)

In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customer side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

B. Platform as a Service (Paas)

Here, a layer of software, or development environment is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

II. Security and Privacy in Cloud Storage

A cloud storage system can be considered to be a network of distributed data centers which typically uses cloud computing and application servers, such as LAMP platform (Linux, Apache, MySQL and PHP), restricted J2EE, Ruby etc. Google’s App Engine, Force.com, etc are some of the popular PaaS examples.

To increase the availability of the data, it may be redundantly stored at different locations. In general, all of this is not visible to the user. Many cloud storage providers are active on the market, offering various kinds of services to their customers. Basic cloud storage services are generally not designed to be accessed directly by users but rather incorporated into custom software using Application Programming Interfaces (API).

The security requirements include the interaction with the web application via browser, the actual data storage and transmission as well as basic features of the cloud storage client applications and special features such as file sharing and publication. Cloud storage providers usually require the creation of a user account
before any services can be used. In case of a security breach, the easiest way to minimize potential data theft is to limit data collection to the bare minimum needed to operate the service – this approach is also called “data minimization”. The absence of valuable personal data might even make the service less attractive to financially-orientated attackers. Cloud storage providers usually provide client software which assists users in setting up their synchronization or backup schemes on the local devices. The actual transmission of all data with the remote storage servers is also handled by the client software. Therefore, the server must authenticate itself to the client and all communication should be encrypted and its integrity ensured. All data should be encrypted on the client system before the data is transmitted into the cloud using a key unknown to the service provider. Standalone software may be used to encrypt all data on the client system, but this has drawbacks: The software has to be installed, administrated and operated on all client systems in addition to the client software of the cloud storage provider. The key used to encrypt the data needs to be distributed to all devices which are used to access the stored data. In the event that this key is lost, the data can never be decrypted again. As a precautionary measure, all keys used to encrypt data could be integrated into some kind of key escrow system to guard against data loss. Different from the traditional computing model, cloud computing utilizes the virtual computing technology. User’s personal data may be scattered in various virtual data centers rather than stay in the same physical location, even across the national borders. At this time, data privacy protection will face the controversy of different legal systems. On the other hand, users may leak hidden information when they accessing cloud computing services. Attackers can analyze the critical task depending on the computing task submitted by the users. The major privacy issues relate to i) Trust, i.e. whether there is unauthorized secondary usage of PII (Personally Identifiable Information), ii) Uncertainty, i.e. ensuring that data has been properly destroyed by the one who controls retention of data on how the privacy breaches have occurred and how the fault is determined in such cases iii) Compliance, i.e. environments with data proliferation and global, dynamic flows, and addressing the difficulty in complying with trans boarder data flow requirements. The content of data security and privacy protection in cloud is similar to that of traditional data security and privacy protection. It is also involved in every stage of the data life cycle. But because of openness and multi-tenant characteristic of the cloud, the content of data security and privacy protection in cloud has its particularities. The concept of privacy is very different in different countries, cultures or jurisdictions. The definition adopted by Organization for Economic Cooperation and Development (OECD) is “any information relating to an identified or identifiable individual (data subject)”. Another popular definition provided by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) in the Generally Accepted Privacy Principles (GAPP) standard is “The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information.” Generally speaking, privacy is associated with the collection, use, disclosure, storage, and destruction of personal data (or personally identifiable information, PII). Identification of private information depends on the specific application scenario and the law, and is the primary task of privacy protection. Data security and privacy protection issues, the fundamental challenges are separation of sensitive data and access control. Our objective is to design a set of unified identity management and privacy protection frameworks across applications or cloud computing services. As mobility of employees in organizations is relatively large, identity management system should achieve more automatic and fast user account provisioning and de-provisioning in order to ensure no un-authorized access to organizations’ cloud resources by some employees who has left the organizations. Authorization and access control mechanisms should achieve a unified, reusable and scalable access control model and meet the need of fine-grained access authorization. Accountability based privacy protection mechanisms will achieve dynamical and real-time inform, authorization and auditing for the data owners when their private data being accessed.

III. Conclusion
Although cloud computing has many advantages, there are still many actual problems that need to be solved. According to service delivery models, deployment models and essential features of the cloud computing, data security and privacy protection issues are the primary problems that need to be solved as soon as possible. Data security and privacy issues The challenges in privacy protection are sharing data while protecting personal information. The typical systems that require privacy protection are e-commerce systems that store credit cards and health care systems with health data. The ability to control what information to reveal and who can access that information over the Internet has become a growing concern.

References
Mula Aswini (Student), M.Tech-C.S.E., Final Year (II-II), Kaushik College of Engg., Visakhapatnam, India.

Sri. P.Suresh Babu, B.Tech,M.E. is working as Associate Professor in the Department of Computer Science & Engineering Kaushik College of Engineering, Visakhapatnam, Andhra Pradesh. He has 15 years of teaching and 4 years of Industrial experience. He has guide 30 UG and 11 PG projects.