Abstract - this paper provides an insightful analysis of the existing status on cloud computing data processing issues based on a detailed survey carried by the author. It also makes an attempt to describe the security challenges in data processing framework of cloud computing and also endeavors to provide future research directions.

Keywords - cloud computing, data, integrity, security, availability, confidentiality, authentication, infrastructure, services.

I. INTRODUCTION

Cloud computing is a complete new age technology. Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. From a user perspective, cloud computing provides a means for acquiring computing services without any need for deep understanding of the underlying technology being used. From an organizational perspective, cloud computing delivers services for consumer and business needs in a simplified way, providing unbounded scale and differentiated quality of service to foster rapid innovation and decision making.

Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT services over the Internet. However, cloud computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies, it also inherits their security issues. In general cloud providers offer three types of services i.e. Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

Clouds are the new trend in the evolution of the distributed systems, the predecessor of cloud being the grid. The user does not require knowledge or expertise to control the infrastructure of clouds; it provides only abstraction. It can be utilized as a service of an Internet with high scalability, higher throughput, quality of service and high computing power. Cloud computing providers deliver common online business applications which are accessed from servers through web browser [1].

Fig 1. The cloud reference architecture.

Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers,
storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud Computing appears as a computational paradigm as well as distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [2,3]. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [4].

Cloud can be divided into three types: public cloud, private cloud, and hybrid cloud. Public cloud is as the property of service provider and can be used in public, private cloud refers to being the property of a company, and hybrid cloud is the blend of public and private cloud. Most of the existing cloud services are provided by large cloud service companies such as Google, Amazon, and IBM. A private cloud is a cloud in which only the authorized users can access the services from the provider. In the public cloud, anybody can use the cloud services whereas the hybrid cloud contains the concept of both public and private clouds.

Cloud computing environment provides two basic types of functions: computing and data storage. In the cloud computing environment, consumers of cloud services don't need anything and they can get access to their data and finish their computing tasks just through the internet connectivity. During the access to the data and computing, the clients don't even know where the data are stored and which machine executes the computing tasks.

A. Applications

There are a few applications of cloud computing as follows:

1. Cloud computing provides dependable and secured data storage center.
2. Cloud computing can realize data sharing between different equipment's.
3. The cloud provides nearly infinite possibility for users to use the internet.
4. Cloud computing does not need high quality equipment for the user and it is easy to use.

I. CLOUD DATA ANALYSIS

To achieve interoperability among clouds and to increase their stability and security, cloud standards are needed across different standard developing organizations. For example, the current storage services by a cloud provider may be incompatible with those of other provider. In order to keep their customers, cloud providers may introduce so-called “sticky services” which create difficulty for the users if they want to migrate from one provider to the other, e.g., Amazon’s S3 is incompatible with IBM’s Blue Cloud or Google storage.

A. Cloud Data Management

Processing data in the cloud can be very large (e.g., text-based or scientific applications), unstructured or semi-structured, and typically append-only with rare updates. Cloud data management is an important research topic in cloud computing. Since service providers typically do not have access to the physical security system of data centers, they must rely on the infrastructure provider to achieve full data security. Even for a virtual private cloud, the service provider can only specify the security setting remotely, without knowing whether it is fully implemented. The infrastructure provider, in this context, must achieve the objectives like confidentiality, auditability.

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness [5].

Confidentiality is for secure data access and transfer, and auditability for attesting whether security of applications has been tampered with or not. Confidentiality is usually achieved using cryptographic protocols, whereas auditability can be achieved using remote attestation techniques. However, in a virtualized environment like the clouds, Virtual Machines can dynamically migrate from one location to another; hence directly using remote attestation is not sufficient. In this case, it is critical to build trust mechanisms at every architectural layer of the cloud.

B. Cloud Platform Management

Cloud Computing challenges in delivering middleware capabilities for building, deploying, integrating, and managing applications in a multi-tenant, elastic and scalable environments. One of the most important parts of cloud platforms provides various kinds of platform for developers to write applications that run in the cloud, or use services provided from the cloud, or both. Different names are used for this kind of platform today, including on-demand platform and platform as a service (PaaS). This new way of supporting applications has great potential. When a development team creates an on-premises application (i.e., one that will run within an organization), much of what that application needs already exists. An operating system provides basic support for executing the application, interacting with storage, and more, while other computers in the environment offer services such as remote storage.
C. Service Level Agreement

It is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. Cloud is administrated by service level agreements that allow several instances of one application to be replicated on multiple servers if need arises; dependent on a priority scheme, the cloud may minimize or shut down a lower level application. A big challenge for the cloud customers is to evaluate SLAs of cloud vendors. Most vendors create SLAs to make a defensive shield against legal action, while offering minimal assurances to customers. So, there are some important issues, e.g., data protection, outages, and price structures that need to be taken into account by the customers before signing a contract with a provider.

To satisfy the requirements of next century computing, cloud computing will need to mean more than just externalized data centers and hosting models. Although architectures that we deploy in data centers today should be able to run in a cloud, simply moving them into a cloud stops well short of what one might hope that cloud computing will come to mean. In fact, tackling global-scaled collaboration and trading partner network problems in government, military, scientific, and business contexts will require more than what current architectures can readily support.

D. Characteristics

We identify technical characteristics below that must not be overlooked in future architectures:

1. An architecture style that should be used when implementing cloud-based services
2. External user and access control management that enables roles and related responsibilities that serve as interface definitions that control access to business functionality
3. An Interaction container that encapsulates the infrastructure services and policy management necessary to provision interactions
4. An externalized policy management engine that ensures that interactions conform to regulatory, business partner, and infrastructure policy constraints
5. Utility computing capabilities necessary to manage and scale cloud oriented platforms

II. SECURITY MEASURES

There are numerous security issues for cloud computing as it encompasses 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 applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

Security is a big challenge in cloud system due to its nature of outsourced computing. Mainly, confidentiality, integrity and authentication are the primary pain areas. Unless robust security scheme and user-centric security policy is implemented, cloud system would be vulnerable to different attacks and susceptible by the users. Data security has
consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in the entire globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture.

One of the primary focuses to provide cloud security is to have one integrated solution enabling the required security primitives like confidentiality, authentication and integrity. Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users. Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS. Besides data storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature. In a SaaS deployment model, sensitive data is obtained from the enterprises, processed by the SaaS application and stored at the SaaS vendor end. All data flow over the network needs to be secured in order to prevent leakage of sensitive information. This involves the use of strong network traffic encryption techniques such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) for security.

The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The availability of cloud service providers is also a big concern, because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization. In [6, 7], it is described that cloud specific security solutions like confidentiality-enabled computing, user-defined authentication and access control, atomic data integrity are the main issues to be addressed for a sustainable and scalable data processing in cloud computing.

III. CONCLUSION

In this paper we discussed several aspects on secure data processing in cloud computing. A framework on processing data includes data confidentiality, data authentication, availability of data and data integrity gives us the required security to process. Using this framework the cloud computing can be more reliable to use the services that are needed by the organizations and individuals in near future.

REFERENCES


