Journal of Fundamental and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

CLOUD COMPUTING: A NEW ERA

S. Namasudra

School of Computing Science and Engineering, Galgotias University, Uttar Pradesh, India, Pin-201310

Received: 04 March 2018 / Accepted: 30 April 2018 / Published online: 01 May 2018

ABSTRACT

Cloud computing is a new paradigm of Information Technology (IT), which allows users to access software, hardware and data from the cloud server. Cloud computing provides many services to the users. Nowadays, access control and security are two most critical problems with cloud computing. Access control can be defined as a procedure by which users can access data from the cloud server. At the time of accessing data, there are many problems, such as data security, high data accessing time, data loss, overhead, data redundancy, etc. Several access control models have been already developed based on attribute-based encryption. In the first part of this paper, a brief discussion of fundamentals of cloud computing are presented. Moreover, all the issues of cloud computing are also discussed in this paper. Finally, future work directions have been identified for the cloud computing environment.

Keywords: Cloud Computing, Cloud Service Provider, Data Owner, Access Control, Encryption.

Author Correspondence, e-mail: suyelnamasudra@gmail.com

doi: http://dx.doi.org/10.4314/jfas.v10i2.9

1. INTRODUCTION

Cloud computing is an emerging area in IT sector, which utilizes the concepts of virtualization, service-oriented architecture and parallel computing. Distributed computing can be referred as a synonym of cloud computing over a network. The word “cloud” can be referred as a blend of

networks, hardware, storage and interfaces to deliver a service. The main features of cloud computing are agility, reliability, scalability, pay-per-use, on demand service, resiliency, performance, security and resource pooling [1-2]. Currently, many IT companies like Microsoft, Google, Yahoo, Amazon, etc. are providing the cloud services to the users because of many advantages, such as reduced IT cost, scalability, business continuity, flexibility of work practices, almost unlimited storage, speed, etc. [3-4]. In cloud computing, users need not to worry about software, hardware or any external equipment. In cloud computing, users do not know where the data are actually stored on the cloud servers. It provides an infrastructure to the users to save data on the cloud server. However, along with these advantages, there are some disadvantages also, namely security and privacy in the cloud, transferability, downtime, understanding and limited control [5]. Many business models are developed by cloud computing [6]. In future, cloud computing can be used as a business computing model. Due to its current development in IT sector, there is a raise in need for security and privacy protection.

In cloud computing, there are three parties, namely Cloud Service Provider (CSP), Data Owner (DO) and users. The CSP provides the cloud infrastructure for both DOs and users. The CSP records the profile of each user and DO, and controls all the tasks of the cloud server [7]. The CSP allows DOs to store their data or files on the cloud server, and the users can access these data from the cloud server according to their demand. Figure 1 shows the simple scenario of cloud computing. There are few requirements for cloud services:

- For accessing any data or service, the CSP must specify the access control policies for both DOs and users.
- The security of an organization lies in its ability to enforce more access policies to the users. When a user requests a resource from a cloud server, s/he has to associate with the access policies of the CSP. To provide requested resource to the user, there must be a mapping of access policies between the CSP and organizations with the available resources. There is always a chance to violate the mapping of policies. So, enforcing of more access policies by the organization are beneficial in regard to secure accessing of resources.
- The DO must offer all kind of services to the consumers.

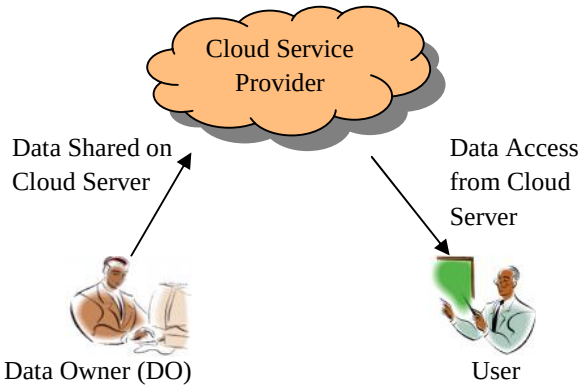

Fig.1. Simple scenario of cloud computing

Cloud services are fully based on the internet. We know that there are many hackers or malicious users over the internet. So, cloud services used to face many security issues [8]. There are many policies and technologies have been developed for web services. These policies have an important impact for solving security or privacy issues of cloud services.

Access control is a major issue out of all the privacy and security issues. Access control model can be defined as a procedure by which a user can access data, file or any kind of services from the cloud servers [9]. It has been a very important security topic since 1970s [10]. Because of the static nature of the traditional access control models, they cannot be applied in the cloud environment. There are some important characteristics of cloud services, such as a large number of dynamic users, a large amount of resources, etc. which must be considered for developing any access control model. Many access control schemes have been already proposed for cloud computing [11-13]. The main contributions of this paper are mentioned below:

- In the first part of this paper, fundamentals of cloud computing are presented.
- All the issues or problems of cloud computing are discussed in this paper one by one.
- Many future work directions have been also explained in this paper for the cloud computing environment.

The rest of the paper is organized in different parts. Section 2 provides the fundamentals of cloud computing. In section 3, all the issues of cloud computing have been discussed in details. Section 4 highlights the future work directions. Finally, conclusions of the paper are given in section 5.

2 FUNDAMENTALS OF CLOUD COMPUTING

In this section, fundamentals of cloud computing are discussed in details

2.1 History of cloud computing

In the 50s, there were large scale mainframe computers. It was so costly that users could not afford to buy such computer for individual use. For this reason, they had started a practice, which was known as “time sharing”. “Time sharing” allowed many users to use a single computer. It is the same principle like virtualization, which gives us a wonderful path towards the cloud computing. Table 1 shows the history of cloud computing.

Table 1. History of Cloud Computing

Year	Achievement
1969	J.C.R. Licklider introduced the idea of "intergalactic computer network". He was trying to connect all the computers, which were located over globally [14]. Other experts gave their idea of “cloud” concept to scientist John McCarthy.
1970	IBM launched an operating system, namely VM, and then, practical implementation of virtual machines takes place in IT companies. In this infrastructure, several computers work in the same processing environment.
1980	IBM launched an affordable user’s computer. At that time, Microsoft also gave its operating system.
1990	Internet started to offer sufficient bandwidth and companies interconnected their staffs with their own computers.
1999	In 1999, salesforce.com was the main milestone cloud of computing [15]. Its aim was to deliver applications via a simple website. Many companies following the technology of salesforce.com to deliver services.
2002	Amazon started to offer many services including storage, applications and computation through the Amazon Mechanical Turk.
2006	In 2006, Amazon introduced its Elastic Compute Cloud (EC2) for commercial use [16]. EC2 provides the cloud to companies and individual users, where they can run their own applications. Amazon EC2/S3 was the first widely

	usable cloud infrastructure.
2007	Cloud computing became much popular, when there was the collaboration between Google and IBM.
2009	In 2009, Web 2.0 hits in the market. Through “Google Apps”, Google and other companies started to offer browser-based applications.
2012 and onwards	Nowadays, many IT companies recognize their benefits in the cloud computing environment. In IT industries, cloud computing mainly increases storage and flexibility.

2.2 Service delivery model

Cloud computing is usually delivered by three services, namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a service (IaaS) [17].

2.2.1 Software as a Service (SaaS)

In SaaS model, a license version of a software application is provided by the cloud provider. Any company or user can purchase this software on demand. Sometimes, SaaS is referred as "on-demand software". In SaaS, users can pay money as they need like yearly, monthly, weekly or hourly. So, there is no issue that for how much time users have to pay money. In SaaS, users need not to worry about any external installation. Users can access that software by any browser or by any client device. In SaaS, information security is the key challenge because of using the web browser. Here, Extensible Markup Language (XML) encryption and Web Services (WS) security processes are used for security. In Figure 2, service delivery model of cloud computing is shown.

Examples of SaaS providers: Salesforce.com, Google Mail, MuxCLoud, etc.

Advantages of SaaS:

- SaaS reduces the complexity of installing the software.
- From the user’s side, no need to worry about maintenance and upgrade SaaS.
- In SaaS, one user can use multiple services from many SaaS providers.

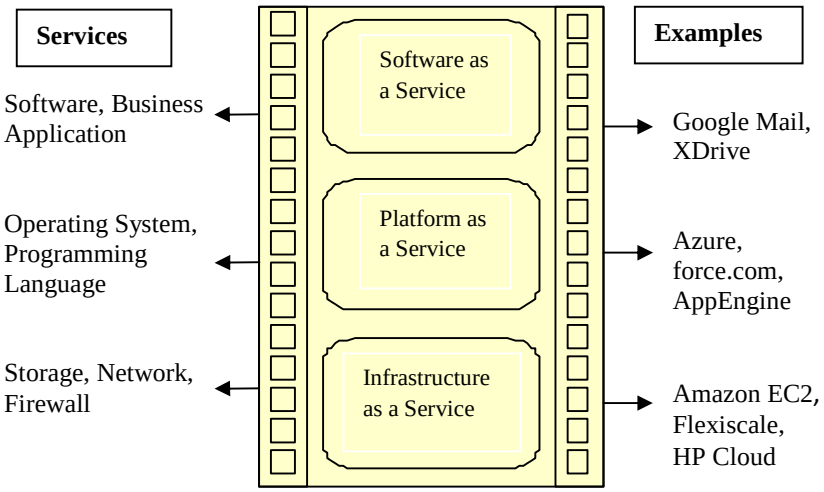

Fig.2. Service Delivery Model of Cloud Computing

2.2.2 Platform as a Service (PaaS)

In PaaS, the cloud service providers provide an environment, including operating systems, databases, programming languages execution environments and web servers. PaaS offers a cloud environment, where users can create, run and deploy applications. Here, users need not to worry about how much memory they have used and how many processors are currently using. PaaS offers load balancing, scalability and fault tolerance.

Examples of PaaS providers: Aneka, Azure, AppEngine, Force.com, etc.

Advantages of PaaS:

- In PaaS model, users need not to worry about scalability and any kind of software or hardware.
- In PaaS, users need not to worry about how much memory is used for running a software.
- It provides a complete platform to develop software.

2.2.3 Infrastructure as a Service (IaaS)

Nowadays, in IT companies, IaaS is the most popular. In IaaS model, the client can usually use the infrastructure of the cloud providers. This infrastructure can be storage, network, firewalls, etc. IaaS provides many resources like raw based storage, load balancers, virtual local area networks, IP addresses and software bundles. For deploying IaaS applications, users have to install the operating system and software on the cloud environment. IaaS provides services on the basis of user's demand. IaaS providers used to take the bill from users on the basis of how much they have used the cloud services.

Examples of IaaS providers: Amazon EC2, Flexiscale, GoGrid, RackSpace, HP Cloud, etc.

Advantages of IaaS:

- IaaS provides a mechanism to control other two service models, namely SaaS and PaaS.
- Users are responsible for doing scalability in IaaS. So, cloud providers do not have control in scalability.
- Improvement of the network's performance can be done by IaaS.

2.3 Deployment model

There are mainly four types of cloud, namely private cloud, public cloud, community cloud and hybrid cloud. The CSP decides what type of cloud can be given to the users.

- *Private cloud:* A private cloud is a cloud infrastructure, which is solely operated by a single organization. It can be managed by an organization or by a third-party. A private cloud provides computing power as a service within a virtual environment using an underlying pool of physical resources. In a private cloud, resources are only accessible by the customers of any organization, which increases security and privacy policy of that organization. Using of private cloud is more secure than other clouds because it is originally handled by one organization [18]. Figure 3 shows a block diagram of deployment model of cloud computing.

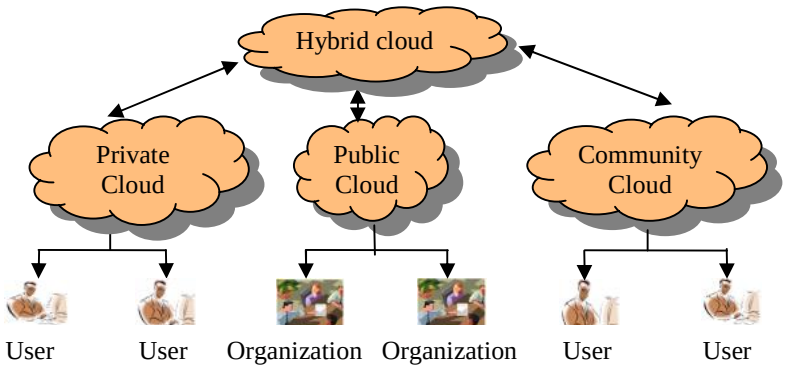

Fig.3. Deployment model of cloud computing

- *Public cloud:* In the public cloud, the CSP provides the resources, such as network, server, data center, etc. [19]. In the public cloud, users can pay money for how much they have used the public cloud. It helps IT companies to expand or reduce the use of cloud according to their requirements [20]. In the public cloud, customers or users from many organizations are mixed together, and they use the same cloud or network. Due to a large number of users from many organizations, there may be many attackers. So, security concern is a big deal in the

public cloud. Security in the public cloud is less in comparison to other clouds. This problem can be minimized, if the CSP regularly check the cloud server.

- *Community cloud:* In a community cloud, infrastructure or cloud environment is shared by a community of several organizations [21]. All these organizations have to be a common goal. The community cloud is managed by all these organizations or by the third party. The community cloud sometimes is used for national security purpose. “Open Cirrus” is an example of community cloud. “Open Cirrus” is used by many researchers or universities for the testbed. The community cloud is also used for inter-agency and collaboration needs.
- *Hybrid cloud:* Hybrid cloud is a combination of the public and private cloud. It is managed by the central administrator [22]. The hybrid cloud gives IT solutions by a combination of public, private and community clouds, and it provides secure access control between users and cloud providers. In the hybrid cloud, if there are many data access requests among CSP, DO and users, these requests do not effect to other clouds.

3 ISSUES OF CLOUD COMPUTING

Nowadays, many companies are providing cloud services. The CSP must ensure that users do not face any problem like data loss or security at the time of data accessing since there are many hackers in the cloud servers [23-34]. Some problems of cloud computing environment are listed below:

3.1 Availability

Availability is a very critical problem for all types of cloud, namely private cloud, public cloud, community cloud and hybrid cloud. The aim of availability in the cloud computing environment is to provide services to the users at any time from any place.

Currently, CSPs who are providing infrastructures and platforms are mainly based on the virtual machines. Here, virtual machines are allowed to block traffic with respect to IP addresses. These security strategies are placed along with the virtual machines to put availability in the cloud system.

3.2 Confidentiality

Confidentiality of a cloud environment can be defined as to keep user’s data secret in the cloud environment. In a cloud computing environment, confidentiality plays a vital role for managing user’s data, which are stored across multiple data centers. Nowadays, cloud computing has lots of

malicious users, who are creating critical problems for the public network in comparison to the private network. So, the CSP must carefully examine those malicious users, when DOs stored their data on the cloud server. The CSP must assert confidentiality at different layers of cloud application to protect user's sensitive data.

3.3 Access control

Access control ensures that only authorized users can access the data from the cloud server. By access control, the CSP monitors all the access requests made by the customers or users to access a data or file. For accessing data or file, there are many steps like authentication, authorization and accountability, which are followed at the time of accessing data. In cloud computing, DOs must be always online, when users want to access data. So, if DOs are not online, access is not possible. Sometimes, for providing one data, the CSP has to search the whole database. So, searching cost is increased, and for this reason, users have to wait for a long time to get a data from the cloud server.

Cloud computing increases the threat to confidential data or file. At first, sometimes, there may be arising of many risks because of government surveillance over databases. In a cloud environment, data can be stored in any country, where data were not previously saved. The government of that country has legal rights to see the data [35- 36]. In some cases, customers do not get any kind of notification that their data have accessed by the government of abroad or not.

Secondly, any authorized users of IT companies reveal their database to the malicious users. Then, malicious users can get access to data or file from the cloud server. There may be many employees or DOs in the cloud environment, who always break the security policies.

3.4 Data related issues

There are several issues related to data, which are given below:

- *Data integrity:* Data integrity in a cloud environment allows maintaining information integrity i.e. user's data must not be modified by any unauthorized user or by the CSP. Sometimes, it has been seen that data saved by the DOs are not same as data access by the users. Data are modified by the hackers or malicious users. So, it is the responsibility of the CSP to provide data integrity to the users.
- *Data loss:* If the cloud provider stops their services due to a financial crisis or due to some other reasons, there may be data loss. Users are not able to access data in future because data are not available on the cloud servers**.** So, data loss is a major problem in cloud computing.

- *Data leakage:* Data leakage happens, when data goes to wrong hands like hackers or malicious users. Hackers always hack the original data, and access some confidential data. It always creates a critical issue.
- *Data location:* Locations of data are obscure to users. Users do not know where the data are actually stored. It may be stored in their country or outside the country. Only the CSP knows, where the data are stored. Most of CSPs have their data center across the world [37].
- *Unwanted access:* Cloud computing has many risks for maintaining the confidentiality of data or file. For an example, if user's data are stored outside their country, the government of that country can view the actual data under the circumstances. So, the user's data are not safe in such condition.
- *Data segregation:* In cloud computing, different users use the same device for storing data. The CSP does not store data of different users on different devices. Poor segregation of data gradually increases the risk. This problem can be solved by giving complete isolation of storage of customer's data in the cloud server. Nowadays, encryption is used to solve this problem. Strong encryption may also increase costs. Even data can be destroyed at the time of encryption. Sometimes, the CSP uses a strong encryption for security. So, the CSP has to remember that user's data must not be destroyed or changed at the time of encryption.
- *Vendor lock-in:* Vendor lock-in is a technique, which allows users to depend on the vendor's services. Vendor lock-in is achieved by building IT solutions. It is considered as one of the main issues of cloud computing. When a vendor stops to deliver a service, the CSP tries to deliver the service from another vendor, which may be belonging from another cloud server (CSP). Moving services from one CSP to another is very difficult and insecure also.
- *Data deletion:* Another main issue in the cloud server is that how can users know that the data or file are fully deleted from the server, and it cannot be recovered again. All the data on the cloud server can be backed up by the CSP [38]. Currently, there are no procedures to know that user's data are completely deleted from the cloud server or not. The CSP stores data in several physical devices. In one device, there are many data, and the device cannot be destroyed from the cloud server. Therefore, it creates a critical data issue for DOs.
- *Data investigation:* In a cloud computing environment, there are several distributed systems. Therefore, searching information is very difficult. When users make a request for data, the CSP takes much time to analyze the data. So, it takes more time for giving the information. In

addition, the CSP stores data in multiple data centers across the big geographical area, which makes the issue more complex.

- *Secure data transfer:* In a cloud computing environment, all the traffic are placed between users and cloud provider networks. If attackers get a link to access the cloud network, they can easily hack the data. Sometimes, in a cloud environment, there is no secure data communication channel, which creates a major problem for the customers. The CSP has to make sure that data are usually transferred through a secure channel.
- *Customer data manipulation:* There are many applications, such as SQL injection, insecure direct object references, command injection, cross-site scripting, etc. Hackers manipulate data and attack these web applications.

3.5 Storage related issues

Cloud computing provides an environment, where data are stored in the CSP's site, and manage it by the CSP or third party. Data are usually saved in remote drives across the world. The CSP has very large memory space for data storage. Users pay money for the using of storage space. The CSP offers services, which are accessed by users through an Application Programming Interface (API) over the internet [39]. The CSP provides data safety by dividing data into many small pieces. After dividing, the CSP stores data in various data storage centers. If any portion of data is crashed, data can be recovered from another portion of data. There are many issues related to storage of data, which are given below:

- *Security provider:* Since the CSP controls all the tasks of a cloud environment and it is untrusted, many users get worried regarding the vulnerability of the resources. Cloud providers must be more sensitive to this issue.
- *Ownership:* When data are not used for a long time in the cloud, some users worry about losing their own rights. Many CSPs address this problem with very strong agreements. By these agreements, users do not need to worry about the rights of their own data.
- *Multiplatform support:* In cloud computing, another issue for IT departments is that how services are integrated with different operating systems, such as Linux, OS, Windows, etc. Multiplatform support is a issue in IT companies for using cloud services.
- *Data recovery:* There may be an accident on the cloud server. So, data can be loss. It is the responsibility of the CSP to create the backup of data from which data can be recovered if necessary.

- *Data portability and conversion:* Sometimes, in critical condition, it is very difficult to transfer data. Partitioning and converting file or data mainly depends on the CSP. After converting, the CSP has to remember the format of data, which cannot be revealed to the malicious users.

3.6 Policy issues

Privacy of a cloud environment differs with the cloud scenario. Some clouds have low privacy threats, and some clouds have high privacy threats. Sometimes, services are personalized based on the calendar, social networks, people's location and preferences. In that condition, privacy is a great deal because the potential risk is very high.

Public cloud is much suitable, when cost is considered. But, public cloud is faced a lot of policy issues. The CSP has faced many problems in controlling the public cloud. Some of them are listed below:

- *Lack of user control:* In SaaS cloud environment, from the user's side, visibility and control of data are limited. So, the main question is that how data are stored on the cloud server and how users get control over data. These are the legal requirements of users. Users do not have personal control over the data.
- *Unauthorized secondary usage:* Unauthorized uses of data create a big risk in the cloud environement. In cloud computing, the CSP always wants to earn money from the uses of user's data. In many cases, secondary data uses are declined by the CSP. Nowadays, there are no restrictions on such secondary uses.
- *Data proliferation:* "Data proliferation" is defined as the ability of a cloud server to involve several multiple parties, where DOs have no data control. A legal jurisdiction is needed for transferring data from one cloud to another cloud. This increases risk and legal complexity [40-41]. When the CSP wants to access data from outside his/her own domain, the CSP used to face many rules of government. The risk can be arised if users choose a wrong business partner, where knowing the jurisdiction is very difficult [42].
- *Dynamic provisioning:* In cloud computing, it is not clear that which third party is responsible for observation of personal information or who sets the standard for handling the data [43]. It is also unclear that data are periodically audited or not.

3.7 Security issues

In the traditional model, there was self-control system for managing a cloud or stored data. The security in the cloud becomes a sensitive issue in the sense that confidential data or file may be stored outside the user's own domain.

The public cloud does not raise only privacy issues, but it also shares security concerns. Security is rated as top challenge of the cloud environment in a recent survey [44].

The main issues arise in cloud computing to define which party is responsible for which type of security. This division of security issue arises because there is no standardized API. According to the cloud security alliance, the main issues of cloud computing are insecure interfaces, shared technology issues, malicious insiders, account hijacking, data loss or leakage and unknown risk profile [45].

- *Authentication and identity management:* Identity Management (IDM) mechanism is used by the CSP to authenticate the users and provide services [46]. A major problem related to IDM is interoperability. IDM used many identity tokens, and there are many identity negotiation protocols. Existing authentication techniques are mainly based on passwords, which have many limitations. An IDM system must be able to protect private and sensitive information related to the users and processes. In multi-tenant cloud server, IDM is not yet well understood. Customer's identity and information must segregate in multi-tenant cloud infrastructure.
- *Backup:* In a cloud computing environment, it is very difficult to guarantee adequate availability and backup. Backup of data is very critical, if there is any failure. The CSP usually stores backup files without informing the users of that particular data.

  There are two new risks in the cloud environment, namely self-healing and self-optimization. Self-healing provides appropriate business continuity and the ability to recover and back-up of data. The main problem is that it is not possible to determine where the data processing is going on [44]. "Self-optimization" means autonomy in decision making. To deal with the changing requirements of users, the role of the CSP is determined through self-optimization.
- *Lack of standardization:* Most of the issues arise due to the lack of standardization of cloud computing. Grid computing was also failed to gain adoption for virtual organizations because of standardization. Service Oriented Architecture (SOA) tried to solve many issues by establishing better standards. In cloud computing, there is no standardized communication

among CSP, DOs and users. For establishing security frame, works in heterogeneous environments are affected due to the lack of standards.

- *Multi-tenancy:* Multi-tenancy is a feature, where a single software runs on a SaaS server, and this software is used by various organizations. This software is designed in such a way that it is virtually partitioned the data. Other organizations can also use the portion of that software. Some CSPs use job scheduling algorithm to maximize hardware utilization. But, most CSPs use the virtualization for maximizing hardware utilization. Virtual Machines (VMs) are isolated from each other, which make the system safe for users to share hardware. For using virtualization, new security issues like cross-VM side-channel attacks are occurred [47].
- *Audit:* In cloud computing, the CSP needs to monitor the implementation process. The external audit process is also needed for the CSP. Many new issues have been arising in a cloud computing environment from an audit perspective. Transaction detail of cloud server needs a proper record for maintaining the data integrity. However, in the public cloud, a full audit of the cloud environment is still unsolved.

3.8 Trust issues

The benefits of cloud computing in IT sector bring a great interest to users, but it also bring lots of problems in data privacy and security. These two problems are very critical in the financial sector and also for health data. Cloud users are not able to utilize the cloud mechanism to protect their own data against unauthorized users and hackers. They usually depend on the CSP or another third party to protect their data against hackers.

Trust is not an easy concept in the cloud server. Universally, a complete definition is not accepted by all researchers. Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another [48]. Security is one procedure to establish online trust. If there is strong security, there must be strong trust. Trust is an issue, which can be solved by the CSP and users.

Reputation is another component of trust, which is one of the valuable things for companies [49]. Many users just go to a company for reputation only. For this reputation, trust is usually increased. But, trust can be broken in a very fast manner.

In cloud computing, there are mainly two types of trust, namely persistent trust and dynamic trust. “Persistent trust” is associated with long-term underlying infrastructure, and it appears in static technological and social mechanisms. “Dynamic trust” deals with short term or changeable

information. Dynamic trust of a system assured how information is stored on the cloud server and how data are accessed by users.

- *Weak trust relationships:* In cloud computing, it may be possible that for some reasons trust of service delivery become weak, but existing service delivery must not be delayed. Risk can be introduced, when a transaction is initiated. If the data do not transfer in such a way that the CSP wants, risk can also occur. When a transaction is going on, all the information about that transaction is not transparent to the user. So, people cannot see what is going on in the cloud server. But, in that case, instead of solving problems, people used to get frustrated about data security. In some cases, users are not agreed to use the CSP in the future. Sometimes, a new cloud provider is added in the cloud server to gain an extra load in real time. But, this causes serious issues. The new cloud provider may not check user's identity, data confidentiality, data integrity, etc. in a proper way.
- *Lack of customer trust:* The CSP sometimes asks users to provide their personal information like why users want to access data from the cloud server. But, this supply chain leads to suspicion and distrust of users [50]. There is also a question whether data in the cloud are totally protected [51]. So, users decline to use the cloud server without knowing the risks and how the CSP faces those risks. This is basically happened when personal or confidential data like financial or healthcare information is associated with the cloud server.

3.9 Legal aspects

For the protection of user's confidential data or sensitive data, legal frameworks are a major key. In each and every country, there are such frameworks. For an example, in US, a framework, namely "patchwork" of legislation is used for sector and data information. These frameworks are still used in the cloud server. Sometimes, it is not sure that in which route a transaction is completed. A single transaction may be processed in many countries. So, legal aspect of that country causes a security problem in cloud computing. In this sub-section, all legal aspects have been discussed.

In cloud computing, users do not know the exact location, where data have been stored. It may be stored across the world. So, the different law can be applied on the data on the basis of where data have been stored. Multiple copies of data or file are saved on the cloud server. In addition, these copies are managed by different entities. There are already existing legal constraints provided by many CSPs, which are dealt with user's personal data or file. Privacy laws change

with the location of data. European countries allow data processing according to the personally identifiable details of the data. Place restrictions also apply for the transaction of the sensitive data like health or financial data [52]. The access of particular data is not granted until or unless the purposes of data accessing is matched against the required personally identifiable information. In Europe, sometimes, data accessing for marketing purposes. In that case, accessing is not granted for personally identifiable information [53].

Storing data on the cloud server is much risky, which may impact on policy, status and obligations. There are several acts for privacy maintaining in cloud computing, such as health laws or Canadian Privacy Act. But, it is almost impossible to maintain all these laws.

3.10 Attacks on the cloud environment

Various attacks are made by malicious users, which are very critical in a cloud environment. Some of attacks are listed below:

- *Denial of Service Attack (DoS):* When a user sends many invalid requests to the server, then DoS occurs. On the cloud server, there are many unauthorized users. They always make many requests to access cloud's sensitive data. Intrusion Detection System (IDS) is used to solve this problem [54]. When a cloud server is attacked, IDS makes an alert to the systems. Thus, cloud server's performance is not degraded.
- *Cookie poisoning:* Sometimes, unauthorized users try to modify cookie for accessing data. This condition is known as cookie poisoning. The CSP must concern about cookie poisoning.
- *Distributed Denial of Service Attacks (DDoS):* DDoS occurs in a distributed environment, where accessible data are under the control of the attackers [54].
- *Virtual library checkout:* Nowadays, many companies use many virtual machines for the data center. The virtual library has many virtual machines, which are controlled by the CSP. Employees of that company upgrade virtual machines periodically on their own personal machines. So, any employee can be attackers, who can easily hack user's sensitive data.
- *Migration attack:* This attack is related to the virtual machines. When virtual machines are migrated from one place to another, then this attack occurs. Many IT companies move their virtual machines to various places according to their uses. Attackers attack those machines, and hack user's sensitive data.

- *Encryption attack:* This attack is used to extract unauthorized information from the cloud server by creating security problems. This attack is very critical, and generally not found in the cloud server.
- *DNS attack:* When a server is called by name, cloud hackers can easily connect to that network by the server name. So, unauthorized users can access user's sensitive data, if the data are not secured.
- *Sniffer attack:* Sometimes, the user's data are not encrypted before storing it on the cloud servers. In that case, attackers can easily read the content of the data from the cloud server. Sniffer program can track all the data, which are flowing in the cloud network [54].
- *Cloud malware injection:* In this attack, an attacker uploads a fake copy of a data on the cloud server. This fake data are related to the victim's service instance in such a way that same victim service is executed on that malicious instance. Here, attackers have all the control of a victim's data to understand that how data are maintained on the cloud server.

4. FUTURE WORK DIRECTIONS

On the basis of the above discussions, several future opportunities are given in this section:

- In a real-time cloud environment, third parties are allowed to take participate for improving the security. However, at present, it is not cleared that how security is providing to the user's sensitive data. Third parties may use it for their own sake. So, a strong standard (agreement) should be developed to protect the data.
- In the traditional system, access structure is always exposed to the CSP. So, any hacker or any malicious CSP can easily hack user's data, and can provide that data to another unauthorized user. Therefore, a new model can be developed to provide a strong security of the user's sensitive data.
- In the cloud server, there are many DOs who share their data on the cloud server. The CSP usually takes a long time to provide a data. So, users have to pay more for using the cloud service. Therefore, an adequate strategy can be developed that takes less time to provide the data. So, users can pay less money for using of cloud service.
- In the existing schemes, computational overhead is increased, when there are many users in the system. A new technology can be developed that reduces the overhead with respect to the number of users.

- In cloud computing, many computers are interconnected over the world. So, there is always a chance of international data leakage. A new strategy can be developed to protect the data against the international data leakage.
- A new scheme can be introduced to detect and handle fault efficiently, that can support to run multiple equipments on the cloud server.
- A new scheme can be developed to prevent the data loss due to any natural disaster.

5. CONCLUSIONS

Nowadays, cloud computing is very popular because of its flexibility and cost effectiveness. Since there are many hackers and malicious users over the internet, data access control is a very challenging issue in cloud computing. The main problem takes place, when users want to access data or file from outside their domain. In the first part of this paper, fundamentals of cloud computing are discussed. Many security issues of cloud computing are discussed in this paper, namely availability, confidentiality, access control, data related issues, storage related issues, policy issues, security issues, trust issues, legal aspects and attacks on the cloud environment. Moreover, future work directions are also presented in this paper. In future, a new access control model can be developed for an efficient and secure data accessing among the CSP, DO and user.

6. REFERENCES

[1] Schouten, E.: Cloud computing defined: characteristics & service levels. Available online at http://thoughtsoncloud.com/2014/01/cloud-computing-defined-characteristics-service-levels/ (2014)

[2] Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., Leaf, D.: NIST cloud computing reference architecture. NIST special publication 500-292 (2011)

[3] Zhang, Q., Cheng, L., Boutaba, R.: Cloud computing: state-of-the-art and research challenges. J. Internet Services and Applications. **1**(1), 7-18 (2010)

[4] Queensland Government. Benefits of cloud computing. Available online at https://www.business.qld.gov.au/business/running/technology-for-business/cloud-computing-business/cloud-computing-benefits

[5] Tsagklis, I.: Advantages and disadvantages of cloud computing-cloud computing pros and cons. Available online at http://www.javacodegeeks.com/2013/04/advantages-and-disadvantages-of-cloud-computing-cloud-computing-pros-and-cons.html (2013)

[6] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A view of cloud computing. Commun. of the ACM. **53**(4), 50-58 (2010)

[7] Namasudra, S., Nath, S., Majumder, A.: Profile based access control model in cloud computing environment. In: Proceedings of the International Conference on Green Computing, Communication and Electrical Engineering, pp. 1-5. IEEE, Coimbatore, India (2014)

[8] Anthes, G.: Security in the cloud. Commun. of the ACM. **53**(11), 16-18 (2010)

[9] Khan, A.R.: Access control in cloud computing environment. ARPN J. of Engineering and Applied Sciences. **7**(5), 613-615 (2012)

[10] Anderson, R.: Technical perspective: a chilly sense of security. Commun. of the ACM. **52**(5), 90-90 (2009)

[11] Namasudra, S., Roy, P.: Secure and efficient data access control in cloud computing environment: a survey. Multiagent and Grid Systems-An International Journal. **12**(2), 69-90 (2016)

[12] Majumder, A., Namasudra, S., Nath, S.: Taxonomy and classification of access control models for cloud environments. In: Mahmood, Z. (Ed.) Continued Rise of the Cloud, pp. 23-53, Springer, London (2014)

[13] Namasudra, S., Roy, P.: A new secure authentication scheme for cloud computing environment. Concurrency and Computation: Practice and Exercise. **29**(20), (2017). DOI: 10.1002/cpe.3864

[14] Kandukuri, B.R., V, R.P., Rakshit, A.: Cloud security issues. In: Proceedings of the International Conference on Services Computing, pp. 517-520. IEEE (2009)

[15] Naik, N.D., Modi, K.J.: Evolution of IT industry towards cloud computing: a new paradigm. IJRIT Int. J. of Research in Information Technology. **1**(5), 236-242 (2013)

[16] Harauz, J., Kaufman, L.M., Potter, B.: Data security in the world of cloud computing. IEEE Computer and Reliability Societies. 61-64 (2009)

[17] Savolainen, E.: Cloud service models. In: Seminar-Cloud Computing and Web Services. University of Helsinki. Department of computer science (2012)

[18] Dooley, B.J.: Architectural requirements of the hybrid cloud. Available online at http://www.information-management.com/news/hybrid-cloudarchitectural- requirements-10017152-1.html (2010)

[19] Morsy, M.A., Grundy, J., Müller, I.: An analysis of the cloud computing security problem. In: Proceedings of APSEC Cloud Workshop. Sydney, Australia (2010)

[20] A platform computing white paper. Enterprise cloud computing: transforming IT. In: Platform computing (2009)

[21] Marinos, A., Briscoe, G.: Community cloud computing. In: Proceedings of the 1st International Conference on Cloud Computing (CloudCom 2009). Beijing, China (2009)

[22] Global Netoptex. Demystifying the cloud-Important opportunities, crucial choices (2009)

[23] Namasudra, S.: An improved attribute-based encryption technique towards the data security in cloud computing. Concurrency and Computation: Practice and Exercise. (2017). DOI: 10.1002/cpe.4364

[24] Namasudra, S., Roy, P., Balamurugan, B.: Cloud computing: fundamentals and research issues. In: Proceedings of the 2nd International Conference on Recent Trends and Challenges in Computational Models, IEEE, Tindivanam, India (2017)

[25] Deka, G. C., Das, P. K.: An overview on the virtualization technology. *Handbook of Research on Cloud Infrastructures for Big Data Analytics*, **289** (2014)

[26] Namasudra, S., Roy, P.: Time saving protocol for data accessing in cloud computing. IET Communications. **11**(10), 1558-1565 (2017)

[27] Namasudra, S., Roy, P., Balamurugan, B., Vijayakumar, P.: Data accessing based on the popularity value for cloud computing. In: Proceedings of the International Conference on Innovations in Information, Embedded and Communications Systems (ICIIECS), IEEE, Coimbatore, India (2017)

[28] Deka, G. C., Kathing, M., Kumar, D. P.: Library automation in cloud. In: Proceedings of the International Conference on Computational Intelligence and Communication Networks. IEEE, Mathura (2013)

[29] Namasudra, S., Roy, P.: Size based access control model in cloud computing. In: Proceedings of the International Conference on Electrical, Electronics, Signals,

Communication and Optimization, pp. 1-4. IEEE, Visakhapatnam, India (2015)

[30] Namasudra, S., Roy, P.: A new table based protocol for data accessing in cloud computing. Journal of Information Science and Engineering. **33**(3), 585-609 (2017)

[31] Deka, G. C., Borah, M. D.: Cost benefit analysis of cloud computing in education. In: Proceedings of the International Conference on Computing, Communication and Applications. pp. 1-6 (2012)

[32] Namasudra, S., Roy, P.: PpBAC: popularity based access control model for cloud computing. Journal of Organizational and End User Computing. (2018)

[33] Sarkar, S., Saha, K., Namasudra, S., Roy, P.: An efficient and time saving web service based android application. SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE), **2**(8), 18-21 (2015)

[34] Namasudra, S., Roy, P., Vijayakumar, P., Audithan, S., Balamurugan, B.: Time efficient secure DNA based access control model for cloud computing environment. Future Generation Computer Systems. (2017). DOI: http://dx.doi.org/10.1016/j.future.2017.01.017

[35] Regulation of Investigatory Powers Act 2000, Part II, UK. Available online at http://www.legislation.gov.uk/ukpga/2000/23/part/II

[36] USA patriot Act of 2001. Available online at http://www.ratical.org/ratville/CAH/Section501.html

[37] Shuijing, H.: Data security: the challenges of cloud computing. In: Proceedings of the 6th International Conference on Measuring Technology and Mechatronics Automation, pp. 203-206. IEEE (2014)

[38] Brender, N., Markov, I.: Risk perception and risk management in cloud computing: results from a case study of Swiss companies. Int. J. of Information Management. **33**(5), 726-733 (2013)

[39] Hashizume, K., Rosado, D.G., Medina, E.F., Fernandez, E.B.: An analysis of security issues for cloud computing. J. of Internet Service and Application. **4(**5), 1-13 (2013)

[40] Rastogi, I., Chandra, A., Gupta, V.K., Vaish, A.: Privacy issues and measurement in cloud computing: a review. Int. J. of Advanced Research in Computer Science. **4**(2), 81-86 (2013)

[41] Fratto, M.: Internet evolution: cloud control. InformationWeek. Available online at http://reports.informationweek.com/abstract/5/729/Cloud-Computing/INTERNET-EVOLUTION:-Cloud-Control.html (2009)

[42] Reidenberg, J.R.: Technology and internet jurisdiction. University of Pennsylvania Law Review. **153**, 1951-1974 (2005)

[43] Security guidance for critical areas of focus in cloud computing V2.1. Cloud security alliance (2009)

[44] Mckinley, P.K., Samimi, F.A., Shapiro, J.K., Tang, C.: Service clouds: a distributed infrastructure for constructing autonomic communication services. In: Proceedings of the 2nd International Symposium on Dependable, Autonomic and Secure Computing, pp. 341-348. IEEE, Indianapolis, IN (2006)

[45] Top threats to cloud computing v1.0. Cloud Security Alliance (2010)

[46] Bertino, E., Paci, F., Ferrini, R., Shang, N.: Privacy-preserving digital identity management for cloud computing. IEEE Technical Committee on Data Engineering. **32**(1), 21–27 (2009)

[47] Ristenpart, T., Tromer, E., Shacham, H., Savage, S.: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 199-212. ACM, New York, USA (2009)

[48] Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not so different after all: a cross-discipline view of trust. Academy of Management Review. **23**(3), 393-404 (1998)

[49] Nissenbaum, H.: Can trust be secured online? A theoretical perspective (1999)

[50] Crane, S., Tweney, A.: Trustguide2: an exploration of privacy preferences in an online world. In: Cunningham, P., Cunningham, M. (Eds.) Expanding the Knowledge Economy: Issues, Applications, Case Studies. IOS Press, Amsterdam (2007)

[51] Mearian, L.: No, your data isn't secure in the cloud. Available online at http://www.computerworld.com/article/2483552/cloud-security/no--your-data-isn-t-secure-in-the-cloud.html (2013)

[52] Guidelines governing the protection of privacy and transborder flow of personal data. Organization for Economic Co-operation and Development (OECD). Geneva.

[53] PGP Compliance Brief. E.U. data protection directive 95/46/EC (2008)

[54] Bhadauria, R., Chaki, R., Chaki, N.: A survey on security issues in cloud computing. Cornell University Library, USA. Available online at http://arxiv.org/abs/1109.5388 (2013)

How to cite this article:
Namasudra S.Cloud computing: a new era. J. Fundam. Appl. Sci., 2018, *10(2), 113-135.*