Cloud computing literature review computer science

[Michael et al. 2010] Cloud computing is the IT liberation model that provides infrastructure and computer resources as service. In an organization, the information is shared by implementing the private cloud. The achievement of an organization is based on the important advantages such as simplifying management, reducing costs and accelerating processes. In a broad diversity of designs, the cloud computing technologies can be implemented under different services and deployment methods. In the organization cloud computing is used to transfer the existing server infrastructures into dynamic environments. By adopting the cloud computing, the business activities can be carried out with little difficulty and greater efficiency. Cloud computing offers many advantages to different ranges of customers and it is simple to acquire.

By considering the above views of authors it can be concluded that, cloud computing is IT delivery model and it gives the infrastructure and computer resources. By implementing the cloud, the information can be shared. Simplifying management, reducing costs and accelerating process such advantages provides success to the organization. Based on different services and deployment methods, the cloud computing technologies can be implemented in a broad diversity of designs. This provides many advantages for different ranges of customers and these advantages are simple to obtain. Through adopting the cloud computing, business activities can be done with great efficiency and little hassle.

[Meiko et al, 2009] Generally, cloud computing provides the dynamical and scalable resources as a service over the internet. Cloud is used for reducing the capital and operational expenditure, and provides economical growth.

This is happened in realism and however, there are some confronts are explained by the cloud. It is described as a valuable consideration for an enterprise IT integration. Even the adoption of cloud computing has many advantages and still it faces a number of risks. The security of cloud is one of the important issues in the cloud computing.

By considering the above views of authors it can be concluded that cloud computing provides dynamical and scalable resources over the internet. Cloud provides economic growth and reduces the capital and operational expenditure. It defines as a valuable consideration for IT integration. It has a number of advantages but still it faces some risks. Sometimes cloud cannot provide security for the customer’s property. It considers important disadvantages of cloud computing.

[Chang et al, 2005] Usually, in the cloud computing, the significant data of the customer can be stored in data centers. Actually, Data centers means where the data should be stored on the centralized location by having a large size of data storage. The data processing is done on the servers. The important data should be handled by the cloud provider. Therefore, the customers have to trust the cloud provider on the data security as well as on availability. For this, the legal agreement which is called as SLA (service legal agreement) should be provided by cloud computing between cloud customer and cloud provider. The provider can gain trust of the client through this agreement, so, SLA should be consistent. In the cloud environment, the whole security depends on the security levels of the cloud. This concept of cloud computing is promising to change the future of the computing by

providing many benefits in the field. And the main obstacle in achieving this is nothing but the disadvantage of the security concern.

From the above views of authors it can be concluded that, generally, in the cloud computing, the data will be stored in the data centers. Data storing methods are being done on the data servers. A large si9ze data can be stored in the data centers. In the cloud computing, the data of customer should be handled by the cloud provider. Therefore the cloud providers should give the guarantee on the data security. To have trust on the cloud provider, the cloud customer should follow the legal agreement which is called as SLA that should provided by cloud computing between cloud customer and cloud provider.

[McKinsey, 2009] Basically, cloud computing is the self motivated specification of the IT capabilities (hardware, software, or services). Clouds are hardware based services that offers computing, networking and storage capacity. It has exclusive features that need risk measurement in parts such as data honesty, revival, and privacy. A security perimeter is set up to create a trust boundary where customer’s valuable information is stored and proceed. The network provides transportation to which works in a similar manner, and which consist of other trusted end hosts. The confidential information may be processed outside and identifies trusted areas as these computing environments often have unclear boundaries as to where data is stored and processed and when the security perimeter becomes unclear in the sense. Privacy issues which frequently happen in the cloud are not only raised by public cloud and also have its own security concerns.

By considering the above views of authors it can be concluded that clouds are hardware based services which offers computing, networking and storage capacity. Particularly, in some parts such as data honesty, revival and privacy it has exclusive aspects which need risk measurement. A security border is used to create a trusted boundary where customer's valuable information is stored and secured. The network which includes the cloud is used to transport the trusted end hosts which work in the similar manner. Public cloud is not only reason for the privacy issues which regularly happen in the cloud computing and also have it share of security concerns.

2. 2. Different sections of cloud computing:

[Rob, 2008] the cloud computing is divided into three sections namely cloud application, cloud platform, and cloud infrastructure. These sections can be represented as the " cloud pyramid" in the cloud computing.

Cloud application:

[Rob, 2008] the cloud application is the first section that presents in the top of the pyramid. According to the cloud application, the interaction of the applications via web browser is taken place in the cloud computing. Through the cloud application, the need to install and run the application on the customer's own computer can be eliminated. It reduces the difficulty for the customer to maintain the software and its process.

From the above discussion it can be concluded that in the cloud computing pyramid, three sections are there namely cloud application, cloud platform and cloud infrastructure. Cloud application is the first section in the cloud

pyramid and used to communicate the applications with each other via web browser. It used to reduce the difficulty for the customer in maintaining the software and its process.

Cloud platform:

[Rob, 2008] Usually, the theoretical work as a service or the calculating platform is provided by the cloud platform. This is the second section and the middle layer of the cloud pyramid. As indicated by the requirement, the cloud platform offers the animatedly necessities, configures and reconfigure servers.

From the above views of the authors it can be concluded that cloud platform is used to calculate the platform and the framework as a service. This is the second section in cloud computing pyramid. The animatedly necessities, configures and reconfigure servers are provided by this section. And this is the middle section of the cloud pyramid.

Cloud infrastructure:

[Rob Lovell 2008] cloud infrastructure is the last layer of the cloud pyramid. It delivers the IT infrastructures by means of the virtualization. Through the cloud infrastructures, the splitting of the hardware into independent and self ruled environments can be completed. The services that are delivered as the web services or farms or cloud centers and other hardware appliances are included in the cloud infrastructure.

Source: Rob Lovell, 2008, “ introduction to cloud computing”- white papers.

From the above discussion it can be concluded that cloud infrastructure is the last section of the cloud pyramid and it delivers the IT infrastructures through the virtualization. By using this section, self ruled environments can be completed. Web services or farms or cloud centers and other hardware appliances are included in the cloud infrastructure.

2. 2. Security issues in the cloud computing:

[Jensen et al, 2009] the cloud is provided responsibility for the security of the data when the user is released the data into the cloud. It has some issues in their operation which are explained as follows:

2. 2. 1. Operational security:

[Jensen et al, 2009] The property of the organization can be uncovered which causes a major drawback in the security point of view throughout the cloud operation. The critical information of the company may be leaked and may cause the data exposures. The cloud may not be managed to sufficient standards in the cloud computing. The defensive of the data may not be secured in a proper way in the clouds then it causes for the security issues. Among the customer and the provider a complete security management system must be developed. It can be protects the data from hacking by third parties.

By considering the above views of authors it can be concluded that generally cloud provides responsibility for secure the customer’s valuable information. But sometimes it faces some problems when data transfers into the cloud. Operational security is one of the major issues in the cloud computing.

Through the cloud operation, the property of the organization can be unsecured. The cloud may not ensure to sufficient standards in the cloud computing. Through this type of security issues, the protecting of the information may not be done in a proper way in the clouds. This security management system must be developed between customer and provider. Then it can be protects the data from the hackers.

2. 2. 2. Privacy:

[Siani et al, 2010] The service supplier of the cloud should be able to give the declaration of the vital data. And they make sure that any unpermitted person cannot view or access the confidential data or the information of the user.

From the above views of authors, the service providers have to give guarantee about the valuable information and make sure that any unpermitted person cannot view or access the private information of their customer.

2. 2. 3. Reliability:

[Siani et al, 2010] The modification of the innovative data or any efforts to alter the data should be severely prohibited by the provider and this make sure that the data detained in the system of the cloud is proper and used to maintain the integrity.

2. 2. 4. Accessibility:

[Siani et al, 2010] The entire resources which are needed by the user for processing the data should be accessible and this should not be made unavailability at any chance by the interference of the outsiders or the spiteful actions of the unauthorized persons.

2. 2. 5. Non-Reputation:

[Siani et al, 2010] It is make sure that the agreements which are created automatically between the organizations or authorized persons and the officials should have been created to be confirmed if necessary.

The security is needed at various levels in the organizations. The requirement is about the access to server, internet, database and the programs. The service supplier of the cloud should be ensured that the privacy of the data is well preserving.

From the above views of authors it can be concluded that reliability, accessibility and non-reputation are common issues in the cloud computing security point of view. Modification of the innovative data ca be prohibited by the provider and this data should be used in proper way to maintain the integrity in the cloud. The complete resources which are needed by the user for processing the data should be accessible. This should not be created unavailability at any chance by the interference of the outsiders.

2. 2. 6. Other issues:

[Steve, 2008] In a traditional enterprise environment, there are a number of tools which have been already developed for attaining the security in computer, storage and network. The data of the users is processed and co-

located on the shared equipment in the concept of cloud computing. Basically, cloud computing can implemented in any type of the companies such as large medium and small and even startup companies. The given specific threats are caused for cloud security issues. The significant issues of securities are related by which parties are responsible for which features of security. Through the customer data security, some problems are raised such as the risk of loss, unauthorized collection and problem in usage of that.

From the above views of authors it can be concluded that, according to usual project environment, there are a number of tools that have been previously developed for achieving the security in computer, storage and network. In the thought of cloud computing, the data of the users is developed and co-located on the communal tools. Cloud computing is used in any type of the companies such as large, medium, and small. Security issues in the cloud computing are caused by under given threats.

Failures in the security provision:

[Steve, 2008]The data is stored and the applications are run on the hardware and hypervisors and these are controlled by the cloud. The security of the cloud provider should be at very good standards.

Form the above views of authors it can be concluded that, storing the data and the operation of applications are controlled by cloud and it employs based on the hardware and hypervisors. The cloud provider should have very good standards in the sense of security.

Other customers attack:

[Steve, 2008]All the customers inside of the cloud or connected with the cloud can be shared the data in the cloud environment. Access of the data or the interference of the data by other users can be possible at any chance if the barriers break down between the users.

From the above views it can be concluded that, the customer of the cloud shares the data in the cloud environment. When the barriers break down between the users then interfering of the data or access of the data can be possible at any chance.

Legal and regulatory issues:

[Mather, 2009] Many legal and regulatory issues are being raised by implementation of the cloud computing techniques. There might be a restriction in the export of the data in an authority. In any cases such sensitive issues happened in cloud computing, there legal and regulatory problems should be addresses and resolved.

By considering the above views of authors it can be concluded that, by implementing the cloud computing techniques in any organizations, many legal and regulatory issues are being raised. Legal and regulatory issues are happened hen the common issues raised.

Perimeter Security Model Broken:

[Mather, 2009] To have strong security at the perimeter of the enterprise network, the model of the perimeter security is being employed by most of the organizations. Over the years, this model has been failing with outsourcing and workforce as well as with high mobility. Some critical data

and the applications can be stored by the cloud now even though it is certainly outside the perimeter of the enterprise.

From the above views of authors it can be concluded that, the model of the border security is being employed by most of the organizations to have strong protection at perimeter of the enterprise network. From the past years, this model has been failing with high mobility, workforce as well as with outsourcing.

2. 3. Fuzzy key word search in cloud computing:

[Jin Li et al 2008] the unclear (fuzzy) key word search is widely prolonged the system usability via giving back the same files when the user’s penetrating contributions equals the predefined keywords accurately or the nearby believable corresponding files are dependent on keyword similarity semantics when specific match becomes ineffective.

By considering the above views of authors it can be concluded that, the fuzzy keyword is extensively protracted the system usability by means of giving back the alike files when the users penetrating contributions equals the predefined keywords correctly. Otherwise, if the specific match becomes ineffective, the nearby credible matching files are needy on keyword similarity semantics.

2. 4. Plain text fuzzy keyword search:

[Li et al, 2008] The significance of the fuzzy search has increased focus in the conditions of the plain text search in information recovery zone. This problem has been documented in the classical information access paradigms

through providing the user to search without trying and study the technique for determining the applicable data based on the predictable string corresponding. Therefore, the estimated string corresponding algorithms between one and another can be classified into two sections such as on-line and off-line.

From the above views of authors it can be concluded that, in the plain text fuzzy keyword search, some problems are happened such as the significance of the fuzzy search has focus in the conditions of the plain text search in information recovery zone. Therefore, through providing the user to search without trying and study the technique for determining the suitable data based on the predictable string corresponding, this problem has been documented in the conventional information access paradigms. The estimated corresponding algorithms between one and other can be classified into two sections such as online and offline.

[Chakrabart et al, 2006] However, according to the on-line techniques, the method of doing search without the participation of index seems to be unwanted for their short explores capability while the off-line technique employs indexing techniques for generating it to be completely faster. There is a number of indexing algorithms such as suffix trees, metric trees and q-gram methods and so on. On the first look, it is attainable for the user to describe these string matching algorithms are explicitly to the viewpoint of the searchable encryption through evaluating the trapdoors on the nature support locating in an alphabet. But, this insignificant structure will experience attacks connected with dictionary and statistics and somehow ineffective to achieve the search privacy.

By considering the above views of authors it can be concluded that, in the sense of online techniques, the method of doing search without performance of index seems is unwanted for their short explore of capability. This method is done while the offline technique uses indexing techniques for generating it to be faster. It has a number of indexing algorithms such as suffix trees, metric tress, and q-gram methods and so on. But the important structure can be experienced which attacks connected with index and statistics.

2. 5. Searchable encryption:

[Curtmola et al, 2006] The previous searchable encryption methods have been extensively evaluated in the cryptography conditions. These works are majorly focused on the security definition formalizations and efficiency developments. In the early creation, each statement in the text is encrypted independently in a two covered encryption structure. Behind them, bloom filters approached into existence in order to create the indexes for the data files.

[Bellare et al, 2007] This technique is developed and accumulated on the server for every file which consists of the trapdoors of overall words. In order to search for a word and finally sends it to the server, the user has to create the search request through evaluating the trapdoor of the word. After getting the request, the server checks whether any bloom filter have the trapdoor of the query word or bounces back the equal file recognizers.

By considering the above views of authors it can be concluded that the earlier searchable methods are widely calculated in the cryptography circumstances. Theses works are significantly focused on the security

definition formalizations and efficiency developments. In the previous generation, every statement in the text is encrypted independently in a two covered encryption structure. After that, bloom filters move towards into existence in order to create the indexes for data files. For each file, this method is developed and accumulated on the server which consists of the trapdoors of overall words. The user has to create the search request through measuring the trapdoor of the word in order to search for a word and finally sends it to the server.

[Waters et al, 2004] Similar “ index” techniques should be projected for achieving more successful search. This technique created a single encrypted confusion table index for the overall file compilation. Every entry has an encrypted group of file identifiers whose equivalent data files contain the keyword in the index table. And it has the trapdoor of a keyword. A Public - key based searchable encryption technique is also developed as a complementary approach for the first one. Though, these are not considered due to the issues with the agreement of the users. In fact, they are applicable for cloud computing as these whole current techniques assist just accurate keyword search.

By considering above views of authors it can be concluded that, for accomplishing more successful search, similar “ index” techniques should be projected. For overall file completion, this technique created a single encrypted confusion table index. In the index table, each entry has an encrypted group of files identifiers whose equal data files contain the keyword. And also it has the trap door of key word. Key based searchable encryption technique is also urbanized as balancing approach for the first

one. However, these are not considered as a development, due to the issues with the agreement of the users. In fact, they are related for cloud computing as these whole current techniques help as accurate keyword search.

[Shi et al, 2007] The confidential matching data in the conditions of the secure multi-party calculation is used to allow dissimilar parties in reviewing some function of their individual data without revealing their data to others collaboratively. These functions have the connection or approximate private matching of the two different sets. However, this technique is frequently employed method to recover the correspondent sets in secret. This has been widely employed in data retrieval from database and it usually acquires calculation complexity randomly.

From the above views of authors it can be concluded that, the private corresponding data is used to permit different parties in reviewing some functions of their individual data without revealing their data to others in conditions of the secure multi party calculations. These functions have the approximate matching or the connection between two different sets. However, to recover the correspondent sets in confidential; this technique is frequently employed method. It is usually acquires calculation complexity randomly and it has been widely employed in data retrieval from data base.

2. 6. Advanced techniques for building fuzzy key words:

[Chow et al, 2009] Highly developed techniques are used to provide more sensible and efficient fuzzy keyword search constructions which include storage and search efficiency. They are mostly projected to expand the

uncomplicated approach for structuring the unclear keyword set. The scholars concerted on the case of edit distance d= 1 without loss of generalization in this technique. The calculation is same for better values of'd'. This technique is carefully designed in such a way that it will not force the search accuracy while restraining the unclear keyword set.

In accordance with the above observations, wild card based fuzzy set construction is developed in order to signify correct operations at the equal location. To avoid security issues in cloud computing, wild card based, gram based and symbol based fuzzy key words are used.

From the above views of authors it can be concluded that, in avoiding security issues in cloud computing, wild card based, gram based and symbol based fuzzy key words can be used. More sensible and efficient fuzzy keyword search creations are provided by highly developed techniques which include storage and search efficiency. Basically, they are mostly projected in developing the simple approach to create the fuzzy keyword set. The researchers concentrated on the case of edit distance d= 1 without defeat of simplification in this method. The computation is similar for improved principles of'd'. Through this method, wildcard based fuzzy set structure is developed in order to mean right operations at the equal site.

2. 6. 1. Wildcard-based Fuzzy Set construction:

[Song et al, 2000] A wild card based fuzzy set construction techniques are projected to signify the correct operations at the same position. The unclear or fuzzy set of wi signifies as Swi, d={SA? a,¬A? wi, 0, SA? a,¬A? wi, 1, A·A·A· , SA? a,¬A? wi, d} with its edit distance ' d', where SA? a,¬A? wi, A?

aˆz signifies the set of words wA? a,¬A? i with A? aˆz wildcards. The correct operation on wi is accepted by each wildcard. It is completely described by considering the equation. For example, the words CASTLE with the pre-set of correct distance d= 1 and its wildcard fuzzy key word is constructed as following:

The storage in the clouds can be decreased based on the pre-set edit (accurate) distance d= 1. When the correct distance is set 2, then the representation of size Swi, 2 will be

When the correct distance is set to 3, then the representation of size Swi, 3 will be

By considering the above equations it can be concluded that, wildcard based fuzzy set structure is developed in order to mean right operations at the equal site. The accurate operation is accepted by this each wildcard. It is completely considered from the above equation. The data storage of the clouds can be decreased based on the pre-set edit distance d= 1. The representation of size is based on their edit distances.

2. 6. 2. Gram based fuzzy set construction:

[Behm, 2009] gram based creation is one of another efficient technique which is used to build the fuzzy set. The gram of the string is a substring which is used as a signature for the efficient estimated search. These grams are used for the matching purpose. The sizes are represented as follows:

==

For the keyword CASTLE, the fuzzy word set can be created as follows:

{CASTLE, CSTLE, CATLE, CASLE, CASTE, CASTL, ASTLE}

By considering the above views of authors it can be concluded that, to create the fuzzy search set, this gram based fuzzy set construction is one of another best techniques. To use as a signature for the efficient estimated search, this creation of the string is considered as the substring. For the corresponding purpose these grams can be used.

2. 6. 3. Symbol-based Trie-traverse search scheme:

[Feigenbaum, 2001] for improving the search efficiency, a symbol based trie-traverse search scheme is developed. A multi way tree is created for storing the fuzzy keyword set over a limited symbol set. The main reason behind the creation of the symbol based trie traverse search scheme is all the trapdoors sharing the common prefix and that may have common nodes. The symbols which involves in a trapdoor can be improved in a search from the root to the leaf at where the trapdoor ends. An empty set is present at the trapdoor then symbols can be recovered.

By considering the above views of authors it can be concluded that, a symbol based trie-traverse search scheme is developed to expand the search efficiency. For storing the fuzzy keyword set over a limited symbol set, a multi way tree is created. The symbols can be recovered when any empty set is present at the trapdoor.

2. 7. An efficient fuzzy keyword search scheme:

[Boneh et al, 2004]The following points to be considered in order to build the efficient key word search scheme. They are stated below:

At first, the information holder creates an unclear keyword set Swi, d to create the index for wi using the wildcard based technique. After that it needs to compute trapdoor set {Twi} for each wi’ AZAμ S wi d with a secret key Sk shared data holder and the certified users. The data holder encrypts FID wi as,.. Though, the directory table and locked data files are outsourced to the cloud server for storage the data.

The approved user computes the trapdoor set to search with w and k in which S w, k is also derived from the wildcard based fuzzy set structure. Then users send to the server. The server evaluates them with the locked file recognizer’s upon getting the search request. At the end, the user recovers appropriate files of interest and unlocks the returned results.

[Bao et al, 2008] The method of creating search request for ‘ w’ is matching to the creation of directory for a keyword in this onset. Thus, the search request is a trapdoor set needy on S w, k as an choice of a single trapdoor as in the straightforward method. In this way, the searching result accuracy can be assured.

From the above views of author it can be concluded that, to create an efficient fuzzy key word search, above given two points would be considered. They are: the first one is fuzzy keyword is created by the information holder. And the second one is the accepted user computes the trapdoor set to search with wildcard based fuzzy keyword structure.

2. 8. Conclusion:

Cloud computing is the IT liberation model which offers infrastructure and computer resources as service. Through take up the cloud computing, business activities can be carried out with little difficulty and greater efficiency. Cloud computing provides many advantages to various ranges of customers and it is simple to acquire. Generally, cloud computing provides the dynamical and scalable resources as a service over the internet. Cloud is used for reducing the capital and operational expenditure, and provides economical growth. Even the adoption of cloud computing in organizations has many advantages and still it faces a number of risks. In the cloud computing, the significant data of the customer can be stored in data centers.

The cloud computing is divided into three sections namely cloud application, cloud platform, and cloud infrastructure. It has some issues in their operation they are: operational security, privacy, reliability, accessibility, non reputation, failures in the security provision, other customer attacks, legal and regulation issues, and perimeter security model broken. The fuzzy keyword is extensively prolonged the system usability by means of giving back the alike files when the users penetrating contributions equals the predefined keywords correctly. The significance of the fuzzy search has increased focus in the conditions of the plain text search in information recovery zone.

The confidential matching data in the conditions of the secure multi-party calculation is used to allow dissimilar parties in reviewing some function of

their individual data without revealing their data to others collaboratively. Highly developed techniques are used to provide more sensible and efficient fuzzy keyword search constructions which include storage and search efficiency. To avoid security issues in cloud computing, wild card based, gram based and symbol based fuzzy key words are used.