DJ Journal of Advances in Electronics and Communication Engineering, Vol. 1(2) 2015, pp. 12-23

REVIEW ARTICLE

Cloud Computing: Characteristics, Issues and Possible Security Solutions - A Review

[*]M Julie Emerald Jiju[1], E Arun[2]

[1]Assistant Professor, Department of MCA, CSI Institute of Technology, Thovalai, Kanyakumari, Tamil Nadu, India.

[2]Professor, Department of Computer Science and Engineering, Ponjesly College of Engineering, Tamil Nadu, India.

Received-7 October 2015, Revised-5 November 2015, Accepted-25 November 2015, Published-28 November 2015

ABSTRACT

Cloud computing is one of the research areas where a large amount of studies and investigations are going on. With the advent of technology the security concerns and issues related to cloud computing are on the rise and thus they require a serious attention. In this article we have attempted a review of the cloud computing scenario; their characteristics, issues and possible solutions. The types of cloud computing can be classified as public, private and hybrid cloud computing. The services and characteristics of cloud computing are presented with a special mention to resource pooling, flexibility, accessibility, measurability and on demand cell service. The issues in cloud computing are provided with emphasis on storage security and distributed denial of service. Three methods viz data classification, layered frame work and Attribute Based Encryption (ABE) have been presented as the viable methods for improved security in cloud computing. Next the usage of cloud computing in malware detection is outlined. Finally general measures for improving security in cloud computing is discussed.

Keywords: Resource Pooling, Storage Security, Data classification, Layered frame work, Attribute based encryption**.**

1. INTRODUCTION

Cloud computing can be defined as a technique in which servers which are placed at remote locations on the internet facilitate storing, processing and managing data instead of a local server or a PC. It is also known as on-demand computing as it provides services on demand. Cloud computing varies considerably with respect to grid computing and utility computing. It is similar to electricity where the customers can use them as a utility rather than constructing the entire infrastructure needed. Users need to pay only for the services they use. Measurement is made at the granular level. The major goal of cloud computing is to provide high performance similar to supercomputing applications. There are several benefits of cloud computing including centralized data storage, improved bandwidth, elasticity and self-service positioning. They are remotely hosted, ubiquitous and commoditised. Thus cloud computing is an enabling emerging technology. In short cloud computing can be defined as a broad term which is used for referring internet based development and services. The real value of a cloud is that it unambiguously makes data, software and computing techniques available everywhere.

1.1. Types of cloud computing services

There are three types of cloud computing services viz

1)Public cloud computing

2)Private cloud computing and

3) Hybrid cloud computing.

In a public cloud computing model, the resources are made available to the general public. It may be either free or paid. They are cheap as the costs are met by the provider.

*Corresponding author. Tel.: +91919442037244

Email address: jijudiaz45@gmail.com (M.J.E.Jiju)

Double blind peer review under responsibility of DJ Publications

http://dx.doi.org/10.18831/djece.org/2015021002

Resources are not wasted as only the used resources are paid. Private cloud possesses a proprietary architecture. Private cloud serves only a single organization whereas the public cloud is dedicated to multiple organizations. The organization has a direct control over the data. It provides the same advantages of public computing including scalability and multi-tenancy. However the main disadvantage is that they require the same handling cost for a single organization as that of multiple organizations in a public cloud model. Hybrid cloud model is a mix of public cloud and private cloud models. They possess greater flexibility. Hybrid cloud model requires network connectivity and Application Program Interface (API) compatibility. A transactional order system that experiences demand spikes is a typical example of a hybrid cloud.

1.2. Service categories of cloud computing

The categories of cloud computing services can be broadly classified in to the following three types

1)Infrastructure as a Service (IaaS)
2)Platform as a Service (PaaS)
3)Software as a Service (SaaS)

In a Saas the client devices can access various applications. This is facilitated by means of a client interface such as web browsers. The customers do not have control over the networks, operating systems, storage etc., Saas reduces the workload related to maintenance and support of software. The applications are located inside the cloud and internet is made use for delivering software experiences. SalesForce CRM and LotusLive are examples of SaaS service providers. PaaS allows users to develop, modify, debug and control applications without constructing and maintaining the infrastructure. Higher programming levels can be achieved with fewer complexities. They are used when the developers want to create a service but do not want to create their own cloud. Google App and Windows Azure are Paas service providers. In IaaS a user can run operating systems and applications. The service providers make service data centres such as power, scale, networking, storage, hardware, distributed systems etc. The users rent storage, computation and maintenance from service providers. The customers can check and control operating systems, applications and network components. Amazon web services and rackspace Hosting are examples of IaaS service providers. Figure A1 gives a model of cloud computing.

One of the main challenges that cloud computing faces is security. As data forms a major component of the cloud computing services the protection of data from unethical hacking is an area of concern. First we discuss about the different issues that the cloud computing environment faces and then we study about three applicable solutions for improving security in cloud systems.

2. BACKGROUND AND RELATED WORK

[1] emphasizes that cloud computing is the top most one among the current forms of technology. It is gaining importance day by day and may become a prominent and most sought out technology in the near future. The main goal of cloud computing is to provide faster, secure and appropriate data storage along with good computing service. Here the services are regarded as resources transported over the internet [2]. Cloud computing facilitates a low cost alternative to in-house infrastructure. The system applies for both hardware and software. Computing is at the core of a cloud and by means of it the factors such as cost reduction, time for meeting of demands, scalability and speedability is increased [3]. Cloud computing makes use of different technologies including virtualization and dependence on internet to satisfy the demands of the customers. In any case the data are stored in servers [4].

There are several hurdles which prevent the satisfactory implementation of cloud computing in an efficient way the main one being security. Others include hindering privacy and legal matters [5]. Cloud computing is one of the newly evolving models and hence the reliability of such a model is questioned to a great extent. Many users put forward the question of security which made the information executives to state that security is their major concern [6]. The major security concerns are associated with data storage. In many user friendly technologies authorization, authentication and cryptography are employed in order to improve the security concerns. But in an evolving cloud computing scenario it is of less interest and sophisticated methods need to be adopted [7]. The underlying fact is that many

corporates do not want their exclusive data to go out in a public environment. Moreover the users must feel that their data is safe with a service provider and they can achieve their desired performance aspect [8, 9]. [10] discussed about security concerns that are important for a cloud computing model. There is a potential risk in exposing data to an external platform. Accountability is another one concern especially in the case of auditing services. Storage space, data separation, recovery, investigation and long term viability are the other important areas of concern. [11] suggested methods such as management and standardization for guiding users as well as cloud engineers. Cloud computing introduces some new risks, modifies others and influences some existing problems. [12] focused on standardizing the cloud services security as cloud services has emerged as one of the advanced technologies. Security Level Agreement (SLA) agrees clear guarantee and certainty among cloud users. Presence of malware in the cloud computing environment is an important security concern which needs to be discussed [13].

3. CHARACTERISTICS OF CLOUD COMPUTING

The characteristics of cloud computing can be classified in to two types viz common characteristics and essential characteristics. The common characteristics include massive scale, resilent computing, homogeneity, geographic distribution, visulaization, service orientation, low cost software and advanced security. The essential characteristics are the important characteristics of cloud computing which makes them different from the traditional computing techniques [14, 15]. They are

- Resource Pooling
- Flexibility
- Accessibility
- Measurability
- On-demand self-service

3.1. Resource pooling

Based on the demand of the consumers the resources of the service provider can be allocated and assigned to different consumers. This is called resource pooling. In other words providers serve multiple clients and customers. The services can be carried out without affecting the end user needs. The facilities can be used by multiple users.

3.2. Flexibility

The resources are flexible and can be made to scale in or scale out depending on the need and the user with the changing situation. For example consider an office with a multiple number of employees. The employees can gain access to the files in the office system by means of notebooks, smartphones and laptops by means of cloud computing. Flexibility is the property which assists in meeting these standards.

3.3. Accessibility

The cloud computing services can be accessed from various domains including smart phones and laptops. Conventional methods can also be employed in order to get the benefits of cloud computing services. The ease with which a service can be accessed forms a major design criteria and deciding factor in many networking applications.

3.4. Measurability

Resources are used by the consumers and are allocated by the service providers. There should be a transparency in the allocation and usage of resources. This usage is controlled, checked and monitored periodically thereby increasing the accountability. As a result the transparency of the process is much increased which in turn raises user satisfaction.

3.5. On demand self service

On demand self-service refers to the provision of providing cloud services when a demand for a particular service is made. Human interference is not needed as the user can directly interact with the service providers for computing functions such as network storage and server time. Here the host operations are uninterrupted. It is the most prominent feature of the cloud computing application.

4. ISSUES IN CLOUD COMPUTING

Even though there are many advantages and advancements in the field of cloud computing there are certain issues which outplay them, the primary one being security and privacy concerns. Google is one of the leading search engines which provide a variety of user friendly services. However its policy

update established that any data uploaded by the user can be handled by the google authorities exclusively [16]. It means that the user data is not private. In the case of medical records and auditing details the risk is very high. They provide security by means of firewall and virtualization techniques. However they are not 100% fault free. There are numerous occasions where the security measures resulted in failures. The following are the main risks which are found unique to cloud computing systems

- Heterogeneity
- Virtualization
- Outsourcing
- Multitenancy
- Service level agreement
- Shared responsibility

Data location is a significant factor in cloud computing systems. If the actual location of the data is unknown it becomes extremely difficult for the data protection technique to implement correctly [17]. [18] Another problem which the cloud computing environment possesses is trust. It is directly linked to the credibility and accountability of the service providers. All kinds of attacks that are inherent to networking systems are applicable to cloud computing systems also. Common threats such as phishing, man-in-the-middle attack, eavesdropping and sniffing are all applicable to cloud systems also. Spamming and third party API's are all threats to cloud computing systems [19].

4.1. Distributed Denial of Service (DDoS)

In DDoS different systems affected by viruses or trojans are used to target a single system which causes the service rendered by that system to be denied. In DDoS attack all the systems which are controlled by the hacker gets affected along with the end user system. The sources of such an attack is different and blocking IP addresses will not help in dealing with the problem. It is entirely different from Denial of Service attack (DoS) as in that case only a single computer and internet connection is used for the attack. DDoS consumes all available bandwidth thereby interfering with the accessing capabilities of the users in networking systems. It is a major threat to organizations as they can affect their fame and repute, decrease productivity and may result in revenue loss. However it is required to leave DDoS before the process of billing starts for the service provider. The types of DDoS attacks include traffic attacks, bandwidth attacks and application attacks. In traffic attacks large packets are send such that data gets lost. It may be accompanied by malware exploitation. In bandwidth attack the target is loaded with junk data causing DDoS. Application attacks harm the resources in the application layer which in turn causes denial of service.

4.2. Storage security

The following are the challenges which are faced by cloud systems in terms of data storage. They include storage space and vulnerability to attacks. The cloud computing technique is accomplished through a series of service providers. The primary provider uses the facilities of other providers. Hence the data becomes vulnerable to attacks. Sometimes it may become necessary for a service provider to transfer the services owing to merger, acquisition etc., However the data regarding the users may still remain in hard drives thereby posing a security risk.

5. SOLUTIONS FOR CLOUD COMPUTING SECURITY PROBLEMS

Maintaining confidentiality of the data is an important area where cloud computing techniques need to focus on. Data encryption technique can be used to meet this challenge [20]. Qualysgard is a package of services that are used to identify the network weaknesses.

5.1. Data classification as a security measure in cloud computing

[21] As mentioned earlier throughout the paper, data is a significant factor in cloud computing. Since data in a cloud computing technique possess various attributes, the security measures required for them also varies. Data classification is one such security measure where the basis is parameters and dimensions. Parameters are defined based on dimensions.

5.1.1. Process of data classification

In simple words data classification can be defined as the process of identifying data elements based on its business value. This value is calculated based on access control and usage. In data classification, the data can be classified under the following three categories. They are access control, content and storage

[22]. Figure A2 shows the hierarchy of data classification.

5.1.2. Access control

This category expresses the access limitations applied on data. They include

Access frequency: The elements can be accessed more frequently, less frequently and moderately. A customer can take decision on the boundary limit of these values and can classify them based on the type of access

Update Frequency: The elements can be classified based on the frequency with which they are updated. They can be high, less or moderate.

Visibility and accessibility: Based on the data visibility region and accessibility type the data classification can be employed.

Retention period: The amount of time a data is kept under retention can also be a deciding factor in data classification.

5.1.3. Content

The content of data used in cloud computing is also an important property for data classification.

Consistency: Data consistency is one important content factor. Some data require data consistency in a heavy manner while some cases do not require them. In such cases the data becomes permanent once stored. Hence updating is not possible for inconsistent data.

Degree of Completeness: The data can be either complete or incomplete. Hence degree of completeness can be regarded as a factor for data classification. However such a classification is not mandatory.

Auditability: The data can be either auditable or non-auditable. Hence data can be classified based on their auditability.

Validity and accuracy: Precision, accuracy, reliability and validity are the major factors which account to data classification in cloud computing. The levels can be high, moderate or low and data can be classified based on these levels.

5.1.4. Storage

Data storage is another important factor which can be used for data classification. The policies can be broadly classified under the following categories.

Integrity: One critical issue is data integrity and this problem can be addressed by hash algorithms like SHA, MD5 etc.,

Data Quality Standards: For certifying data different standards are available and this standard can increase the quality of data classification.

Storage and communication encryption: There is a huge chance of data being hacked in the to and fro communication. Hence there is a need for cryptography and encryption of data. This process can also be taken into account for data classification.

5.2. Layered frame work for cloud computing

A layered frame work is another one measure that can be carried out for secured cloud computing. The layout of such a frame work is shown in figure A3.

The first layer is the virtual machine layer. The successive layer is called cloud storage layer. This layer is used to integrate resources from multiple cloud service providers such that a massive storage system is build. The third layer is called cloud data layer. The fourth layer is called a virtual monitor layer. It is a combination of both hardware and software solutions [22]. Each layer performs their own functions and security issues are minimised to a great extent.

5.3. Encryption based on enhanced attributes

Attribute based encryption (ABE) uses an asymmetric encryption scheme. Digital signatures and hash functions form the major components of such an encryption scheme. It is a simple and efficient algorithm that can be used for cloud computing applications. Unlike other methods ABE encrypts and decrypts data based on customer attributes. The whole data is not encrypted whereas only the attributes are encrypted. Controlled access structures such as cipher text, master key and private key are used to provide a flexible control. The main advantage of this encryption scheme is that they can restrict access based on roles. However they are applicable to small scale applications. When data retrieval is taken into account ABE is overhead [26]. Figure A4 shows the classification of attribute based encryption.

The cloud applications are broadly classified into high critical, low critical and medium critical applications based on the risk involved. All the applications are critical but in order to adapt suitable measures for each application such a classification is required. High critical applications are those applications in which if proper attention is not provided can lead to huge failures. A high amount of accuracy is needed in such applications. Railway ticket reservation system is an example of this type of critical application. Medium critical applications has less effect when failures occur. A critical example includes project management. When there is no impact on the system if failures occur it is called low critical applications. An example is call fire services. An advantage of cloud computing system is that they can manage the server load to a very great extent.

Non-degeneracy and bilinearity are the major properties of a simple enhanced attribute based encryption method. Digital signature and hash functions are associated with real time applications. Data stored in cloud follows the attribute based encryption. The process can be broken down into three parts viz based on access structures, based on secret key and private key and finally decryption. The legitimate users and their controlled access is specified by the access structure. It stipulates the different access structures to the customers based on their role and attributes. The user enters the public key which is followed by the decision making process. If the user allows it then secret key is generated. Now the user enters the private key with digital signature along with the secret key and private key. The second decision making process is now carried out. Decryption takes place once it is matched and the user is allowed to view the data.

[27] The general architecture in figure A5 explains the step by step process. At first the user is authenticated with the public key related to the access structures. If the user authenticates, it is proceeded to step 2, where the secret key is apparently generated. The input will be the private key of the user along with the digital signature of the user. The user has to match the private key with the generated secret key. They may be either equal or unequal. Once the secret key is generated by the cloud service the access id will be generated. The id associated with the user private key and the generated secret key need to be matched. The hashing function is used here for mapping the two sets. Thus the user is being authenticated more than once. The encryption algorithm is hard to decrypt. Thus the simplified ABE structures with hashing and digital signature are provided. The access limits are based on user attributes of the user hierarchy. The user hierarchy reflects the overall organisational structure and it depends upon the power hierarchy. The main aspect of attribute based encryption is to give a fine grained and individual access to each and every individual of the access structure. The possibility of changing the access structure based on the requirement of the organisation is made possible in the decryption phase. The Attribute Based Encryption (ABE) scheme is one of the widely used scheme for improving security in cloud computing.

6. CLOUD COMPUTING AND MALWARE DETECTION

Antivirus is the traditionally employed software which is used for detecting malwares in any network based system. The vulnerability of such systems get increasingly rapid with the advent of new technologies. In such a scenario normal antivirus software may fail to detect the impending threats. Hence a cloud computing environment itself can be used to detect malware. For facilitating this, the entire architecture can be divided into two sections. The first section is the normal cloud computing part and the next one is the detection part. For detection static signatures and dynamic detection technology has been used. The detection part can again be subdivided into static analysis and dynamic analysis [23]. In static analysis method, the entire dependence is on the signature which is already stored in the database. The methods employed include string matching algorithm, protein sequences and comparison of variants. In dynamic analysis heuristic detection is carried out in suspicious files to determine whether actually it is a malware or not. The heuristic analyser cannot be found out by the antivirus databases. The files which are found by the heuristic analyser will probably be the infected ones.

7. GENERAL MEASURES FOR IMPROVING SECURITY IN CLOUD COMPUTING

There are many issues that are more general to the cloud computing environment and hence there are generalized solutions for the improvement of security. Here we discuss about such generalized measures for improving the security.

7.1. Security of architecture

The security of cloud computing environment can be increased once the disadvantages of such a network are known. Architecture forms a major component of the computing group and hence these components should be assessed for security concerns. The issues related to the architecture should be minimised at the preliminary stage such that they do not have a trial run on the upcoming stages. Storage security and access management are major components of cloud computing architecture [24]. An architecture ontology approach is one such approach which can improve the security of the cloud computing environment

7.2. Data security

Data is the major component of cloud computing systems and hence their leakage should not be allowed. Privacy enhancement methods and tools should be studied and put in use for improving the data security. Benchmarks and agent based security model can be used for providing data security [25]. Encryption algorithm and authentication also enhances data security. Client based privacy manager also help in reducing data leakage. The main properties of such a manager include obfuscation, preference setting, data access and feedback.

7.3. Mirage management system

For the overall security of the cloud, security and integration of the VM management system is of utmost importance. Virtual machine images encapsulate all the applications of the cloud. The components of such a system include access control, maintenance, tracking and running filters. Transparent Cloud Protection System (TCPS) is used to monitor the integrity of cloud components. TCPS can detect modification of kernel data and hence threats can be identified to a very great extent.

7.4. Client based privacy manager

Client based privacy manager helps in reducing the problems related to data leakage and privacy concerns. In addition to it, other privacy related benefits are also provided. The main features include obfuscation, preference setting, data access, feedback and personae. In the first step viz obfuscation, some or all fields of a data structure are obfuscated. In the second step preferences are set. In the data access module users are allowed to access personal data in the cloud. The feedback module shows the feedback and personae allow the user to choose between multiple personae when interacting with clouds.

7.5. Transparent Cloud Protection System (TCPS)

TCPS is located between the kernel and the virtualization layer. The main function is to protect the integrity of the virtual machines. They monitor the kernel and key components of the cloud periodically. Hence they can detect any modification and thus guarantees the privacy of the system.

There are various other problems which are inherited from networks such as SQL injection attacks, cross site scripting attacks, Man in the Middle attacks, DNS attacks, sniffer attacks, security concerns with the hypervisor, denial of service attacks, cookie poisoning, CAPTCHA breaking and Google hacking. These problems are addressed by the normal methods and are given less importance. These normal methods include security configuration, firewalling, transfer security, legislation, provider privilege, e-discovery, data location, redundancy, disposal, cryptography, lock in etc.

8. CONCLUSION

With the growing scenario customers are increasingly depending upon smart phones, tablets and mobile applications for computing needs. Cloud computing resources find their use in these applications. The significance of this approach includes a rise in the number of clients. However security concerns need to be addressed very carefully. Porting legacy applications is a major issue of interest in software related scenarios. One of the important platforms such as open stack and their installation is another one critical issue. Integration problems, development and deployment environment, dealing with

external and virtual resources are some other issues which need to be well addressed. Interoperability, data management and infrastructure are the main research issues studied recently. Research and experimentation should be carried out extensively focussing exclusively on the need to raise the security of data included in the process. The main areas of concern include network security, virtualization, data protection and isolation of resources. The security measures should be carried out in such a way that it should gain the confidence of the users. In short trust management should be taken care off.

REFERENCES

[1] Christy Pettey, Gartner Identifies the Top 10 Strategic Technologies for 2011; Analysts Examine Latest Industry Trends During Gartner Symposium/ITxpo, Orlando, Florida, 2010.

[2] Shuai Zhang, Shufen Zhang, Xuebin Chen and Xiuzhen Huo, Cloud Computing Research and Development Trend, IEEE 2nd International Conference on Future Networks, Sanya, Hainan, China, 2010, pp. 93-97.

[3] Ammar Khalid, Cloud Computing: Applying Issues in Small Business, International Conference on Signal Acquisition and Processing, Bangalore, India, 2010, pp. 278-281.

[4] Alexandros Marinos and Gerard Briscoe, Community Cloud Computing, 1st International Conference on Cloud Computing, Beijing, China, 2009, pp. 472-484, http://dx.doi.org/10.1007/978-3-642-10665-1_43.

[5] From Hype to Future, IT Advisory, KPMG'S Cloud Computing Survey, 2010, pp. 1-44.

[6] Tim Mather, Subra Kumaraswamy and Shahed Latif, Cloud Security and Privacy-New from O'Reilly: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, Inc, Sebastopol, California, United States, 2009, pp. 1-338.

[7] Wenjuan, and Lingdi Ping, Trust Model to Enhance Security and Interoperability of Cloud Environment, 1st International Conference on Cloud Computing, Beijing, China, 2009, pp. 69-79, http://dx.doi.org/10.1007/978-3-642-10665-1_7.

[8] John W. Rittinghouse and James F. Ransome, Cloud Computing: Implementation, Management and Security, CRC press, Taylor and Francis Group, USA, 2009, pp. 1-127.

[9] B.R.Kandukuri, V.R.Paturi and A.Rakshit, Cloud Security Issues, Proceedings of the 2009 IEEE International Conference on Services Computing, Washington, DC, USA, 2009, pp. 517-520.

[10] J.Brodkin, Gartner: Seven Cloud-Computing Security Risks, InfoWorld, 2008.

[11] K.Popovic and Z. Hocenski, Cloud Computing Security Issues and Challenges, Proceedings of the 33rd International Convention in MIPRO, 2010, pp. 344-349.

[12] S.Ramgovind, M.M.Eloff and E.Smith, The Management of Security in Cloud Computing, Information Security for South Africa, Sandton, Johannesburg, 2-4 August 2010, pp. 1-7.

[13] Safaa Salam Hatem, Maged H.Wafey, Mahmoud M.El-Khouly, Malware Detection in Cloud Computing, International Journal of Advanced Computer Science and Applications, Vol. 5, No. 4, 2014, pp. 187-192.

[14] Farrukh Shahzada, State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions, Procedia Computer Science, Vol. 37, 2014, pp. 357-362, http://dx.doi.org/10.1016/j.procs.2014.08.053.

[15] Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. Cloud Security Alliance, 2011, pp. 1-177.

[16] Google Drive Owns Everything you Upload? Privacy Policy Concerns Remain, 2012.

[17] David Teneyuca, Internet Cloud Security: The Illusion of Inclusion, Information Security Technical Report, Vol. 16, No. 3-4, 2011, pp. 102-107,

http://dx.doi.org/10.1016/j.istr.2011.08.005.

[18] Patrick Ryan and Sarah Falvey, Trust in the Clouds, Computer Law and Security Review, Vol.28, No. 5, 2012, pp. 513-521, http://dx.doi.org/10.1016/j.clsr.2012.07.002.

[19] Swarnpreet Singh and Tarun Jangwal, Cost break down of Public Cloud Computing and Private Cloud Computing and Security Issues, International Journal of Computer Science and Information Technology, Vol. 4, No. 2, 2012, pp. 1-15.

[20] M.Armbrust, A.Fox, R.Grith, A.D.Joseph, R.Katz, A.Konwinski, G.Lee, D.Patterson, A.Rabkin, I.Stoica and M. Zaharia, A View of Cloud Computing," Communications of the ACM, Vol. 53, No. 4, 2010, pp. 50-58, http://dx.doi.org/10.1145/1721654.1721672.

[21] Rizwana Shaikha and M.Sasikumar, Data Classification for Achieving Security in Cloud Computing, Procedia Computer Science, Vol. 45, 2015, pp. 493-498, http://dx.doi.org/10.1016/j.procs.2015.03.087.

[22] Prince Jain, Security Issues and their Solution in Cloud Computing, International Journal of Computing and Business Research, Proceedings of I-Society at GKU, Talwandi Sabo Bathinda, Punjab, 2012.

[23] Amit Sahai and Brent Waters, Fuzzy Identify-Based Encryption, Proceedings 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 2005, pp. 457-473, http://dx.doi.org/10.1007/11426639_27.

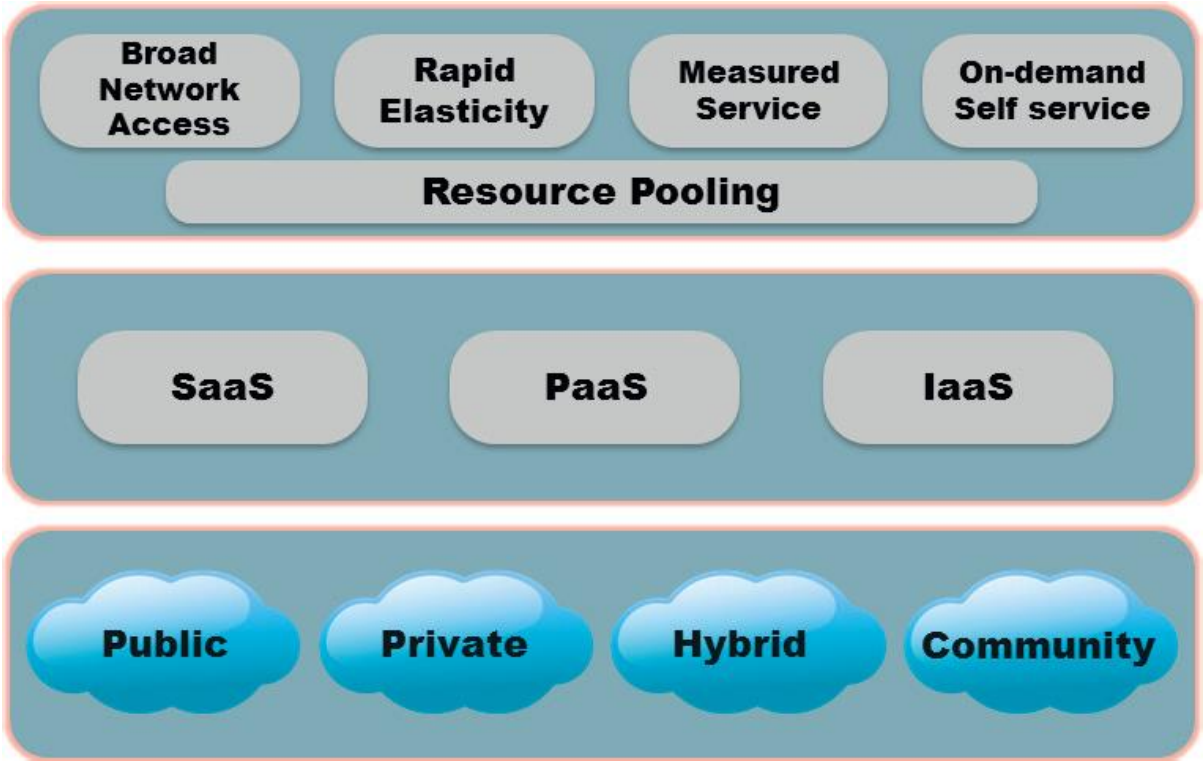
[24] N.Saravana Kumar, G.V.Rajya Lakshmi and B.Balamurugan, Enhanced Attribute Based Encryption for Cloud Computing, Procedia Computer Science, Vol. 46, 2015, pp. 689-696, http://dx.doi.org/10.1016/j.procs.2015.02.127.

[25] Scott Treadwell and Mian Zhoul, A Heuristic Approach for Detection of Obfuscated Malware, IEEE International Conference on Intelligence and Security Informatics, Dallas, Texas, 2009, pp. 291-299, http://dx.doi.org/10.1109/ISI.2009.5137328.

[26] Ronald L. Krutz and Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing,

[27] Tetsuya Morizumi, Kazuhiro Suzuki and Hirotsugu Kinoshita, A System for Search, Access Restrictions and Agents in the Clouds, IEEE Ninth Annual International Symposium on Applications and the Internet, Bellevue, Washington, 2009, pp. 201-204.

APPENDIX A



Adapted from [14]

Figure A1.A cloud computing model

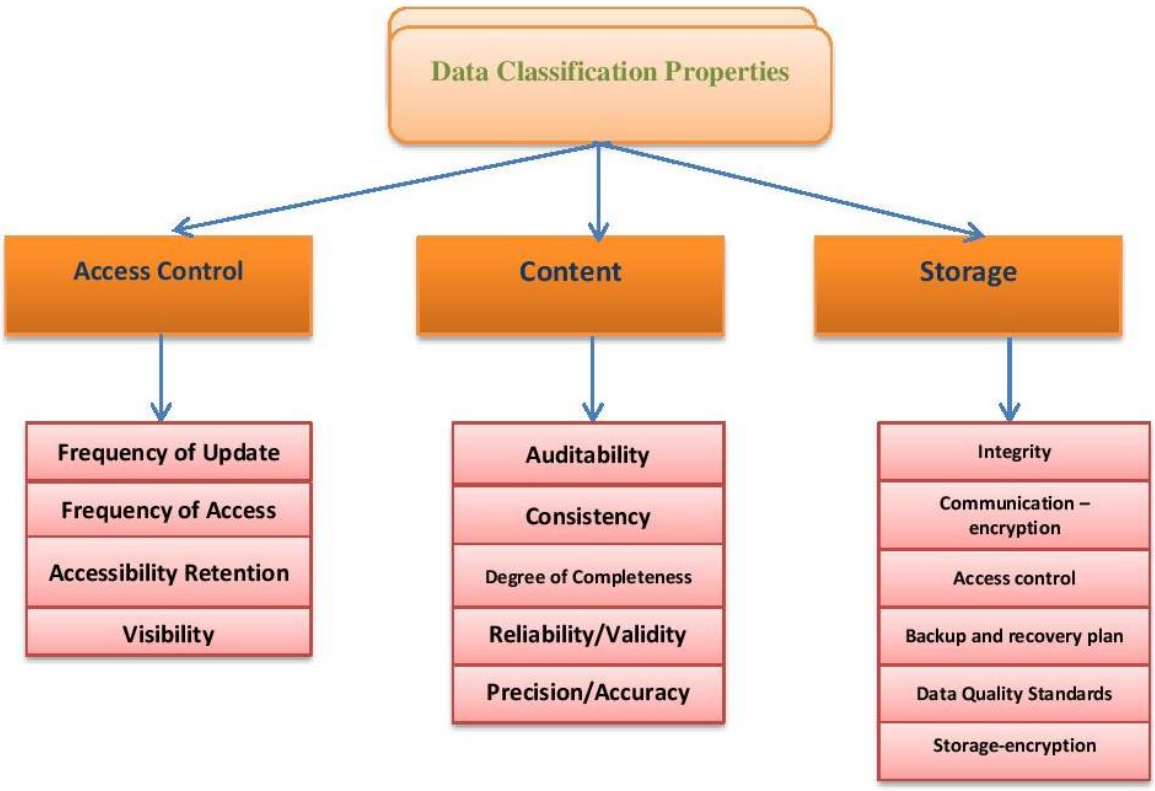
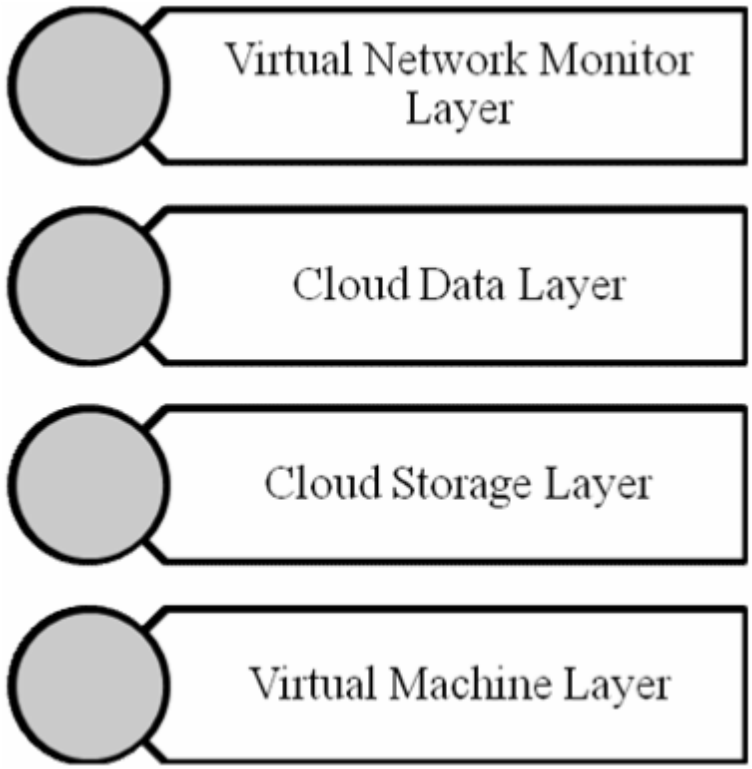


Figure A2.Properties of data classification



Adapted from [22]

Figure A3.Layered frame work for improving security in cloud computing

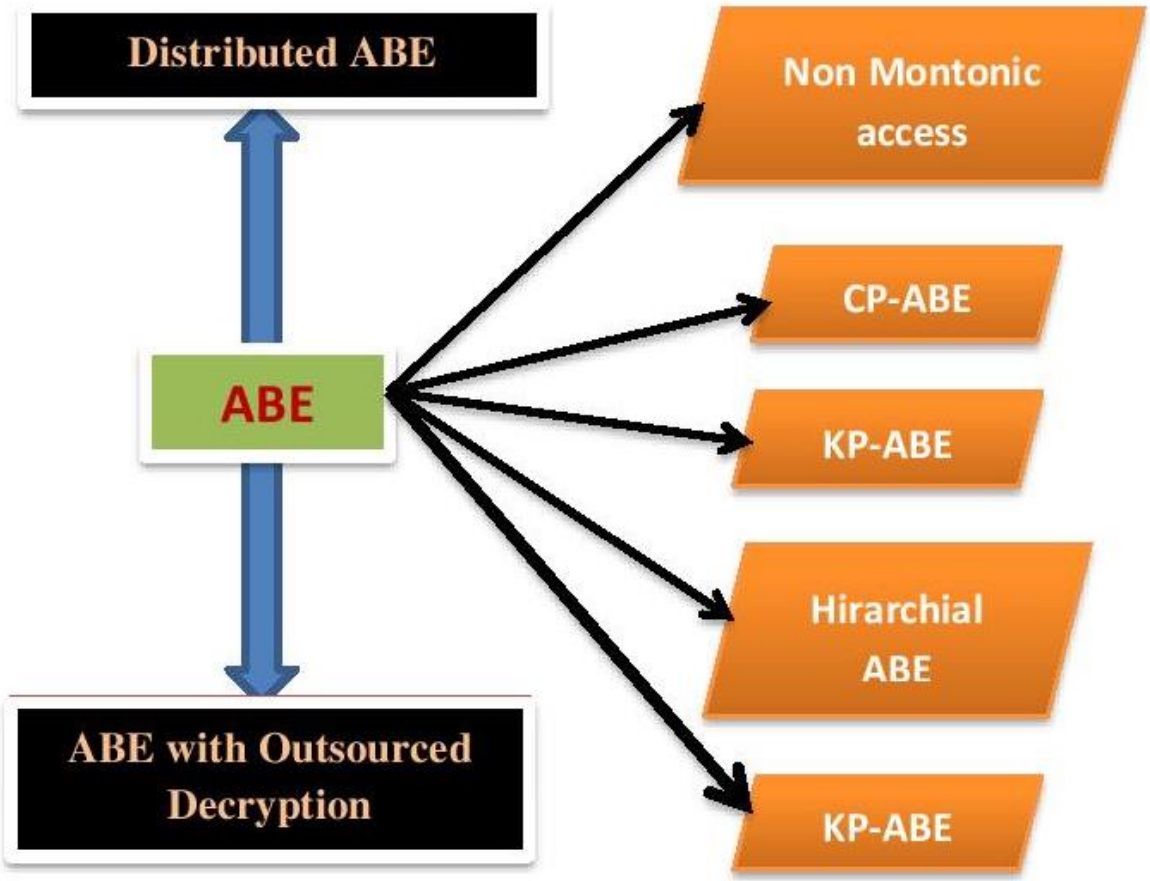
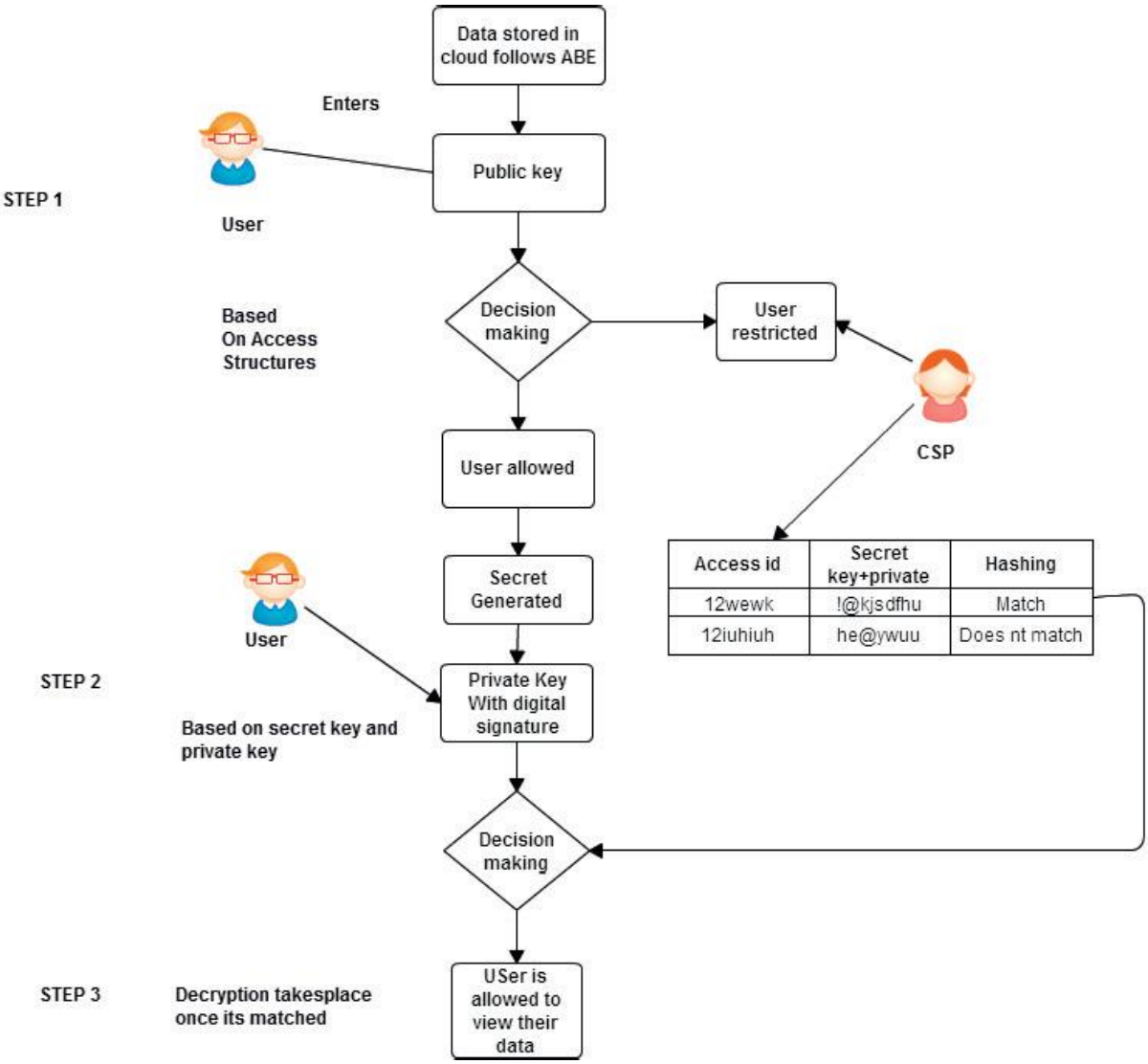


Figure A4.ABE classification



Adapted from [24]

Figure A5.Process of attribute based encryption