مجـلة الـتربـوي
Journal of Educational
ISSN: 2011- 421X
Arcif Q3

معامل التأثير العربي 1.63
العدد 23

مجلة التربوي

مجلة علمية محكمة تصدر عن كلية التربية

جامعة المرقب

العدد الثالث والعشرون
يوليو 2023م

- المجلة ترحب بما يرد عليها من أبحاث وعلى استعداد لنشرها بعد التحكيم .
- المجلة تحترم كل الاحترام آراء المحكمين وتعمل بمقتضاها .
- كافة الآراء والأفكار المنشورة تعبر عن آراء أصحابها ولا تتحمل المجلة تبعاتها .
- يتحمل الباحث مسؤولية الأمانة العلمية وهو المسؤول عما ينشر له .
- البحوث المقدمة للنشر لا ترد لأصحابها نشرت أو لم تنشر .

ضوابط النشر:

يشترط في البحوث العلمية المقدمة للنشر أن يراعى فيها ما يأتي :

- أصول البحث العلمي وقواعده .
- ألا تكون المادة العلمية قد سبق نشرها أو كانت جزءا من رسالة علمية .
- يرفق بالبحث تزكية لغوية وفق أنموذج معد .
- تعدل البحوث المقبولة وتصحح وفق ما يراه المحكمون .
- التزام الباحث بالضوابط التي وضعتها المجلة من عدد الصفحات ، ونوع الخط ورقمه ، والفترات الزمنية الممنوحة للتعديل ، وما يستجد من ضوابط تضعها المجلة مستقبلا .

تنبيهات :

- للمجلة الحق في تعديل البحث أو طلب تعديله أو رفضه .
- يخضع البحث في النشر لأولويات المجلة وسياساتها .
- البحوث المنشورة تعبر عن وجهة نظر أصحابها ، ولا تعبر عن وجهة نظر المجلة .

Information for authors

1- Authors of the articles being accepted are required to respect the regulations and the rules of the scientific research.
2- The research articles or manuscripts should be original and have not been published previously. Materials that are currently being considered by another journal or is a part of scientific dissertation are requested not to be submitted.
3- The research articles should be approved by a linguistic reviewer.
4- All research articles in the journal undergo rigorous peer review based on initial editor screening.
5- All authors are requested to follow the regulations of publication in the template paper prepared by the editorial board of the journal.

Attention

1- The editor reserves the right to make any necessary changes in the papers, or request the author to do so, or reject the paper submitted.
2- The research articles undergo to the policy of the editorial board regarding the priority of publication.
3- The published articles represent only the authors' viewpoints.

Possible solutions to ensure data protection in cloud computing to avoid security problems

Nuria Mohamed Hider
Elmergib University Faculty of Science, Computer Department
aanur284@gmail.com

الملخص: تعتبر الحوسبة السحابية بمثابة تقنية حوسبة مستقبلية. تم تحويل العديد من المؤسسات بالفعل إلى بيئة الحوسبة السحابية للاستفادة من خدماتها متعددة الأبعاد. يتم توزيع العديد من الخدمات السحابية جغرافيًا وتتكون معظم هذه الخدمات من معلومات حساسة لمستخدمي السحابة. حيث توفر الحوسبة السحابية الكثير من الفوائد ، من ناحية أخرى ، فهي مليئة بالمخاطر الأمنية. ظلت الجوانب الأمنية قضية أساسية في الحوسبة السحابية منذ سنوات عديدة. كانت حماية بيانات المستخدمين بشكل خاص من الهجمات الضارة تمثل تحديًا لموفري خدمات الحوسبة السحابية. لذلك ، تركز دراستنا على قضايا أمن بيانات الحوسبة السحابية التي تهتم في الغالب بسريتها وسلامتها وتوافرها (CIA). تعتمد الدراسة بالكامل على نهج البحث النوعي الذي يتضمن الأبحاث السابقة وبعض المقالات الحالية المنشورة من قبل بائعي أمن المعلومات المشهورين مثل المعهد الوطني للمعايير والتكنولوجيا (NIST). تغطي الدراسة أيضًا مناقشة تفصيلية بشأن الحوسبة السحابية ونماذج خدمتها والتحديات الشائعة. ومع ذلك ، فقد تم بالفعل إجراء العديد من الأبحاث في هذا الموضوع. وبالتالي ، إلى جانب إلقاء الضوء على مشكلات أمان بيانات الحوسبة السحابية ، تقدم دراستنا الحلول الممكنة لضمان حماية البيانات في الحوسبة السحابية. نظرًا لأن الدراسة تتكون من الحلول المختلفة التي تمت تغطيتها من الأبحاث الأخرى ، فيمكن اعتبارها دليلًا شاملاً لحلول أمان البيانات للحوسبة السحابية .

ABSTRACT: Cloud computing is considered as a future computing technology. Many organizations are already switched to cloud computing environment to benefit from its multidimensional services. Numerous cloud services are geographically dispersed and most of these services consist on sensitive information of cloud users. Where Cloud computing provides a lot of benefits, on the other hand, it is full of security risks. The security aspects remained a core issue of cloud computing since many years. Specially protecting users' data against malicious attacks has been challenging for cloud computing service providers. Therefore, our study focuses on the cloud computing data security issues that mostly concern with its confidentiality, integrity and availability (CIA). The study is entirely based on qualitative research approach that includes previous researches and some existing articles published by famous information security vendors such as National Institute of Standards and Technology (NIST). The study also covers a detail discussion regarding cloud computing, its service models, and common challenges. However, numerous researches have already been done in this topic. Thus, besides shedding lights on cloud computing data security issues, our study presents the possible solutions to ensure data protection in cloud computing. As the study consists on the various solutions covered from other researches, thus it can be considered as an overall data security solution guide for cloud computing.

Keywords: Cloud computing, Cloud computing data security issues and solutions, cloud computing environment and data protection

I .INTRODUCTION

From initial concept building to current actual deployment, cloud computing is growing more and more mature. Nowadays many organizations, especially Small and Medium Business (SMB) enterprises, are increasingly realizing the benefits by putting their applications and data into the cloud. The adoption of cloud computing may lead to gains in efficiency and effectiveness in developing and deployment and save the cost in purchasing and maintaining the infrastructure. Regarding definition of cloud computing model, the most widely used one is made by NIST as “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.”[1] The cloud computing model NIST defined has three service models and four deployment models. The three service models, also called SPI model, are: Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). The four deployment models are: Private cloud, Community cloud, Public cloud and Hybrid cloud. Compared with the traditional IT model, the cloud computing has many potential advantages. But from the consumers’ perspective, cloud computing security concerns remain a major barrier for the adoption of cloud computing. According to a survey from IDCI in 2009, 74% IT managers and CIOs believed that the primary challenge that hinders them from using cloud computing services is cloud computing security issues [2]. Another survey carried out by Garter in 2009, more than 70% CTOs believed that the primary reason not to use cloud computing services is that there are data security and privacy concerns.

Although cloud computing service providers touted the security and reliability of their services, actual deployment of cloud computing services is not as safe and reliable as they claim. In 2009, the major cloud computing vendors successively appeared several accidents. Amazon's Simple Storage Service was interrupted twice in February and July 2009. This accident resulted in some network sites relying on a single type of storage service were forced to a standstill. In March 2009, security vulnerabilities in Google Docs even led to serious leakage of user private information. Google Gmail also appeared a global failure up to 4 hours. It was exposed that there was serious security vulnerability in VMware virtualization software for Mac version in May 2009. People with ulterior motives can take advantage of the vulnerability in the Windows virtual machine on the host Mac to execute malicious code. Microsoft's Azure cloud computing platform also took place a serious outage accident for about 22 hours. Serious security incidents even lead to collapse of cloud computing vendors. As administrators’ misuse leading to loss of 45% user data, cloud storage vendor Link Up had been forced to close.

Security control measures in cloud are similar to ones in traditional IT environment. As multi-tenant characteristic, service delivery models and deploy models of cloud computing, compared with the traditional IT environment, however, cloud computing may face different risks and challenges. Traditional security issues are still present in cloud computing environments. But as enterprise boundaries have been extended to the cloud, traditional security mechanisms are no longer suitable for applications and data in cloud. Due to the openness and multi-tenant characteristic of the cloud, cloud computing is bringing tremendous impact on information security field: (1) Due to dynamic scalability, service abstraction, and location transparency features of cloud computing models, all kinds of applications and data on the cloud platform have no fixed infrastructure and security boundaries. In the event of security breach, it’s difficult to isolate a particular physical resource that has a threat or has been compromised. (2) According to the service delivery models of cloud computing, resources cloud services based on may be owned by multiple providers. As there is a conflict of interest, it is difficult to deploy a unified security measures; (3) As the openness of cloud and sharing virtualized resources by multi-tenant, user data may be accessed by other unauthorized users. (4) As the cloud platform has to deal with massive information storage and to deliver a fast access, cloud security measures have to meet the need of massive information processing. This paper describes data security and privacy protection issues in cloud. This paper is organized as follows: Section II gives a brief description of what exactly cloud computing security-related issues are. Section III discusses data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Section IV shows current solutions for data security and privacy protection issues in cloud. Section V summarizes the contents of this paper. Section VI describes future research work.

II .CLOUD COMPUTING DEPLOYMENT MODELS

Cloud computing includes applications that have to be delivered as being services through the internet. It also includes systems’ software and hardware in the main data centers. In cloud computing, there are four major cloud delivery models as illustrated in Figure.1 in accordance with the provisions of NIST (Badger et al., 2011). The classifications were based on the provider of cloud computing services.

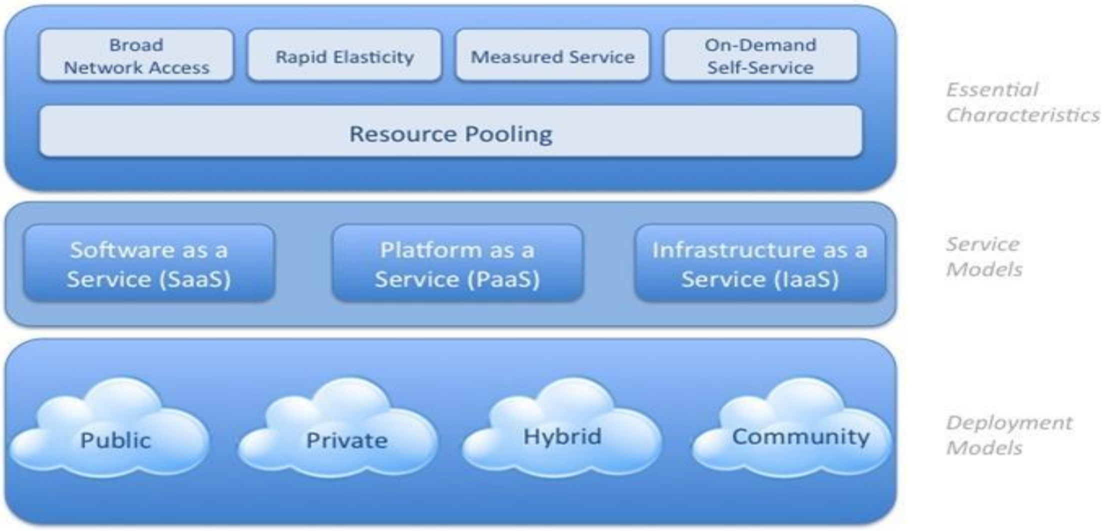


Figure 1: Cloud Computing Models (Mell e Grance , 2011)

The four models include public, private, community & hybrid clouds. The details about these models are given below:

A. Private Cloud

It is a cloud computing infrastructure mainly used in private firms. It may be operated either by a third party or the organization itself. A private cloud entails a sub-set of a chain of interfaces, services, applications, hardware and networks which the organization controls. The organization ensures that all these applications are ready and convenient for use by the partners, customers and even employees in a firm (Kim-Kwang, 2010). However, it is possible for a third party to create and control a private cloud. Such a form of a cloud has a firewall to ensure that there is security, appropriate governance and compliance. Private clouds are mainly not open for use by the public because it is mainly set in a private and controlled environment. A private cloud is mainly more secure than a public cloud. Moreover, it has more privacy features when compared to a public cloud and it is easier to control. Other features of a private cloud that make it ideal for use in a commercial premises include energy and cost efficiency that makes it more reliable (Ritesh, 2015). The features of a private cloud are illustrated in Figure.2:

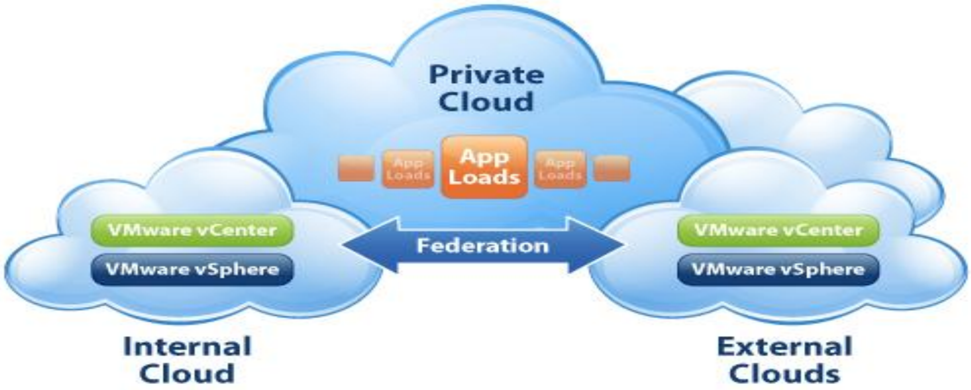


Figure 2: Private Cloud Model (Ritesh, 2015)

Private cloud contains almost all the features of a public cloud. It is not only secure but also efficient and its performance is fairly reliable. One of the major demerits of a private cloud is that it is quite complex; thus, it has to be run by experts who have appropriate knowledge of cloud architecture. Similarly, the experts should be able to patch, secure, upgrade, scale and monitor a cloud environment for maximum functionality (Creeger, M, 2009).

B. Community Cloud

Community clouds are applications that are designed as common facilities for public use. Its structure makes it easy to share between many organizations. In a community cloud, there is a group of experts whose task is to provide security as sharing a cloud cause a chain of security consequences to the firm. These security threats have to be managed. When a cloud infrastructure is available and is being shared by many firms, there are communal concerns which arise. Some of them include security demands, and compliance. An organization or a third party may manage a community cloud. Interestingly, a community cloud may exist both within and outside the premise (Winkler, 2011). Figure 3 illustrates the example of community cloud:

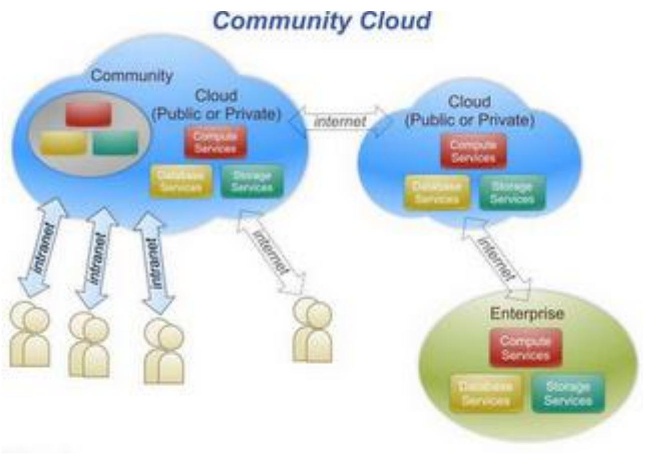


Figure 3: Community Cloud Model (Rahul Dasgupta , 2016)

C. Public Cloud

The most distinctive model of cloud computing for many consumers is the model of a public cloud, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet. A public cloud model is specifically based on the platform where web hosted services, applications and software's are available for public use. Various public cloud computing service providers like Amazon web services, Google cloud, Microsoft Azure owns and host public cloud infrastructure at their data center. The infrastructure of a public cloud makes it possible to avail it to the public and even large industries. A public cloud is mainly the property of a firm that sells cloud services. A public cloud has a robust infrastructure that makes it possible to provide services to many clients using shared applications. A public cloud is home to a chain of interfaces, applications, networks, hardware and storage devices that may be owned by a third party that avails it to firms and individuals. The infrastructure of a public cloud is mainly not revealed to the customers. Public clouds are ideal for the management of repetitive workloads that makes them more viable for use by large firms. Just like a private cloud, a public cloud too provides a chain of merits such as cost efficiency, flexibility, reliability, and scalability (NIST, 2009).

Figure.4 is an example of a public cloud:

Public Cloud
Customer A
Customer B
Customer C

Figure 4: A Public Cloud Model (NIST, 2009)

D. Hybrid Cloud

A cloud infrastructure is a combination of more than one cloud such as public, private and community clouds. The clouds remain as being unique entities. A standard or a proprietary technology binds them together. The public and private clouds in a hybrid cloud arrangement are distinct and independent elements. This allows organizations to store protected or privileged data on a private cloud, while retaining the ability to leverage computational resources from the public cloud to run applications that rely on this data. There are instances when a firm has to handle a wide range of software applications that involves the transfer of data between public and private data centers. A firm may also use a public platform to transfer data using a private cloud application or a data center. A cloud is not branded as being hybrid if a firm uses Software as a Service (SaaS) especially when there is no movement of data from the application to the firm’s data center. A cloud is also not hybrid when a firm’s developers have to use public clouds for purposes such as prototyping a new application that has been disconnected from a private cloud and data center (Leighton, 2009).

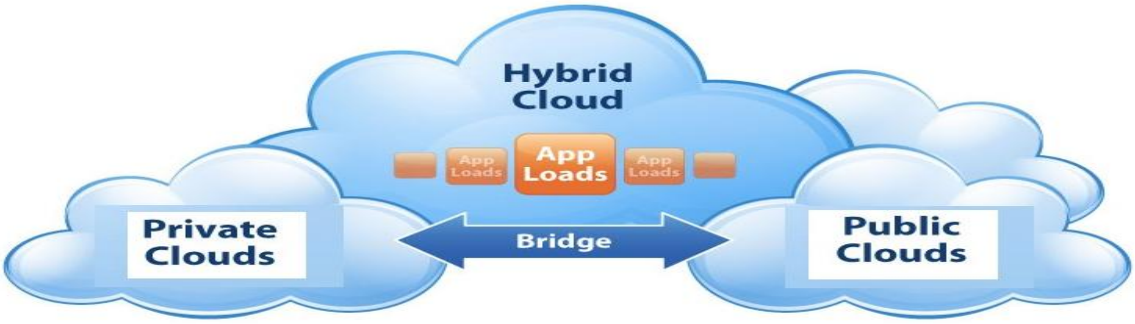


Figure 5: Hybrid Cloud Model (Leighton, 2009)

III . CLOUD COMPUTING SERVICE MODELS

It is possible to access cloud services through cloud computing models as illustrated in Figure 6. Many of the cloud computing services have some characteristics that satisfy an organizational requirement. The firm selects the best service and customizes it for organizational use (Rohit et. all, 2014). Cloud computing services models are shown in Figure.6:

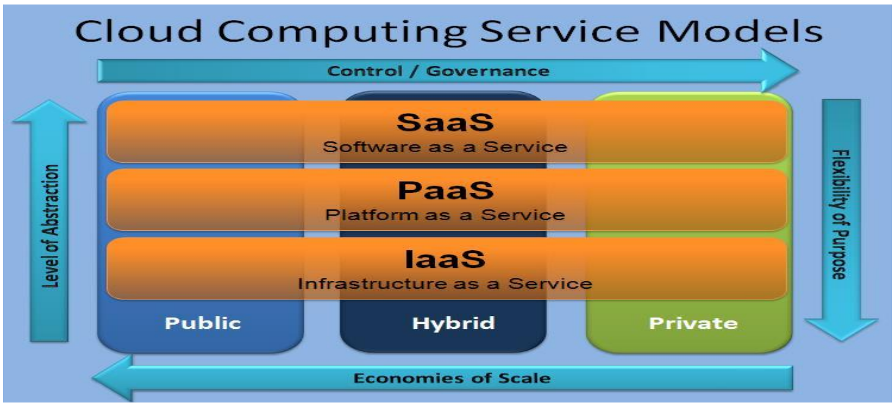


Figure 6: Cloud computing services (Rohit et. all., 2014)

A. CLOUD COMPUTING CHALLENGES

Although the steady growth of cloud computing; users have raised a number of concerns about the adoption and use of cloud computing technology. However, the advantages outweigh the disadvantages to them. Thus, it is recommended that companies adopt the model. Some of the main challenges include cloud computing:

B. Data Protection

Security is a great concern for customers when moving their data to the cloud. Although security in the cloud is generally reliable and proficient, customers need to know that the cloud provider they chose to work with has a fully secure cloud environment. Firms are quite reluctant to purchase an assurance of data security from various data vendors. Many firms dread losing their data or having it revealed to unwanted third parties. In many cases, the storage location remains private. This increases the security concerns of firms. In the available cloud technology models, there are firewalls in data centers which shield sensitive information from unwanted access. The firewalls are mainly owned by enterprises. In cloud, service providers have the task of ensuring that data is secure and that their security measures are reliable (Catteddu, 2010).

C. Data Recovery and Availability

Business applications have some level agreements that users have to take on to. There are operational teams which manage service level agreements and govern the use of applications. They provide the following support in a production environment:

1.Fail over and appropriate clustering
2.Performance and capacity management
3.Data recovery
4.Maintenance
5.Data replication
6.System monitoring

If a cloud provider does not provide enough infrastructures for any of the above services, the impact becomes so severe for an enterprise (Torry Harris, 2015).

D. Interoperability and Portability

Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT.

IV. CLOUD COMPUTING DATA SECURITY ISSUES

Data security has become a major challenge in information technology. It is an issue that raises concerns in a computing environment when compared to any other environment. The case is attributed to the fact that in a computing environment, data is mainly scattered in various storage devices such as personal computers, servers, different machines, mobile devices such as smart phones and sensor networks. In cloud computing, data security is more complicated when compared to the situation in the traditional information systems (Yunchuan et. al, 2014). Cloud computing is a new model in the field. Hence, there is a lot of uncertainty regarding data security in almost all levels such as host, network, data levels and applications. Security depends on the movement of applications to cloud computing. This has made executives believe that data security should be their major concern when they adopt the use of cloud computing technology (Hashizume et. al, 2013).

There are various security challenges in cloud computing as it involves a number of technologies such as operating systems, databases, networks, virtualization, load balancing, memory management, transaction management, resource scheduling, and concurrency control. Hence, many of the security concerns in these systems are synonymous with those of cloud computing. For instance, a network that links cloud systems should be very secure. In addition, cloud computing's virtualization paradigm causes many security concerns. For instance, the exercise of mapping virtual machines into being physical ones has to be very safe (Kevin Hamlen, 2010).

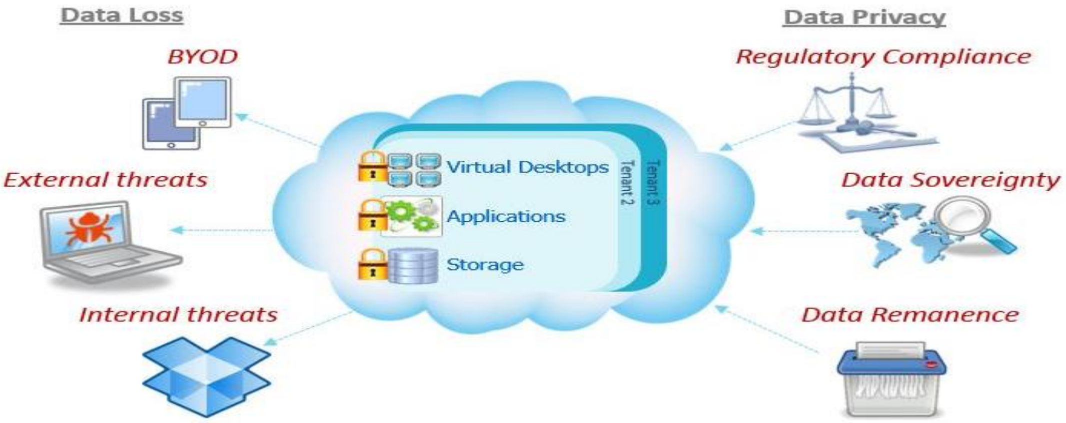


Figure 7: Data Security Issues in Cloud Computing (Techpluto, 2016)

Data security is one of the major issues of grave concern in cloud computing. Many users express concerns over the privacy of their private data. In a cloud computing environment, data insecurity raises serious issues among users who express concerns over the security of their data. The case is attributed to the fact that data is channeled to various machines and storage devices such as personal computers, servers and some mobile devices such as smartphones and wireless sensor networks. In cloud computing technology, data security has more complications when compared to the case in traditional information systems (D. Chen & H. Zhao, 2012). The aim of data security in cloud storage is to ensure that the server and its connections are safe from unwanted access. In this case, security is our major concern. Data availed to the server should not be exposed to unwanted parties as it is confidential. However, it should be readily available and consistent for a higher utility to the user. When a server contains some data, it should be set in a way that it is available for easy retrieval and use by the user (Shwetha Bindu & Yadaiah, 2011).

A. Trust management

Trust management refers to the reliance on strength, integrity, surety and ability of a thing or an individual. Entrusting one's data to a third party who is in this case the provider of cloud computing services is a challenge (Yunchuan et. al, 2014).

B. Security Provider

Cloud computing service providers use various measures to secure data from unauthorized access. These measures include encryption, authorization and user authentication. Clients often express worries of the vulnerability of data stored remotely. They worry about cyber-criminals such as hackers who many access the data and use it for other purposes apart from the intended. Cloud service providers have increasingly become wary of this challenge. In response, they have come up with many resources to mitigate this challenge (Kanchana & Dr. Dhandapani, 2013).

C. Privacy Protection

Unlike the traditional computing models, modern day cloud computing technology uses virtual technology. Therefore, it is possible to scatter one's private data virtually in a data center instead of confining it to a single physical location. Interestingly, it is possible to scatter data even beyond national boundaries. In such a case, data privacy becomes prone to a chain of controversies in various legal systems (Subashini & Kavitha, 2010).

D. Ownership

When data is delegated to cloud, customers express worries regarding the loss of their rights. They also express concerns of lack of or poor protection of their basic security rights. Interestingly, many cloud service providers respond to this concern through user-sided agreements. The agreement dictates that users may seek data security advice elsewhere (Balachandra, et. al, 2009).

E. Data location and Relocation

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data (Te-Shun Chou, 2013).

F. Multiplatform Support

One of the major issues facing many information technology departments is cloud based service integration across operating systems and various platforms such as Windows, OS X, thin clients and Linux. Having more support platforms for multi-purpose platforms will ease user interfaces as all of them will become web-based (Wang et. al, 2012).

G. Data recovery

Incidents such as a server breakdown are not desirable as they may cause damage that may lead to loss of user data. To avoid some such problems, it is important to back-up data to ensure that it can be recovered in the future in an unfortunate event of data loss. Cloud users may back up critical data on their local computer (Jonathan Katz, 2002).

H. Data Backup

Cloud providers may use resources such as redundant servers among other routine data back-up processes to keep their data safe from loss. Unfortunately, some people express worries over their ability to control their back-ups. Some providers have resulted to offering data bumps on media. They may also allow users to back up their data using regular downloads (Balachandra, et. al, 2009).

V .DATA SECURITY SOLUTIONS

There are various security challenges associated moving data into a cloud environment. Users and particularly organizations have to consider some of these data insecurity risks as they have the ultimate responsibility to mitigate these risks. Users need assurance of security of internal databases when data is migrated into cloud. They also need assurance of data confidentiality, availability and integrity. In cloud computing, data should be secure while at rest, in use and in transit. In this case, access to data may be controlled (NIST, 2011). Figure 4.1 reveals some six major areas of cloud computing there both software and equipment demand security measures (Trusted Computing Group’s White Paper, 2010).

These areas include:

1. Data in rest
2. Data in transit across various locations
3. Data while in use

4. Authentication for processes, users and applications
5. Separation of data that belongs to different users
6. Regulatory and legal issues in cloud computing
7. Incident response.

Figure 8 shows the major security concerns in cloud computing:

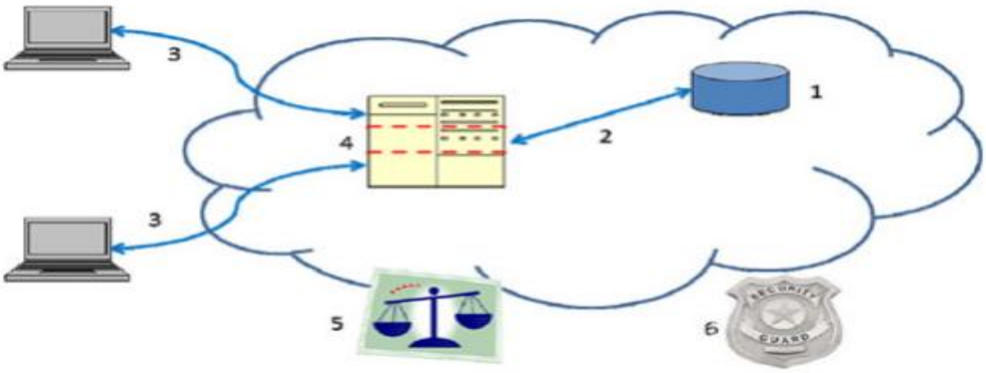


Figure 8: Areas for security concerns (NIST, 2011)

To ensure that data is secure, accessible in time and reliable in cloud, it is critical to involve to CIA (confidentiality, integrity and availability) aspects of data security. In this part of the project, there are detailed suggestions of solutions that shield CIA against many security issues that confront cloud computing technology as discussed earlier.

A. Encryption

Encryption is one of the most trusted means of securing sensitive data in a cloud environment especially for data while in rest or in transit. Almost all providers of cloud databases provide encryption support services for data in transit. These providers use Transport Layer Security and Socket Secure Layer (TLS/SSL) for transfer data. However, only a few of them offer encryption services for data at rest. Basically, there are three encryption options for cloud consumers for data at rest (Huang & Tso, 2012). These include:

- Partial encryption of the database depending on the standard encryption techniques.
- Full encryption of the database depending on the available standard encryption techniques.
- Full encryption of the database depending on the cloud provider’s proprietary encryption techniques.

Some cloud service providers offer all the data encryption options. However, this raises the cost of hosting such a database when compared to internal hosting. Some providers offer alternatives for all database encryption options. These alternatives have only a minimal impact to the performance of the system. Unfortunately, it utilizes a very ineffective technique that is very easy to bypass. The other encryption option for customers is the cloud provider’s own custom built encryption solutions. Interestingly, this does not impact on the system’s performance. However, it is not deemed as being safe for some encryption standards such as AES (Advance Data Encryption), DES (Data Encryption Standard), 3DES (Triple Data Encryption

Standard) etc (Huang & Tso, 2012). Figure 9 shows data encryption scenario in cloud computing.

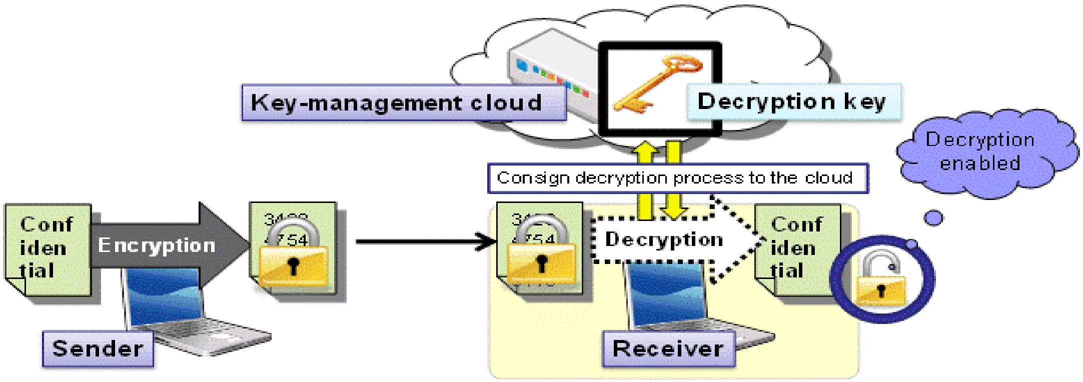
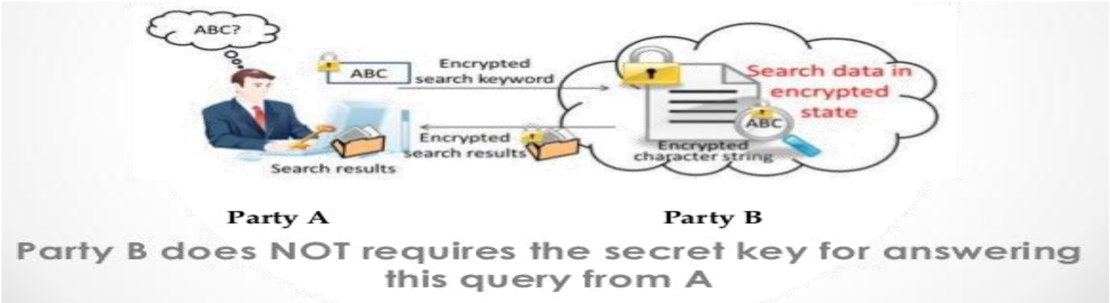


Figure 9: Data Encryption in Cloud (Tebaa M, 2012)

B. Homomorphic encryption

Homomorphism is a Greek term which refers to "same shape/structure". In Mathematics, homomorphism refers to a process of transforming a data set into another form without altering the relationship between the elements of both data sets. In the field of information security, Homomorphic encryption allows a user to apply Mathematical procedures on encrypted data without a compromise to encrypt. The major challenge with other encryption techniques is that servers hosting data cannot process any file on encrypted data. Homomorphic encryption does away with this challenge through introducing a technique of encrypting data that uses Mathematical procedures on encrypted data. Later on, it decrypts the results to come up with similar results even on unencrypted data (Tebaa M, 2012). Figure 10 presents the entire process involving in Homomorphic encryption.



Party B does NOT requires the secret key for answering this query from A

Figure 10: Homomophorbic data encryption process (Tebaa M, 2012)

C. Key Management

All data encryption techniques have an encryption algorithm on the plaintext. These techniques use a secret key to obtain the ciphertext. The levels of security between the private key and encrypted data are the same. Using encryption only as a means of data security does not do away with all the security risks. In real sense, encryption separates data from associated risks through moving the security to the encryption keys. It is important to manage the security of these keys from other insecurity threats. Unfortunately, exercises such as protecting, generating and managing encryption keys for many data sub-sets become an utterly demanding task. Presently, cloud consumers are regarded as being more ideal for cryptographic key management. Hence, it is recommended that employees gain control of the configuration and management of encryption keys (McAfee, 2012). Figure 11 shows the Key management method under PGP (Pretty Good Privacy).

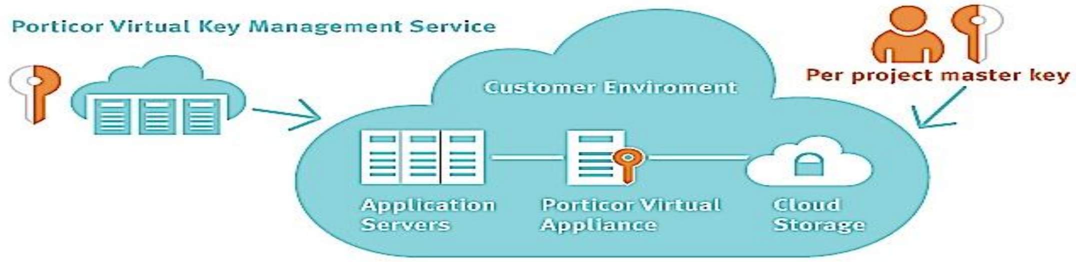


Figure 11: PGP Key Management (McAfee, 2012)

D. Distributed Database monitoring

Database monitoring or auditing refers to the act of recording and reporting the events as they occur in a database system without breaching the security measures. An audited database breeds reports on when, who and how data is accessed or modified. A strong tool for monitoring and auditing a database should enhance visibility of the database despite its location as accessibility is very important for cloud-based database services. Information technology security experts had previously used network based IPS and IDS to handle some of the challenges of shielding premise databases. IPS and IDS are appliances which are placed on the network to inspect traffic for viruses, malicious codes and protocol violations among others. Initially, enterprises would often ignore internal threats and risks. However, when they realized that there were some internal threats that posed serious damages, they decided to monitor their databases to secure them from both local and intra-database attacks as well (McAfee, 2011). McAfee in Figure 12 has demonstrated the distributed database management process in cloud environment.

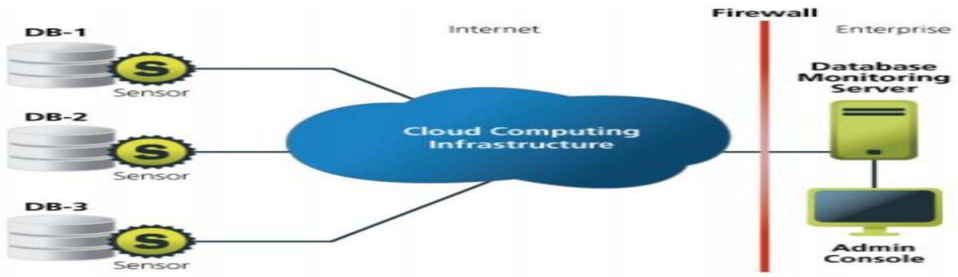


Figure 12: Distributed Database Monitoring (McAfee, 2011)

VI . DISCUSSION A. Comparison between Different Service Providers, There are different cloud service providers, where each vendor offers different security features and services. Some of the active players are Microsoft who has launched Microsoft Azure, IBM which has opened Blue Cloud program, Amazon that had opened

Amazon EC2 (Amazon elastic compute cloud) and Amazon AWS, and Google which has launched Google cloud (Harmandeep Singh, 2014).

At present, there are approximate more than 100 cloud vendors worldwide that works on cloud platform to make business experience innovative and smooth.

Here we are presenting the history of the most popular cloud service providers.

B. Amazon as a cloud service provider

The Amazon cloud system is considered to be the oldest in the cloud computing think tank, launched in 2006. Amazon owns the largest data center in the world, which heightened the Amazon position among the global service providers. Amazon data centers are located in the 10 regions of the globe, with 3 centers in USA and 7 centers across other parts of the globe.

The Amazon Cloud system presents its services in four major categories involving Compute, Databases, Networking, and Storage & Content Delivery. Presently Amazon have its own Hadoop framework which is better known as EMR, further offering kinesis for real time data streaming experience for its users. To meet the upcoming security challenges, Amazon cloud services AWS has built a strong encryption system. Amazon web services also presents NoSQL and relational database services with many third-party integrations for proper data interfaces between different systems.

The Amazon EC2 presents a pay per use model, and provide some ambient surroundings to scamper calculating assets, even as maintenance proper handling upon the statistics and facts within the customers hold. Amazon cloud service provides an easy flexibility and a scalability of the data as per the user’s demand. Amazon presents easy to use dashboard which makes it easy to scale up and down as per the user’s requirement, further Amazon also provides a cloud watch service which assist user to scale up and down as per the user’s demand. In Amazon cloud system, customers can access various customizable features including OS, initiating as well as finish utilization of security, dates, as well as network access controls. Amazon also provides one of the least expensive while costing extra charges for optional task like data movement. The service provider also offers 12-month free trial for small scale users. With the latest report of Synergy, Amazon has captured the largest market share, holding 28% of the total global market (M. Neeraj, 2015).

C. Google as a cloud service provider:

Google first launched its cloud computing system in 2012, as (GCE). Google cloud services are increasing with a ramping speed globally. The Google Compute Engine servers are located within three regions of the Globe including East Asia, Western Europe as well as Central United States. Cloud Google platform offers extensive support for some of the pioneered services including Hadoop, Big Table, and Big Query. Google cloud services presents a user based virtual application to start web application over Google servers by Python and Java environment. Google cloud computing system also provides an easy scalability and flexibility as per the users demand, with instant auto-scaling for Google compute engine. Google presents some added enhancements to its users including comprehensive maintaining for OS, live passage of VMs, load balancing, and faster persistent disks. The pricing strategy of Google (GCS) is very less expensive, which charges its users by minute, with a minimum of 10 minutes. The cloud services of Google provide 100% up-time in which if a machine running in user applications requires any hardware or software patch, the software gets automatically migrated to another server.

D. AMAZON (AWS) VERSUS GOOGLE (GCP) CLOUD SERVICE PROVIDER

1. Amazon Web Service

This is a very popular supplier for the cloud communications. Whenever a customer enters his information to Amazon then it gets:

2.Firewall: The overall firewall ports are closed by default and it means that the client himself will have to unlock docks of inward visit. Amazon offers skill for crack layers of entrance groups.

3.Isolation instances: Numerous visitors will organize over the single physical machine. Though case does not have straight entrance to the physical disk, they are specified entrance to the virtual information storage. To keep away from mutual influence of virtual information of dissimilar cases located over one single physical machine, the program offers a double-check before "giving" empty space to another case. Therefore, in paying concentration to information contact evasion, Amazon gives a great level of security for every case. To make sure that the information from dissimilar applications don't manipulate everyone in the case of disk space release, data from every of the storage units is automatically deleted (the value is set as zero).

4.Hypervisor: Amazon EC2 utilizes a customized version of the Xen hypervisor that will be considerably civilizing the presentation of virtual machines via para-virtualization after that it will get entrance to the central processing unit comes with split rights. The guest operating g system is at level 1, the host operating g system had the greatest at level 0, as well as the applications had at least rights at level 3.

5.Security of the host operating system: A multi-factorial authentication system has been designed for managerial entrance to the host's management. If a worker no longer requires this entrance, then their account is stopped automatically.

6.Guest Operating system security: Support for security here lies completely over the expansion team, like the suppliers don't have entrance for both the guest as well as instances the OS which is installed on it. This is, in real, an advantage in the terms of application safety, but also makes possible susceptibilities for the assaults. Configuration errors might offer assailant entrance to the facts, applications, as well as the overall virtual machines.

7.API access: API calls to begin and break off change firewall settings, instances, as well as the other tasks which are marked via a secret key. Entrance to an API is not possible lacking of it. Moreover, the API calls are encrypted utilizing a cryptographic SSL protocol.

8.Multilevel safety: Safety mechanism has been designed at numerous levels -- firewalls, virtual instances, for host OS, virtual guest Operating system, as well as API calls.

9.Security Groups, Network ACLS, and Firewalls:

Amazon cloud computing system is enriched with both security groups and network ACLs, where user can control the incoming and outgoing levels. In Amazon Cloud services, the Network ACLs works at subnet level, where it can allow or deny specific IP address keeping a track of the security concerns.

E. Google Cloud Platform

Now, there are the data safety squad which has like 500 specialists in, request, system safety as well as data, that group has been assigned with preserving the firm's safety systems, rising safety appraisal procedures, applying Google's safety strategies as well as structuring safety transportation.

F. DECIDING WHAT, WHEN, AND HOW TO MOVE TO THE CLOUD

All the way through this direction a wide proposal have been offered over decreasing the peril when adopting cloud computing, but still they did not cover the overall necessary proposal and still sensible for the entire cloud deployment. Also from the information that was collected from different working groups, it was soon realized that there simply is not enough space to provide a degree of accuracy in completely difference proposals for overall potential danger situations. Merely like it may be a very dangerous application it is significant that the transition to public cloud supplier, there may be little or no cause to pertain a wide safety controls for low-value facts migration towards the cloud storage.

With a lot of choices of dissimilar cloud deployment such as the SPI service models, public versus private deployment that might wrap the overall situations.

Companies would take on a risk-based loom to the transition to the cloud as well as choose safety choices. What follows an easy structure in order to assist assess the risk of primary and Cloud informed security decisions.

G. Identify the asset for the cloud deployment

In simplest, the property that carried via cloud is data or application/function.

The very Initial stage in risk assessment for the cloud is to determine precisely what statistics or function it is measured in the cloud. And it should contain the possible exercises for the assets once this shifts to cloud to calculate the range crawl.

H. Evaluate the asset

After that another stage is to determine how significant the facts and information or function is for the company. You do not need to make detailed evaluation process only if your organization's procedure for it, but you need at least an uneven measurement of the origin of the sensitivity it is, and how important it is for Application / function / process. Essentially we are assessing honesty, privacy as well as accessibility necessities for the asset.

I. Map the asset to potential cloud deployment models

And now there will be the third stage which is determining the consumption representation we are contented with. Before we start gazing at the possible supplier, you must understand that if you can recognize the dangers implied to several consumption representations such as: personal, civic, social and mixture.

Same goes for the hosting situations such as: exterior, interior, and joint.

J. Security Guidance For Individual Users

This part gives a narrow sequence of steps for the cloud clients in order to assess as well as organize the safety of their exercise for the cloud services, with the aim of extenuating risk as well as allocating a suitable level of support.

K. Security Guidance For Enterprices

There are seven the most important steps that SMEs s will have to follow it whenever; choosing a Cloud provider, organizing a cloud contract as well as thinking about a cloud service. Cloud security is still a major concern for small and medium-sized enterprises (SMEs), and still often cited as a major obstacle to the transition to the cloud. This is understandable; security breaches can have a significant negative impact to the business sector.

VII .CONCLUSION

Cloud computing technology is a computing model that has gained much attention in the industry and in the education sector. Data security is a critical consideration for those who may wish to deploy cloud computing applications in their organizations. This project has discussed some of the basic concepts of cloud computing. It has also introduced the security issues in cloud computing. It particularly defines the data security model in cloud computing.

Additionally, the project presented an analysis of each of the issues and provides some security solutions on the basis of the available techniques. The major data security threat for databases in cloud environment is the issue of availability, unreliable access control mechanisms, poor monitoring and unreliable auditing tools. Other issues include improper encryption, key management technology besides poor data sanitization possibilities. There are some of the security measures that may be eliminated through proper counter-measures. Unfortunately, there are some that are quite challenging to eliminate using counter-measures as no standard solutions exist.

REFERENCES

1-Adam. A Noureddine & Meledath Damodaran (2008). “Security in Web 2.0 Application Development,” iiWAS '08, Proc. of the 10th International Conference on Information Integration and Web-based Applications & Services, pp. 681-685, SBN: 978-1-60558-349-5, DOI: 10.1145/1497308.1497443.

2-Aleksander P. Czarnowski (2014). Service availability (in the clouds).

3-Shwetha Bindu & Yadaiah (2011). “Secure Data Storage In Cloud Computing”, International Journal of Research in Computer Science, Vol 1 Issue 1, pp. 63-73, 2011.

4-Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146.

5- Balachandra, P. V. Ramakrishna & A. Rakshit (2009). "Cloud Security Issues", IEEE International Conference on Services Computing Security Issues, pp. 517-520.

6-Delettre K., Boudaoud and Riveill (2011). “Cloud computing, security and data concealment,” in Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC ’11), pp. 424–431.

7-Ram and Sreenivaasan (2010). “Security as a service (sass): securing user data by coprocessor and distributing the data,” in Proceedings of the 2nd International Conference on Trendz in Information Science and Computing, (TISC '10), pp. 152–155, IEEE.

8-Cloud Security Alliance (CSA)’s Security Guidance for Critical Areas of Focus in Cloud Computing (2009). Available Online at: https://cloudsecurityalliance.org/csaguide.pdf (Accessed on: March 11, 2016).

9-Cloud Security Alliance (2010). Top threats to cloud computing.

10-Cloud Security Alliance (2011). Security guidance for critical areas of focus in cloud computing V3.0. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

11- Cong Wang, Qian Wang, Kui Ren, Wenjing Lou (2011). "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing.

12- Creeger, M., (2009). CTO roundtable: Cloud computing. Communications of the ACM 52(8): 50–56.

13- Kanchana & Dr. Dhandapani (2013). "A Novel Method for Storage Security in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT), Vo 2, Issue 2, pp. 243-249.

14- Klein (2013). "Data security for digital data storage," U.S. Patent Application.

15-Catteddu (2010). Cloud computing: benefits, risks and recommendations for information security. Web Application Security, pages 17–17, 2010. 25, 26, 63.

16-Chen & Zhao (2012). "Data security and privacy protection issues in cloud computing," in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), vol. 1, pp. 647–651.

17-Dimitrios Zissis & Dimitrios Lekkas (2010). Addressing cloud computing security issues. Future Generation Computer Systems, 28 (2012) 583–592.

18-Pinheiro, W.-D. Weber, & L. A. Barroso (2007). "Failure trends in a large disk drive population," in Proceedings of the 5th USENIX conference on File and Storage Technologies (FAST '07), vol. 7, pp. 17–23.

19-Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15th March 2016.

20-Krumm (2009). "A survey of computational location privacy," Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391–399.

21-Winkler (2011). Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBill Meine, Elsevier Publishing.

22-Jonathan Katz (2002). "Efficient Cryptographic Protocols Preventing Man in the Middle Attacks," Doctoral Dissertation submitted at Columbia University. ISBN: 0-493-50927-5. http://www.cs.ucla.edu/~rafail/STUDENTS/katzthesis.pdf /

23-Josh Karlin, Stephanie Forrest, Jennifer Rexford (2008). "Autonomous Security for Autonomous Systems," Proc. of Complex Computer and Communication Networks; vol. 52, issue. 15, pp. 2908- 2923, Oct. 2008, Elsevier North-Holland, Inc. New York, NY, USA.

24-Juniper Networks (2009). "Security Consideration for Cloud Ready DataCentres,". http://www.juniper.net/us/en/local/pdf/whitepapers/2000332-en.pdf

25-Huang & R. Tso (2012). "A commutative encryption scheme based on ElGamal encryption," in Proceedings of the 3rd International Conference on Information Security and Intelligent Control (ISIC '12), pp. 156–159, IEEE.

26-Hwang & Li (2010). "Trusted cloud computing with secure resources and data coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14–22.

27-Vieira (2010). "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, DOI: 10.1109/MITP.2009.89.

28-Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina & Eduardo B Fernandez (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4:5.

29-Kevin Hamlen (2010). The Security Issues for cloud computing. International Journal of Information Security and Privacy, 4(2), 39-51.

30-Kim-Kwang Raymond Choo (2010). Cloud computing: Challenges and future directions. Trends & issues in crime and criminal justice. No. 400.

31-Rodero-Merino, L.M. Vaquero, V. Gil, F. Gal´an, J. Font´an, R.S. Montero, & I.M. Llorente (2010). From infrastructure delivery to service management in clouds. Future Generation Computer Systems, 26(8):1226–1240.

32-Vaquero, L. Rodero-Merino, J. Caceres, & M. Lindner (2008). A break in the clouds: towards a cloud definition, in: ACM SIGCOMM Computer Communication Review, p.50-55.

33-Leighon, T. (2009). Akamai and Cloud Computing: A Perspective from the Edge of the Cloud. White Paper. Akamai Technologies. Available online at: http://www.essextec.com/assets/cloud/akamai/cloudcomputing-perspective-wp.pdf. (Accessed on: March 14, 2016).

34-Levelcloud, 2016. http://www.levelcloud.net/why-levelcloud/cloud-education-center/advantages-and-disadvantages-of-cloud-computing/. Accessed on 25th March, 2016.

35-MCAfee (2012). Database Security in Virtualization and Cloud Computing Environments. Three key technology challenges in protecting sensitive data. White Paper.

36-NIST (2009). The NIST Definition of Cloud Computing, Information Technology Laboratory.

37-NIST (2011). Guidelines on Security and Privacy in Public Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

38-Mahajan, S. Setty, S. Lee et al., (2011). “Depot: cloud storage with minimal trust,” ACM Transactions on Computer Systems, vol. 29, no. 4, article 12.

39-Paul Rubens (2011). Ensuring Data Security in the Cloud. Available at: http://www.esecurityplanet.com/trends/article.php/3933241/Ensuring-Data-Security-in-the-Cloud.htm.

40-R. Velumadhava Rao & K. Selvamani (2015). Data Security Challenges and Its Solutions in Cloud Computing. International Conference on Intelligent Computing, Communication & Convergence, 48, 204 – 209.

41-Ritesh Srivastav (2015). Software as a Service (SaaS). Available on http://www.insuranceportal.tk/2015/12/software-as-servicesaas.html. Accessed on 25th March, 2016.

42-Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki, & Sugata sanyal (2014). A survey on security issues in Cloud Computing. 2067 – 3809.

43-Subashini & Kavitha (2011). “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11.

44-Subashini & Kavitha (2010). "A survey on security issues in service delivery models of cloud computing". Journal Network Computer Application.

45-Salesforce (2015). Why Move To The Cloud? 10 Benefits of Cloud Computing. Available on https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html. Accessed on 26th March, 2016.

46-Somani U., (2010). Implementing digital signature with RSA encryption algorithm to enhance the data Security of Cloud in Cloud Computing. In: 1st International conference on parallel distributed and grid Computing (PDGC). IEEE Computer Society Washington, DC, USA, pp 211–216.

47-Tebaa M, (2012). Homomorphic encryption method applied to Cloud Computing. In: National Days of Network Security and Systems (JNS2). IEEE Computer Society, Washington, DC, USA, pp 86–89.

48-Techpluto (2016). Latest Cloud Computing Threats To Organizations & Prevention Strategies. Available at: http://www.techpluto.com/latest-cloud-computing-threats-to-organizations-prevention-strategies/.

49-Te-Shun Chou, 2013. Security Threats on Cloud Computing Vulnerabilities. International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3.

50-Torry Harris, 2015. Overview of cloud computing. Could-computing-overciew.pdf.

51-Wang. C, Ren. K, Lou.W & Li (2012). "Toward publicly auditable secure cloud data storage services. Network", IEEE Proc. pp.19-24.

52-Wylie J, Bakkaloglu M, Pandurangan V, Bigrigg M, Oguz S, Tew K, Williams C, Ganger G, & Khosla P (2001). Selecting the right data distribution scheme for a survivable Storage system. CMU-CS-01-120, Pittsburgh, PA.

53-Xu K, Zhang X, Song M, Song J (2009). Mobile Mashup: Architecture, Challenges and Suggestions. In: International Conference on Management and Service Science. MASS’09. IEEE Computer Society, Washington, DC, USA, pp 1–4.

54-Yunchuan Sun, Junsheng Zhang, Yongping Xiong, & Guangyu Zhu (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks.

55-Shen, L. Li, F. Yan, and X. Wu (2010). “Cloud computing system based on trusted computing platform,” in Proceedings of the International Conference on Intelligent Computation Technology and Automation (ICICTA ’10), vol. 1, pp. 942–945, IEEE.

56-Xiao & Xiao (2013). Security and Privacy in Cloud Computing, Communications Surveys and Tutorials, IEEE. 15(2): 843-859.

57-Zouheir Trabelsi (2004). "Malicious Sniffing System Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet (SAINT'04), pp. 201-207, 2004, ISBN: 0-7695-2068-5.

58-Zouheir Trabelsi, Hamza Rahmani, Kamel Kaouech, & Mounir Frikha (2004) . "Malicious Sniffing System Detection Platform", Proceedings of the International Symposium on Applications and the Internet (SAINT'04), pp. 201-207, 2004, ISBN: 0-7695-2068-5.

59-http://www.computerweekly.com/opinion/Cloud-security-for-SMEs-7-key-steps

الفهـــرس