Global Scientific JOURNALS

GSJ: Volume 7, Issue 7, July 2019, Online: ISSN 2320-9186
www.globalscientificjournal.com

CLOUD COMPUTING SECURITY ISSUES AND THREATS IN BUSINESS ENVIRONMENT

Faisal Imran[1]

Email: faisalimran.cs@gmail.com
Department of Computer Science and Engineering
Chongqing University, Chongqing China

Dr. Yin Yunfei[2]

Email: yinyunfei@cqu.edu.cn
Department of Computer Science and Engineering
Chongqing University, Chongqing China

Mohammad Ikram[3]

Email: ikram1994@hotmail.com
Department of Communication Engineering
Chongqing University, Chongqing China

ABSTRACT: Cloud computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. In today's era, it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud computing stores the data and disseminated resources in the open environment, security has become the main obstacle which is hampering the deployment of Cloud environments. Even though the Cloud Computing is promising and efficient, there are many challenges for data security as there is no vicinity of the data for the Cloud user. In this report, I with the help of related survey studied different research papers in the field of Cloud Security. I identified different Issues, Vulnerabilities, Threads, Challenges and Risk associated to Cloud Security. Some contribution and proposed techniques to Cloud Security by different researchers are studied in-depth and mentioned in related work section.

KEYWORDS: Cloud Computing, Service Models, Deployment Models, Security Issues

1. INTRODUCTION TO CLOUD COMPUTING

Before going to study the Cloud Computing Security we should know about the Cloud Computing. Cloud computing is quickly becoming one of the most popular and trendy phrases being tossed around in today's technology world. It is the big new idea that will supposedly reshape the information technology (IT) services landscape. According to the researchers, it changes the way of today's computing. The first reference to the Cloud" originated from the telephone industry in the early 1990s, when Virtual Private Network (VPN) service was first offered. Rather than hard-wire data circuits between the provider and customers, telephone

companies began using VPN-based services to transmit data. This allowed providers to offer the same amount of bandwidth at a lower cost by rerouting network traffic in real-time to accommodate ever-changing network utilization. One of the main driving forces behind the development of cloud computing was to fully harness the already existing, but under-utilized computer resources in data centers. Cloud computing is, in a general sense, on-demand utility computing for anyone with access to the cloud. It offers a plethora of IT services ranging from software to storage to security, all available anytime, anywhere, and from any device connected to the cloud [1]. According to [2], architecture of Cloud Computing is given below

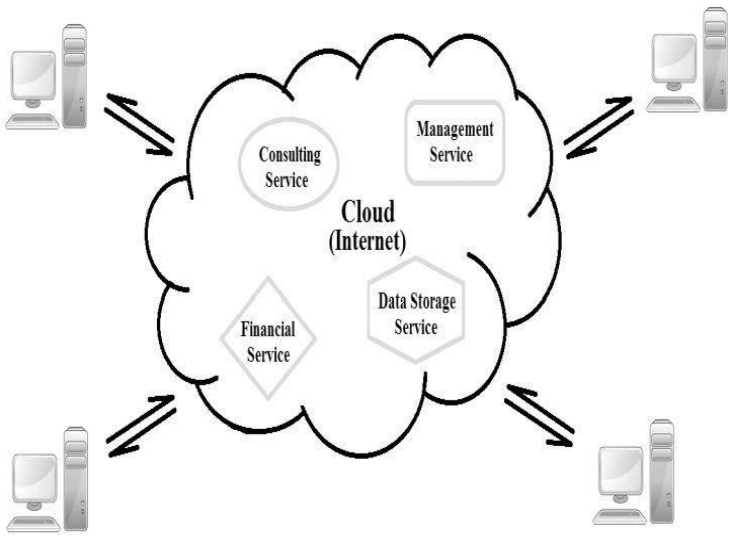

Figure 1: Architecture of Cloud Computing [1]

The advantages of using cloud computing include:

- Reduced hardware and maintenance cost,
- Accessibility around the globe, and
- Flexibility and highly automated processes wherein the customer need not worry about mundane concerns like software up-gradation.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage devices and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In such an environment users need not own the infrastructure for various computing services. In fact, they can be accessed from any computer in any part of the world. According to the different types of services offered, cloud computing can be considered to consist of three layers:

Infrastructure as a Service (*IaaS):* is the lowest layer that provides basic infrastructure support service.

Platform as a Service (*PaaS):* layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications.

Software as a Service (SaaS): is the top most layer which features a complete application offered as service on demand. Cloud services can be deployed in four ways depending upon the customers' requirements [3]:

Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party. Multiple enterprises can work on the infrastructure provided, at the same time. Users can dynamically provision resources through the internet from an off-site service provider. Wastage of resources is checked as the users pay for whatever they use

Private Cloud: Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider. This uses the concept of virtualization of machines, and is a proprietary network.

Community cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider.

Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. Moreover, with the technological advancements, we can see derivative cloud deployment models emerging out of the various demands and the requirements of users [3].

2. CLOUD COMPUTING SECURITY

The cloud computing model represents a new paradigm shift in internet-based services that delivers highly scalable distributed computing platforms in which computational resources are offered 'as a service'. Although the cloud model is designed to reap uncountable benefits for all cloud stakeholders including cloud providers (CPs), cloud consumers (CCs), and service providers (SPs), the model still has a number of open issues that impact its credibility. Security is considered one of the top ranked open issues in adopting the cloud computing model, as reported by IDC. A reasonable justification of such increasing concerns of the CCs about cloud security includes [4];

- The loss of control over cloud hosted assets (CCs become not able to maintain their Security Management Process (SMP) on the cloud hosted IT assets)

- The lack of security guarantees in the SLAs between the CPs and CCs.

- The sharing of resources with competitors or malicious users. Accordingly, no matter how strongly the model is secured, consumers continue suffering from the loss of control and lack of trust problems.

On the other hand, the CPs struggle with the cloud platform security issues because the cloud model is very complex and has a lot of dimensions that must be considered when developing a holistic security model including the complex architecture of the cloud model, the model characteristics, the long dependency stack, and the different stakeholders' security needs. These dimensions result in a large number of heterogeneous security controls that must be consistently managed. Moreover, the CPs host services they are not always aware of the contents or the security requirements to be enforced on these services. This leads to a loss of security control over these services and the cloud platforms. Although much research into cloud services security engineering has been undertaken, most efforts focus only on the cloud based services offered as web services. Such efforts have investigated capturing security requirements and generating corresponding WS-Security configurations. However, they pay no attention to the underlying platform security or the other cloud service delivery models such as IaaS and SaaS. They also do not address the impact of the multi-tenancy feature introduced by the cloud model on the security of the cloud delivered services. Two new community projects are trying to tackle the CCs trust problem by introducing a list of best practices and checklists such as CSA - GRC project, or by aligning existing security standards to the cloud model such as Fed RAMP . Both projects' focus is to obtain CCs trust by assessing and authorizing the cloud platforms. These projects lack the consumers'

involvement in specifying their security requirements and managing their SMP. The later project fits better with CPs deliver their own services only [4].

Moreover, since the IT infrastructure is now under control of the cloud provider, the customer as not only to trust the security mechanisms and configuration of the cloud provider, but also the cloud provider itself. When data and computation is outsourced to the cloud, prominent security risks are: malicious code that is running on the cloud infrastructure could manipulate computation and force wrong results or steal data; personnel of the cloud provider could misuse their capabilities and leak data; and vulnerabilities in the shared resources could lead to data leakage or manipulated computation. In general, important requirements of cloud clients are that their data is processed in a confidential way (confidentiality), and that their data and computation was processed in the expected way and has not been tampered with integrity and verifiability [5].

In paper [6], researchers employ an attribute-driven methodology to conduct their review. They employ the ecosystem of cloud security and privacy in view of five security/privacy attributes (i.e. confidentiality, integrity, availability, accountability and privacy-preservability), shown in Fig. 2, that are the most representative ones in current research advances. in this paper privacy kept separate from security due to its importance and specialty in cloud environments. Privacy is considered as highly relevant to security, as well as other security attributes that have positive or negative influences on privacy. The security ecosystem is generic and is applicable to any computer and networked systems.

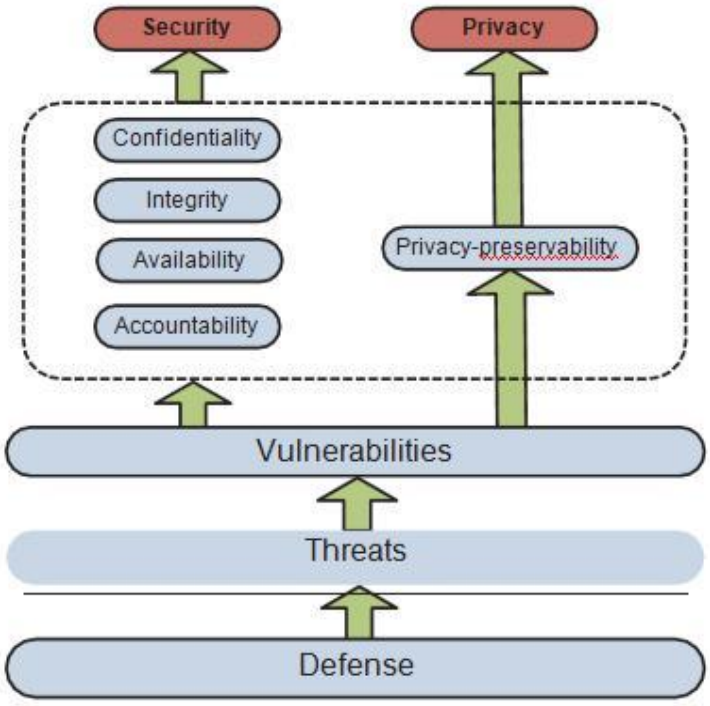

Figure 2: Ecosystem of Cloud Security and Privacy [2].

3. RELATED WORK / DIFFERENT APPROACHES TO CLOUD COMPUTING SECURITY

In paper [4], researchers introduce a new cloud security management framework based on ligning the ISMA standard to fit with the cloud computing model, enabling cloud providers and consumers to be security certified. The framework is based on improving collaboration between cloud providers, service providers and service consumers in managing the security of

the cloud platform and the hosted services. It is built on top of a number of security standards that assist in automating the security management process. Researchers have developed a proof of concept of their framework using .NET and deployed it on a tested cloud platform. They evaluated the framework by managing the security of a multitenant SaaS application exemplar.

Authors in paper [5], focus on applications where the latency of the computation should be minimized, i.e., the time from submitting the query until receiving the outcome of the computation should be as small as possible. To achieve this authors shows how to combine a trusted hardware token (e.g., a cryptographic coprocessor or provided by the customer) with Secure Function Evaluation (SFE) to compute arbitrary functions on secret (encrypted) data where the computation leaks no information and is verifiable. The token is used in the setup phase only whereas in the time-critical online phase the cloud computes the encrypted function on encrypted data using symmetric encryption primitives only and without any interaction with other entities.

Paper [7] highlights and categorizes many of security issues introduced by the "cloud"; surveys the risks, threats and vulnerabilities, and makes the necessary recommendations that can help promote the benefits and mitigate the risks associated with Cloud Computing. In paper [9] authors discusses the current use of cloud computing in government, and the risks–tangible and intangible–associated with its use. Examining specific cases of government cloud computing, and explore the level of understanding of the risks by the departments and agencies that implement this technology. This paper argues that a defined risk management program focused on cloud computing is an essential part of the government IT environment.

Authors proposes RSA algorithm in [10], to encrypt the data to provide security so that only the concerned user can access it. By securing the data, unauthorized access are not allowed to use it. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider; Cloud provider authenticates the user and delivers the data. Author in [11], proposes a layered based approach for security in CC. The purpose of this paper is to offer a macro level solution for identified common infrastructure security requirements. This model with a number of emerged patterns can be applied to infrastructure aspect of Cloud Computing as a proposed shared security approach in system development life cycle focusing on the plan-built-run scope. Authors in [12], propose a DDoS attack mitigation architecture that integrates a highly programmable network monitoring to enable attack detection and a flexible control structure to allow fast and specific attack reaction. To cope with the new architecture, they propose a graphic model based attack detection system that can deal with the dataset shift problem. In paper [13], the authors focus on Cloud Computing, which is a distributed architecture that centralizes server resources on quite a scalable platform so as to provide on demand' computing resources and services The authors outline what cloud computing is, the various cloud employment models and the main security risks and issues that are currently present within the cloud computing industry.

According to [14], IaaS serves as the foundation layer for the other delivery models, and a lack of security in this layer will certainly affect the other delivery models, i.e., PaaS, and SaaS that are built upon IaaS layer. This paper presents an elaborated study of IaaS components' security and determines vulnerabilities and countermeasures. Finally, as a result of this research, we propose a Security Model for IaaS (SMI) to guide security assessment and enhancement in IaaS layer. In paper [15], researchers, explain the cloud computing along with its open secure architecture advantages in brief and emphasize on various security threats in cloud computing also the existing methods to control them along with their pros and cons.

A framework comprising of different techniques and specialized procedures is proposed in paper [16], that can efficiently protect the data from the beginning to the end, i.e., from the owner to the cloud and then to the user. We commence with the classification of data on the basis of three cryptographic parameters presented by the user, i.e., Confidentiality (C), Availability (A) and Integrity The strategy followed to protect the data utilizes various measures such as the SSL (Secure Socket Layer) 128-bit encryption and can also be raised to 256-bit encryption if needed, MAC (Message Authentication Code) is used for integrity check of data, searchable encryption and division of data into three sections in cloud for storage. The division of data into three sections renders supplementary protection and simple access to the data. The user who wishes to access the data is required to provide the owner login identity and password.

4. SECURITY RISK, THREATS AND VULNERABILITIES

Vulnerability" refers to a software, hardware, or procedural weakness that may provide an attacker the open door to enter a computer or network and have unauthorized access to resources within the environment. Vulnerability characterizes the absence or weakness of a safeguard that could be exploited. "Threat" is any potential danger to information or systems. The threat is that someone, or something, will identify a specific vulnerability and use it against the company or individual. "Risk" is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact [7], here in this paper researchers conduct a survey and indentified some Risks associated with CC Security which are mentioned below in Fig.3

Information security risks in Cloud Computing (CC) were subject for detailed analysis and assessment. One of the best efforts in this direction was realized by the European Network

Information Systems Agency (ENISA) whom developed a comprehensive detailed research in this regards. Other groups such as Cloud Security Alliance (CSA) who specialize in cloud computing technology and information security matters also have significant publications. ENISA classifies Cloud Computing (CC) risks into three categories: Organizational, Technical and Legal. CSA threats model avoids classifying

CC's risks but yet introduce a detailed list of considerable issues that need to be properly addressed [5]. The organizational risks classification includes all risks that may impact the structure of the organization or the business as an entity. business reputation due to co-tenant activities and any organizational change that can happen to the cloud provider (as a business organization) including provider failure, termination or acquisition.

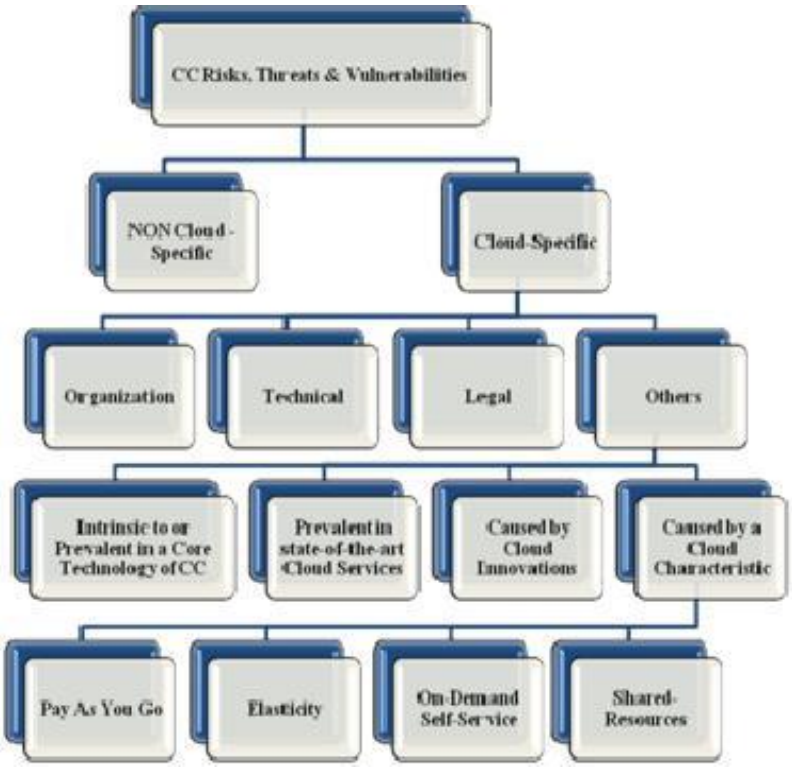

Figure 3: Cloud Computing Risks, Threats & Vulnerabilities [3].

The technical risks classification includes problems or failures associated with the provided services or technologies contacted from the cloud service provider. Examples of such risks include, but not limited to, resource-sharing isolation problems, malicious (insiders or outsiders) attacks on the cloud provider, and any possibility of data leakage on download/upload through communication channels [7].

The legal risks classification refers to issues that surround data being exchanged across multiple countries that have different laws and regulations concerning data traversal, protection requirements and privacy laws. Examples of such risks include, but not limited to, risks resulting from possible changes of jurisdiction and the liability or obligation of the vendor in case of loss of data and/or business interruption.

Cloud Computing is based on a new utilization of technology and many risks that used to be present in other technological implementations do still exist, and are realized as not cloud specific. Risks like social engineering, physical security, lost or stolen backups, and loss or compromise of security logs are just a few examples of such general security risks. The Cloud Security Alliance (CSA) lists the following threats as the top risks associated with CC based on their recent research: malicious insiders, data loss/leakage, abuse and nefarious use of CC and shared technology vulnerabilities. Even though CSA prefers to prioritize risks, it easy to see that each of the listed threats can be included in the ENISA categories or as non-cloud specific, or general, security risk [7]. Other researchers prefer to focus on cloud specific vulnerabilities, without much focus on threats and risks. According to such research, a particular vulnerability can be considered specific to cloud computing if it meets any of the following criteria [8]:

- It is intrinsic to or prevalent in a core technology of cloud computing, such as virtualization, service-oriented architecture, and cryptography.

- It has its root cause in one of essential cloud characteristics, such as elasticity, resource pooling, and pay-as-you-go model

- It is caused by cloud innovations making exiting (tried and tested) security controls hard or impossible to implement; for example, management procedures that were created initially for a fixed hardware structure do not port correctly to virtual machines.

- It is prevalent in established state-of-the-art cloud services.

To appropriately assess the risks that are introduced to an organization when using cloud computing, these four categories based on the Economist's Business Risk model (Managing Business Risks in the Information Age, 1998) can be used to identify possible risks: access, availability, infrastructure, and integrity [9]. In paper [15], authors identified top seven security threads to CC that are listed below:

- Abuse and Nefarious Use of Cloud Computing.
- Insecure Application Programming Interfaces.
- Malicious Insiders.
- Shared Technology Vulnerabilities.
- Data Loss/Leakage.
- Account, Service & Traffic Hijacking.
- Unknown Risk Profile.

5. SECURITY ISSUES AND CHALLENGES IN CLOUD COMPUTING

As we know that there are two main kind of Cloud Computing i.e. Public Cloud and Private Cloud, so we discuss security issues for both.

- **Security issues in a Public cloud [3]**

1) Three basic requirements of security: confidentiality, integrity and availability are required to protect data throughout its lifecycle. Data must be protected during the various stages of creation, sharing, archiving, processing etc. However, situations become more complicated in case of a public cloud where we do not have any control over the service provider's security practices.

2) In case of a public cloud, the same infrastructure is shared between multiple tenants and the chances of data leakage between these tenants are very high. However, most of the service providers run a multitenant infrastructure. Proper investigations at the time of choosing the service provider must be done in order to avoid any such risk.

3) In case a Cloud Service Provider uses a third party vendor to provide its cloud services, it should be ensured what service level agreements they have in between as well as what are the contingency plans in case of the breakdown of the third party system.

4) Proper SLAs defining the security requirements such as what level of encryption data should undergo, when it is sent over the internet and what are the penalties in case the service provider fails to do so.

- **Security issues in a Private Cloud [3]**

5) Virtualization techniques are quite popular in private clouds. In such a scenario, risks to the hypervisor should be carefully analyzed. There have been instances when a guest operating system has been able to run processes on other guest VMs or host.
6) The host operating system should be free from any sort of malware threat and monitored to avoid any such risk. In addition, guest virtual machines should not be able to communicate with the host operating system directly. There should be dedicated physical interfaces for communicating with the host.
7) In a private cloud, users are facilitated with an option to be able to manage portions of the cloud, and access to the infrastructure is provided through a web interface or an HTTP end point. There are two ways of implementing a web-interface, either by writing a whole application stack or by using a standard applicative stack, to develop the web interface using common languages such as Java, PHP, and Python etc. As part of screening process, Eucalyptus web interface has been found to have a bug, allowing any user to perform internal port scanning or HTTP requests through the management node which he should not be allowed to do. In the nutshell, interfaces need to be properly developed and standard web application security techniques need to be deployed to protect the diverse HTTP requests being performed.
8) While we talk of standard internet security, we also need to have a security policy in place to safeguard the system from the attacks originating within the organization. This vital point is missed out on most of the occasions, stress being mostly upon the internet security. Proper security guidelines across the various departments should exist and control should be implemented as per the requirements.

Some other issues related to Cloud Security are mentioned below according to paper [17].

Multi-Tendency : Multi-tenancy, as the term implies, refers to having more than one tenants of the cloud living and sharing other tenants the provider's infrastructures, including computational resources, storage, services, and applications. By Multi-Tendency, clouds provide simultaneous, secure hosting of services for various customers utilizing the same cloud infrastructure resources. Multi-tenancy is a feature unique to resource sharing in clouds, especially in public clouds. Essentially, it allows cloud providers to manage resource utilization more efficiently by partitioning a virtualized, shared infrastructure among various customers. High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. Virtualization and multi-tenancy are the big issues on using cloud computing. As the cloud is a shared resources environment, organization want to ensure that all tenant domains are properly isolated from each other that no possibility exists for data or transactions to leak from one tenant domain into the next. Clients need the ability to configure trusted virtual domains or policy-based security zones.

Elasticity: Elasticity implies being able to scale up or down resources assigned to services based on the current demand. Scaling up and down of a tenant's resources gives the opportunity to other tenants to use the tenant's previously assigned resources. This may lead to confidentiality issues. For example, when Tenant A scaled down so it releases resources, these resources are now assigned to Tenant B who in turn uses it to deduce the previous

contents of Tenant A. Moreover, elasticity contains a service placement engine that maintains a list of the available resources from the provider's offered resources pool. This list is used to allocate resources to services. Such placement engines should incorporate cloud customers' security and legal requirements such as competitors services should be avoided being placed on the same server, data location should be within the tenants' country boundaries. Placement engines may include a migration strategy where services are migrated from one physical host to another or from cloud to another in order to meet demands and efficient utilization of the resources. This migration strategy should take into account the same security constraints.

Multiple Stakeholders: In a cloud computing model there are different stakeholders involved: cloud provider, service provider, and customer. Each stakeholder has their own security management systems/processes and their own expectations (requirements) and capabilities (delivered) from/to other stakeholders. This also leads to create issues.

Third-Party Control: The major security challenge is the third-party issue, that is, the owner of the data has no control on their data processing. The biggest change for Information Technology (IT) department of the organization using cloud computing will be reduced control even as they are being tasked to bear increased responsibility for the confidentiality and compliance of computing practices in the organization.

There are many more issues in CC. following are some issues that can also be faced by implementing CC. Privacy Issue, Lack of user control, Unauthorized Secondary Usage, Trans-border Data Flow and Data Proliferation, Dynamic provision, Access Issues, Control over data lifecycle, Availability and backup, Audit, Trust and Mitigation Steps [18].

6. SUMMARY AND RESEARCH DIRECTION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users and provides easy access to high performance, computing resources and storage infrastructure through web services. Cloud computing delivers the potential for efficiency, cost savings and improved performance to governments, organizations, private and individual users. However, it also raises some security problems which may slow down its use.

In this academic report I with the help literature survey introduce the Cloud Computing and the Security associated with it. Some surveys have discussed security issues about clouds without making any difference between vulnerabilities and threats. I have focused on this distinction, where I consider important to understand these issues. Enumerating these security issues was not enough; that is why we made a relationship between threats and vulnerabilities, so we can identify what vulnerabilities contribute to the execution of these threats and make the system more robust. Here in this report I also focus to illustrate the Security aspect of Public and Private Cloud Computing and identified various Security Issues.

Cloud computing is the most modern technology so lots of issues are remained to consider. It has many open issues some are technical that includes scalability, elasticity , data handling mechanism, reliability, license software, ownership performance, system development and management and non-technical issues like legalistic and economic aspect. Cloud computing still unknown "killer application" will establish so many challenges and solutions must develop to make this technology work in practice. So the research is not stop here much work can be done in future. The model presented in this paper is the initial step and needs more modifications; however it can provide the basis for the deeper research on security deployment of cloud computing for the research community working in the field of Cloud Computing [18].

References

[1] Hu, F., Qiu, M., Li, J., Grant, T., Taylor, D., McCaleb, S., ... & Hamner, R. (2011). A review on cloud computing: Design challenges in architecture and security. CIT. Journal of Computing and Information Technology, 19(1), 25-55.

[2] Bégin, M. E., Jones, B., Casey, J., Laure, E., Grey, F., Loomis, C., & Kubli, R. (2008). An egee comparative study: Grids and clouds-evolution or revolution. EGEE III project Report, 30, 1-33.

[3] Bhadauria, R., & Sanyal, S. (2012). Survey on security issues in cloud computing and associated mitigation techniques. arXiv preprint arXiv:1204.0764.

[4] Almorsy, M., Grundy, J., & Ibrahim, A. S. (2011, July). Collaboration-based cloud computing security management framework. In Cloud Computing (CLOUD), 2011 IEEE International Conference on (pp. 364-371). IEEE.

[5] Sadeghi, A. R., Schneider, T., & Winandy, M. (2010, June). Token-based cloud computing. In International Conference on Trust and Trustworthy Computing (pp. 417-429). Springer, Berlin, Heidelberg.

[6] Xiao, Z., & Xiao, Y. (2013). Security and privacy in cloud computing. IEEE Communications Surveys & Tutorials, 15(2), 843-859.

[7] Dahbur, K., Mohammad, B., & Tarakji, A. B. (2011, April). A survey of risks, threats and vulnerabilities in cloud computing. In Proceedings of the 2011 International conference on intelligent semantic Web-services and applications (p. 12). ACM.

[8] Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, "Understanding Cloud-Computing Vulnerabilities", IEEE Security and Privacy, 10 Jun. 2010, IEEE computer Society Digital Library, IEEE Computer Society

[9] Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. Government information quarterly, 27(3), 245 253.

[10] Kalpana, P., & Singaraju, S. (2012). Data security in cloud computing using RSA algorithm. IJRCCT, 1(4), 143-146.

[11] Yildiz, M., Abawajy, J., Ercan, T., & Bernoth, A. (2009, December). A layered security approach for cloud computing infrastructure. In Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on (pp. 763-767). IEEE.

[12] Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and software-defined networking. Computer Networks, 81, 308-319.

[13] Carlin, S., & Curran, K. (2011). Cloud computing security.

[14] Dawoud, W., Takouna, I., & Meinel, C. (2010, March). Infrastructure as a service security: Challenges and solutions. In Informatics and Systems (INFOS), 2010 the 7th International Conference on (pp. 1-8). IEEE.

[15] Srinivasamurthy, S., & Liu, D. Q. (2010, November). Survey on cloud computing security. In Proc. Conf. on Cloud Computing, CloudCom (Vol. 10).

[16] Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), 1831-1838.

[17] Tianfield, H. (2012, October). Security issues in cloud computing. In Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on (pp. 1082-1089). IEEE.

[18] Alvi, F. A., Choudary, B. S., Jaferry, N., & Pathan, E. (2012). Review on cloud computing security issues & challenges. iaesjournal. com, 2.