FEAR OF CLOUD COMPUTING: IDENTIFYING RISKS INVOLVED USING STRIDE

KamalPreet Singh[1], Juhi Aggarwal[2]
Assistant Professor, University of Petroleum and Energy, Dehradun

Abstract

Computing in which services involving software, resources, infrastructure and information are delivered over the internet is known as Cloud Computing. Just like a public utility, cloud computing delivers services only on request of the user. Cloud computing provides access to a pool of shared resources that can be configured on demand. With its ability to deliver users shared and scalable resources, cloud computing has come up as an encouraging platform that avoids large fixed upfront costs and with balanced use of a services, infrastructure, information and applications. However, users' data may contain critical information. Storing this critical and sensitive information on cloud prompt intruders for various attacks creating fear in the mind of users while considering cloud computing. Thus, security is treated as most important issue to be handled in cloud computing. In this paper, various threats involved in Cloud Computing are discussed and. This paper discuss the working of cloud computing, its architecture along with its types and various risks involved in adopting its architecture and various issues involved in acceptance of this information sharing model. STRIDE threat model is used for analyzing security concerns and threats according to the kind of attacks used

Index Terms: Cloud Computing, CSP, Grid Computing, Resource Pooling

I. INTRODUCTION

Cloud computing is an assembly of already developed techniques and technologies, enclosed in a infrastructure platform that provides scalability, more flexibility, business swiftness, reduced management and maintenance costs, and round the clock availability of data and resources. The main attributes of Cloud computing that make it trending are: multitenancy, scalability, flexibility, pay as you use, and self-servicing of resources [1].

- Multitenancy:- Earlier computing models presumed allocation of dedicated resources for task completion, whereas cloud computing is based on a public utility business model in which resources are provided at the network level, host level, and application level on pay-per-use basis.
- Massive scalability:- Cloud computing provides the facility to map to large number of systems. This internet computing also has the capability to extensively scale the bandwidth and storage space.
- Flexibility:- Cloud Computing facilitate the users to briskly change the requirement of their computing resources as and when required. Resources can also be released after use when they are no more needed.
- Pay as you use:- Users only need to pay for the resources they actually use and for only the time they require those resources. They need not to either worry for the maintenance of the resources.
- Self-Servicing of resources:- Resources such as storage, processing power, software are self-provisioned according to their needs. Self-Servicing feature of

cloud computing allows users to order, provision, and use computing resources from an approved cloud services provider such as Amazon Web Services.

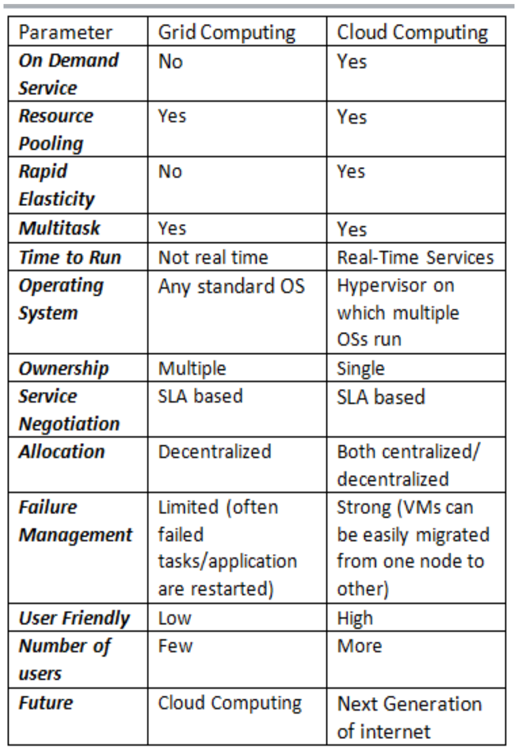
II. Cloud v/s Grid Computing

Grid computing is collaboration of multiple processors on different machines. The objective of Grid Computing is to increase the computational power of the CPU by linking different computers, forming a single consolidated infrastructure [2]. Just like a public utility, Grid Computing also provisions resources whose provision can be turned on or off. Both, cloud computing model and grid computing model are distributed in nature and facilitate common properties, such as resource pooling and broad network access [3].

Besides the server side similarity, both the models mainly differ from their client perspective. Grid Computing services lesser clients with heavy, multitude jobs whereas Cloud Computing supports lightweight storage intensive tasks for thousands of clients with multiple clients on a single node. Cloud Computing provide resources on demand which can be changed as per the need, whereas in grid or cluster, resources need to be reserved prior to use which can be further switched on or off as required. This increases flexibility and omits the possibility of over provisioning [4]. Table 1 summarizes the difference between Cloud Computing and Grid Computing.

III. Cloud Deployment Models

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units. Deploying cloud computing can vary depending on the users' requirements. As per users' need and requirements of service, there are four basic deployment models [5].



Parameter	Grid Computing	Cloud Computing
On Demand Service	No	Yes
Resource Pooling	Yes	Yes
Rapid Elasticity	No	Yes
Multitask	Yes	Yes
Time to Run	Not real time	Real-Time Services
Operating System	Any standard OS	Hypervisor on which multiple OSs run
Ownership	Multiple	Single
Service Negotiation	SLA based	SLA based
Allocation	Decentralized	Both centralized/ decentralized
Failure Management	Limited (often failed tasks/application are restarted)	Strong (VMs can be easily migrated from one node to other)
User Friendly	Low	High
Number of users	Few	More
Future	Cloud Computing	Next Generation of internet

Table 1: Difference between Cloud and Grid Computing

• **Private Cloud**:- Also known as internal cloud, has its infrastructure deployed, maintained and operated for a particular organization. Being private, these offer some benefits of cloud computing on data security, corporate governance [6]. Figure 1 shows scenario of onsite private cloud. Examples of Private Cloud: -

- Microsoft ECI data center
- Eucalyptus
- Ubuntu Enterprise Cloud - UEC
- Amazon Virtual Private Cloud (VPC)

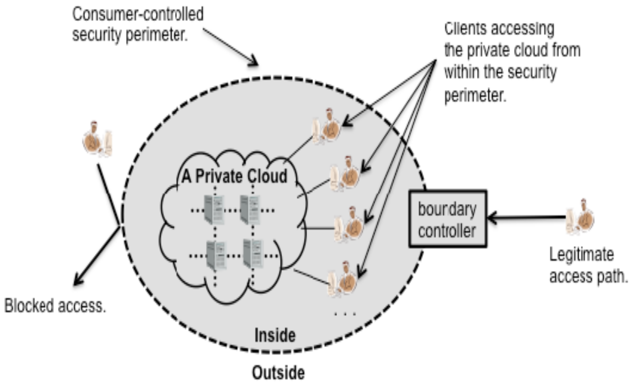

Consumer-controlled security perimeter.
Clients accessing the private cloud from within the security perimeter.
A Private Cloud
bourdary controller
Legitimate access path.
Blocked access.
Inside
Outside

Figure 1: Private Cloud

• **Public Cloud**:- Also known as External cloud, has its infrastructure hosted, operated and managed by a third party vendor, and this infrastructure is made public by a CSP, i.e, cloud service provider on financial basis. This allows users to develop and deploy a service in the cloud with minimal deployment cost involved. In comparison to private cloud, public cloud has lesser degree of control and security [7]. Figure 2 shows the Public Cloud diagrammatically. Examples of Public Cloud:

- Amazon EC2
- IBM Smart Cloud
- Microsoft Windows Azure
- Google App Engine

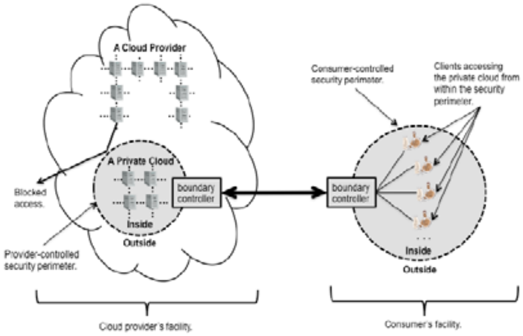

A Cloud Provider
A Private Cloud
boundary controller
Inside
Outside
Blocked access.
Provider-controlled security perimeter.
Consumer-controlled security perimeter.
Clients accessing the private cloud from within the security perimeter.
boundary controller
Inside
Outside
Cloud provider's facility.
Consumer's facility.

Figure 2: Public Cloud

• **Hybrid Cloud:-** Also known as composite cloud, is constitution of two or more clouds(private, public or community) bounded by standardized technology that enables portability of both data as well as application. In hybrid cloud, running non-core applications in public cloud while maintaining core applications and sensitive data in internal cloud combines advantages of both the world. The hybrid cloud infrastructure is capable of moving data and /or applications from one cloud to another through their interfaces. Figure 3 shows Hybrid Cloud. Examples of Hybrid Cloud are

- VMware v
- Cloud Windows Azure

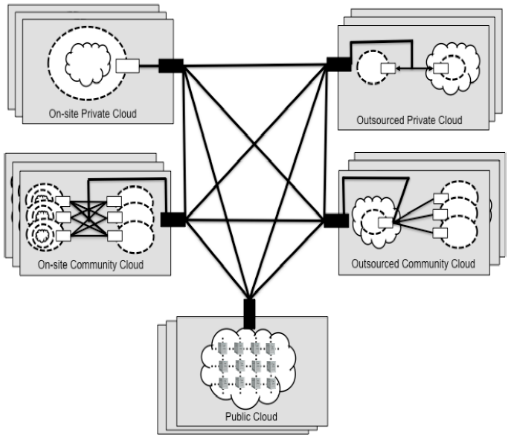


Figure 3: Hybrid Cloud

• **Community cloud:-** The organizations having similar requirements and interest share community cloud infrastructure. Since the costs are shared among the organizations, this reduces the capital expenditure costs for its establishment. Government departments, universities, central banks etc. often use this type of cloud infrastructure [8]. The operation may be in-house (On-Site Community Cloud Scenario) or with the third party (Outsourced Community Cloud) on the premises. Figure 4 shows Community Cloud.

Examples of Community Cloud:

- Google Apps for Government
- Microsoft Government Community Cloud

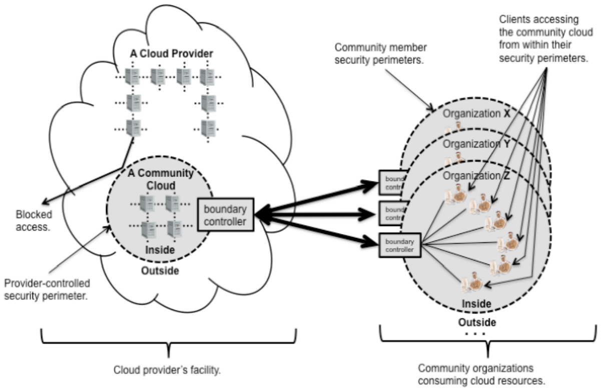

A Cloud Provider
A Community Cloud
boundary controller
Inside
Outside
Blocked access.
Provider-controlled security perimeter.
Community member security perimeters.
Clients accessing the community cloud from within their security perimeters.
Organization X
Organization Y
Organization Z
boundary controller
Inside
Outside
Cloud provider's facility.
Community organizations consuming cloud resources.

Figure 4: Community Cloud

IV. CLOUD SERVICES DELIVERY MODEL

There are three diverse kinds of cloud computing, depending upon the type of service provided by the cloud environment.

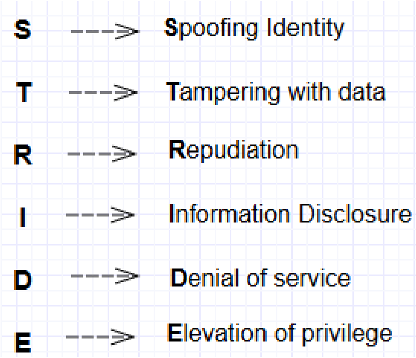
• Software-As-a-Service: Traditionally, customers had to pay a license fee for purchasing and installing the software onto their own hardware. A maintenance agreement was also required to be purchased by the customer for software upgradation and support services [9]. The compatibility issues regarding the installation of patch and operating system were headache of customer. However, in a SaaS model, instead of purchasing the software, the customer uses the software on rent basis.

•Platform-As-a-Service: In a platform-as-a-service (PaaS) model, CSP offers a platform on commercial basis to application developers for developing applications. PaaS is a variety of SaaS in which the development environment is offered as a service.

•Infrastructure-As-a-Service: Traditionally vendor used to leverage entire infrastructure to the customer for running his applications. The IaaS model provides scalable infrastructure to user as per demand on rental basis for running the applications [10].

V. Fear Of Cloud Computing

In this paper, STRIDE threat model [11] is used for analyzing security concerns and threats according to the kind of attacks used. It was developed by Microsoft to characterize known security.



S ---> Spoofing Identity

T ---> Tampering with data

R ---> Repudiation

I ---> Information Disclosure

D ---> Denial of service

E ---> Elevation of privilege

• Spoofing identity (S)

Illegal access of resources by assuming someone else' authentication details such as username and password is an example of identity spoofing. It is risky for multiuser applications which provide single connection of execution at application and database level.

• Tampering with data (T)

Data tempering is mischievous alteration of data thereby violating the integrity of data. Tempering with data can be done at database level by making unauthorized changes to persistent data or at network level by modifying data as it flows between two computers over network.

• Repudiation (R)

With poor check of audit and record keeping, malicious user can perform restricted actions without taking responsibility of that operation. Example, a user may tamper the employee data in the database and later deny performing that operation.

• Information Disclosure (I)

This treat involves disclosure of information to users who are not granted the access of that information. For example, in man in the middle attack, intruder is able to read the data sent between true users thereby leading to disclosure of information [12].

• Denial of service (D)

Denial of service (DoS) attacks hamper availability and reliability of services to genuine users by making Web Services or resources temporary inaccessible and inoperative. By flooding TCP/IP packets on database server, an attacker forbids access of legitimate user.

• Elevation of privilege (E)

In this threat, an unprivileged user increases resources' access thereby accessing unauthorized resources and becoming the part of the system itself. By elevating the privileges, attacker can damage the entire system after becoming the faithful part of the system.

A. COMPROMISATION OF DATA:

In cloud computing, large amount of users' data is placed on cloud, making cloud service provider an alluring spot for the attackers to attack. Data Compromisation occurs when user's susceptible, secured or private data is accessed, such as personal health information (PHI), personal identifiable information (PII) [13] or financial information is discharged or hijacked by an unauthorized individual. The intensity of damage is determined by the acuteness of data, which can be minimized if the data-at-rest is encrypted. Although, Cloud service providers deploy various security controls to avoid data breaches that result in compromised data, ultimately organizations are chargeable for protecting their own data in the cloud thereby creating a fear in their mind to whether shift their sensitive data to cloud or not.

On Feb 4, 2015, in Anthem medical data breach, 80 million records of user held by Anthem Inc. having personally identifiable information were stolen. The compromised information contained medical IDs, social security numbers, names, birthdays, street addresses, e-mail addresses and employment information, including income data.[14][15]

This compromised Data was supposed to be sold on the black market. [16]

B. PERMANENT DATA LOSS:

Destruction of data due to failure of storage system, malicious intrusion or accidental deletion by CSP or any other physical calamity such as earthquake, tsunami results in loss of data which is irrecoverable. Data loss can also occur in case the user loses the encryption key used to encrypt data before transferring it to the cloud. Some CSPs deliberately delete customers' data that has not been used for a long period of time for freeing their resources for monetary benefits [17]. Third Party Auditors are used by organizations to periodically check the integrity of their data present on the cloud. Information being the most valuable asset for all present-day organizations, CSPs also takes certain measures to prevent data loss such as creating back up of data and storing it at different geographical locations to avoid any data loss due to natural or accidental disasters [18].

C. CREEPY INSIDER

According to CERT, "A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

For organizations depending solely on cloud services, insider threat can be of great risk. Insider threats also include jobs that accidentally violate jurisdictions or hamper sensitive data. Detailed logging, efficient monitoring and effective auditing of activities, proper isolation of duties can minimize threats from insider.

D. PROGRESSIVE ENDLESS THREATS:

Progressive Endless Threats submissively penetrate into the computing infrastructure in order to setup a footprint in target system. Advanced Persistent Threats adaptive nature to the measures employed for security against them allow these threats to seek their motive secretly with time. Common entry points for APT include system hacking, transferring the code of attack through USB devices, spear phishing [19]. Threats of these types require users' participation; hence awareness programs are good defensive measures against such types of attacks.

E. INADEQUATE MANAGEMENT OF USERS' CREDENTIALS:

Use of weak passwords [20], absence of multifold authentication, inadequate management of users' credentials improper updating of certificates, passwords and keys on regular intervals boost up the chances of data breach and attacks. Keys used in cryptography and user credentials encapsulated in the source code are more likely to be exposed and abused.

Weak credentials allow attackers to hijack services or account. With access to cloud service credentials, attackers can snoop user activities, tamper data and information or deflect the client to invalid sites. Stolen credentials can also result in account hijacking. Common defense in depth and strong two factor authentication techniques minimize the damage of such threats

Any change in the responsibility or role of user/provider must be properly followed by immediate de-provisioning of rights and access to resources. Cryptographic keys must be secured effectively and for appropriate management of activities related to keys, secured public key infrastructure is required.

F. LACK OF KNOWLEDGE ABOUT CSP:

For smooth running of organization's business on cloud, cloud technologies and Cloud Service Provider must be properly evaluated and due diligence must also be thoroughly investigated. Hurry in adoption of cloud technology and selection of Cloud Service Provider with insufficient due diligence makes the organization open to countless compliance, technical, commercial, legal and financial risks that threats its success. Designing applications for unexplored cloud can result in unidentified architectural and operational issues for architects and designers. Buying a service from cloud results in inheriting their data security issues as well. Federal Trade Commission charged Facebook for falsifying users' privacy by supporting changes that nullify privacy setting without intimating the user and asking for users' approval. In 2011, Facebook complied to settle the complaint filed by FTC [21].

G. SUSCEPTIBLE SYSTEM:

Bugs in programs make the system vulnerable. Any vulnerability within the operating system components such as system library or kernel, allow the attackers to penetrate into the system thereby putting at risk the entire security of system. Multitenancy in cloud computing creates a new area of attack as this feature allows various organizations share cloud memory and resources and work in close proximity [22].

In order to fill the security gaps aroused due to susceptible systems, routine scanning of system must be performed followed by proper report of system threats. Installation and regular upgradation of security patches, along with secure architecture of system further minimizes such threats.

H. ODIOUS AND MISUSE/OFFENSIVE USE OF CLOUD SERVICES VIA VARIOUS METHODS SUCH AS DDOS ATTACK:

Malicious attackers target cloud service providers that offer free trial services of cloud resources and have less secured deployment models of cloud service by flooding Distributed Dos attacks thereby reducing the usage capacity of genuine users. Users and organizations using services of Cloud are affected via crooked signups of user account. Nefarious use of resources of cloud either through phishing campaign, email spams or Denial of Service attacks target users and organizations using cloud services. With DDoS attacks, attackers slow down the services of cloud service provider by targeting their limited resources such as bandwidth of network, processor power, disk space or memory [23]. Cloud services are charged as per the space used and processing power consumed by the users' process. Since DDoS attacks slow down the delivery of services to a large extent, it causes large consumption of processing time, thus resulting in large bills. This unnecessary billing of resources usage with ineffective service delivery creates a doubt of migration to cloud in consumers' mind.

To avoid such circumstances, framework for detection of any fraud and incident response must be provided by CSP to address the abusive use of resources of cloud as well as provision for the users to report any unexpected response from cloud service provider.

I. SHARING RISKS WITH CLOUD SHARED TECHNOLOGY:

CSP deliver resources to users through IaaS, PaaS, or SaaS, which can be scaled as per users' demand and requirements. This scalability is achieved by sharing applications, infrastructure or platforms which further leads to shared risks that can result in compromising of all the delivery models. Misconfiguration in any of the service model IaaS PaaS or SaaS can be to entire service provider's cloud.

The inner infrastructure components that back up Cloud Service such as GPU, CPU Cache etc. might not be constructed to support multiuser application in SaaS or portable platform as required in PaaS or multitenant architecture needed in IaaS [24]. To avoid such vulnerability that can hamper the entire service provider, defense in depth strategy is suggested which comprises of imposition of security of user, application, network, and storage as well as monitoring of the same for all three service models Iaas, PaaS or SaaS.

J. RISKY INTERFACES AND VULNERABLE APIs:

Cloud service users use application program interfaces and software user interfaces to govern and use cloud services. These interfaces, provided by CSP, are used for managing, provisioning, planning and monitoring. Thus, design of these interfaces must be robust enough to handle any malicious or accidental activity that can hamper the policy. As the availability and security of entire cloud service depends on availability and security of such interfaces, protection of such interfaces is utmost important [25].

Organizations using Cloud Services further add their own APIs with some more specific services to aid customers as per their requirements. This further extends the complexity of API increasing their risk factor. APIs and UIs are most attractive target of attacker as they are exposed outside the secured boundary of organization. The utmost important prevention measure to deal with any kind of threat is protection of such vulnerable interfaces [26].

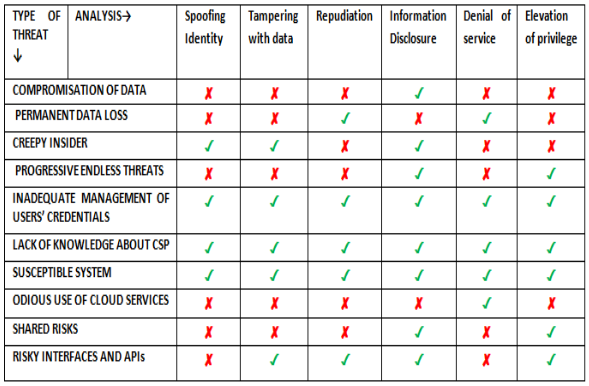
In mid-2015, Internal Revenue Service of US was hacked using "Get Transcript" program in which record of 724000 tax payers was exposed because of vulnerable API [27].

VI. Analysis of various threats using STRIDE Threat Model

Table 2 below shows various threats categorized using the STRIDE threat model. Inadequate Management of user credentials, system vulnerability, and lack of proper knowledge about Cloud Service Provider affect every perspective of threat model.

VII. Conclusion

Adopting cloud computing technique gives various benefits to the consumers such as mass storage, mobility, shared access, and cost saving, built in infrastructure. But while adopting cloud computing the customer must be smart enough to check all the legal and security aspects. This adoption of cloud computing by user as well as larger organizations will depend largely on overcoming fears of the cloud. The main fear of cloud computing is the fear of losing sensitive data. This migration of data to cloud results in loss of control of data as data is stored and managed by third party. Current control measures however do not appropriately address the cloud computing third-party data storage and processing needs. This adoption of technology mainly depends upon the need and requirement of a particular organization or an individual their sensitivity of data and information.



TYPE OF THREAT ↓	ANALYSIS→	Spoofing Identity	Tampering with data	Repudiation	Information Disclosure	Denial of service	Elevation of privilege
COMPROMISATION OF DATA		✗	✗	✗	✓	✗	✗
PERMANENT DATA LOSS		✗	✗	✓	✗	✓	✗
CREEPY INSIDER		✓	✓	✗	✓	✗	✗
PROGRESSIVE ENDLESS THREATS		✗	✗	✗	✓	✗	✓
INADEQUATE MANAGEMENT OF USERS' CREDENTIALS		✓	✓	✓	✓	✓	✓
LACK OF KNOWLEDGE ABOUT CSP		✓	✓	✓	✓	✓	✓
SUSCEPTIBLE SYSTEM		✓	✓	✓	✓	✓	✓
ODIOUS USE OF CLOUD SERVICES		✗	✗	✗	✗	✓	✗
SHARED RISKS		✗	✗	✗	✓	✗	✓
RISKY INTERFACES AND APIs		✗	✓	✓	✓	✗	✓

Table 2: Classification of Threats using STRIDE

REFERENCES

[1] R. Yadav, N. Yadav, Monika and A. Seharawat, Cloud Computing: Flowing Model in IT Services,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 3, March 2015.

[2] Hosam Al Hakami , Hamza Aldabbas, and Tariq Alwada'n International Journal on Cloud Computing: Services and Architecture (IJCCSA),Vol.2, No.4, August 2012.

[3] H. Stockinger. (2007). "Defining the grid: a snapshot on the current view". The Journal of Supercomputing, (1):3 –17.

[4] L.M. Vaquero, L.R. Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, Vol. 39, No. 1, 2009.

[5] .I. Foster, Y. Zhao, I. Raicu and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Proceedings of the IEEE Grid Computing Environments Workshop, pp. 1-10, 2008.

[6] V. Jain, V. Sharma. Surveying and analyzing security challenges and privacy in cloud computing. International Journal of Computer Science and Information Technology & Security, vol. 3(5), 2013, pp. 316-321.

[7] C. Lin, W. B. Su, K. Meng, et al. Cloud computing security: architecture, mechanism and modeling. Chinese Journal of Computers, vol. 36(9), 2013, pp. 1765-1784.

[8] X. F. Ye, B. Khoussainov. Fine-grained access control for cloud computing. International Journal of Grid and Utility Computing, vol. 4(2-3), 2013, pp. 160-168.

[9] S. Naser, S. Kamil, N. Thomas. A case study in inspecting the cost of security in cloud computing. Electronic Notes in Theoretical Computer Science, vol. 318(11), 2015, pp. 179-196.

[10] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proc. of ICDCS'10, 2010.

[11]https://msdn.microsoft.com/en-us/library/ ee823878 (v=cs.20).aspx

[12] Y. Chen, V. Paxson, R. H. Katz. What's new about cloud computing security? Technical Report UCB/EECS-2010-5, Electrical

Engineering and Computer Sciences, University of California at Berkeley, 2010.

[13] https://afmc.org/review/

[14] Weise, Elizabeth (5 February 2015). "Massive breach at health care company Anthem Inc.". USA Today. McLean, VA: Gannett. ISSN 0734-7456. Retrieved 20 February 2017.

[15] Mathews, Anna; Yadron, Danny (4 February 2015). "Health Insurer Anthem Hit by Hackers - WSJ". wsj.com. Retrieved 20 February 2017.

[16] Murphy, Tom; Bailey, Brandon (6 February 2015). "Why hackers are targeting the medical sector". bostonglobe.com. Retrieved 20 February 2017

[17] I. N. C. S. Narayana; G. Gopinath, K. P. C. Mogan, et al. A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment. International Journal of Grid and Utility Computing, vol. 5(4), 2014, pp. 236-248.

[18] M. Mowbray, S. Pearson, and Y. Shen, ”Enhancing privacy in cloud computing via policy-based obfuscation.” Springer Berlin / Heidelberg, 2010, pp. 1-25.

[19] The FBI Federal Bureau Of Investigation, 2009 https://archives.fbi.gov/archives /news/ stories/2009/april/spearphishing_040109 Retrieved 21February 2017

[20]http://www.pcmag.com/encyclopedia/term/54261/ weak-password Retrieved 21February 2017

[21]https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

[22] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM, pp. 534-542, 2010.

[23] H. Xiong, X. Zhang, D. Yao, X. Wu, and Y. Wen, “Towards end to-end secure content storage and delivery with public cloud,” in CODASPY, 2012, pp. 257–266.

[24] S. Meena, E Daniel and Dr. NA. Vasanthi, Surveyon Various Data Integrity Attacks in Cloud Environment and the Solutions, International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013], pp 1076-1081

[25] X. D. Zhu, H. Li, F. H. Li. Privacy-preserving logistic regression outsourcing in cloud computing. International Journal of Grid and Utility Computing, vol. 4(2-3), 2013, pp. 144-150.

[26] M. D. Ryan. Cloud computing security: The scientific challenge, and a survey of solutions. The Journal of Systems and Software, vol. 86(9), 2013, pp. 2263-2268.

[27]http://www.cbsnews.com/news/irs-identity -theft-online-hackers-social-security- number -get-transcript