International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-10 Issue-1, November 2020

Identification of Various Security Issues, Threats and A Novel Service Model in Cloud Computing

Nasreen Sultana Qadri, Kusum Yadav, Yogesh Kumar Sharma

Abstract*—Cloud Computing is a robust, less cost, and an effective platform for providing services. Nowadays, it is applied in various services such as consumer business or Information Technology (IT) carried over the Internet. This cloud computing has some risks of security because, the services which are required for its effective compilation is outsources often by the third party providers. This makes the cloud computing more hard to maintain and monitor the security and privacy of data and also its support. This sudden change in the process of storing data towards the cloud computing technology improved the concerns about different issues in security and also the various threats present in this cloud storage. In the concept of security in cloud storage, various threats and challenges are noted by recent researchers. Hence, an effective framework of providing security is required. The main aim of this paper is to analyze various issues in securing the cloud data threats present in the cloud storage and to propose a novel methodology to secure it. This paper also identifies the most crucial components that can be incorporated in the already existing security measures while designing the storage systems based on cloud. This study also provides us to identify all the available solutions for the challenges of security and privacy in cloud storage.

***Keywords:*, Security, Deployment, Adoption, Data, Threat, Cloud Computing**

I. INTRODUCTION

In the history of Computer science, various actions have been carried to encourage the users to use the hardware of computer for reducing thetime and other utilities etc. These applicationsleads to the growth of various academic and business leaders in this cloud computing. Cloud based Computing is an advanced methodology derived from the application of Information Technology (IT), which leads to understand the process of Operating system present in a computer, its overall architecture etc. These cloud based computing is used to solve the requirements in client side. This cloud based computing technology become more reliable among the users, various concerns are being noticed about the security issues when this this new model is being adopted.

Revised Manuscript Received on November 30, 2020.
***** Correspondence Author
Nasreen Sultana Quadri* is currently a research Shholar in the Department of Computer Science in JJTU University, India, E-mail: nsultanaquadri@gmail.com
Dr Kusum yadav is currently working as an Associate Professor in the Department of Computer Science in Hail University, Hail, Saudi Arabia, E-mail: kusumyadav@gmail.com
Dr Yogesh kumar Sharma is currently working as an Associate Professor in the Department of Computer Science in JJTU University, India.

Various works have been done to improve the architecture of the traditional computing technique. Hence, the cloud computing based architecture model widely differs from the existing architectures. In this paper, various challenges and classifications of various threats that cause the security issues are outlined along with a novel security mechanism. The aim of this paper is to analyze various issues in securing the cloud data threats present in the cloud storage and to propose a novel methodology to secure it. This paper also identifies the most crucial components that can be incorporated in the already existing security measures while designing the storage systems based on cloud. A novel solution for providing security in cloud storage is proposed, which is based on the combination of two already available Platform as a Service **(PaaS)** security models and the Infrastructure as a Service **(IaaS)** which leverages all the clients from the security burden, by trusting the proposed security model. The proposed security modelaims at a particular security level by combining two existing models of security. The proposed model is a combination of services. The proposed methodology is a framework based and it is expected to achieve the main goal of this work as to analyze the various threats and security issues which are present se the cloudSecurity models. The basic models are as follows:

A Infrastructure as a Service (IaaS)

This is a service which lets the user to perform the process of storage, networking tasks, and various other basic tasks which can be done in the cloud architecture. It also allows the user to applyarbitrarybased software, which can include operating systems and various applications.

B Platform as a Service (PaaS)

This is a service which lets the user who uses the system to apply the proposed model or architecture in the infrastructure of cloud based systems. Applications which were created by different programming languages by the user can also be applied in the cloud using this service. It also supports other developing tools proposed by the user. The user no need to manage all the cloud services such as the architecture, networking, hardware's connected to it, operating systems and other storage devices. It had to look over the applied services or the outsourced services only.

C Software as a Service (SaaS)

This is a service which gives the capacity to a user to utilize the various applications which are executed in the system by a service provider. These applications can be installed within the clouds architecture.

These applications can be made available within the devices which the clients are using. It can be achieved using a web based browser such as an e-mail. Hence, it can be easily managed by the user from a remote side.

By this service, the user is not responsible for any types of hardware's connected to the cloud such as the networking components, operating systems installed in the cloud etc. Based on these services, four deploying models are proposed earlier. It is as follows:

D Private Cloud

This cloud architecture is exclusively designed for some organizations working as privately. The entire cloud and all its resources are managed by the particular organization or by a third party.

E Community cloud

The community cloud has a shared type architecture which is designed for a particular community or a group of people. This type of cloud will consider various security requirements such as the definition of policy, compatibility issues etc. Third party service providers can manage these types of clouds

F Public cloud

This type of cloud architecture is designed in a way such that it will be available for public. It can also be used by a group of public or a public based organization.

G Hybrid cloud

This hybrid cloud is the combination of two or more cloud architectures such as the private or public or the community. The main advantages of these types of clouds are they have a particular services common [2] and it can be monitored and maintained by the subscriber as well as the service provider [6, 7]. In general, the cloud services have various resources which are provided by the subscriber and the service provider. In IaaS, the resources such as Application, Data, Runtime, Middleware were handled by the subscriber. Meanwhile, the hardware services such as the Virtualization, Servers, Storage and the Networking were handled by the service provider.

II. FACTORS FOR CLOUD ADOPTION

Adoption is the process of applying a methodology in the existing technology. Providing security in the cloud computing is a preliminary process of a cloud provider. The cloud provider should be cautious about the security of data store in the cloud before providing it. In this section, various factors that are most important for adopting the cloud architecture are depicted. Various researches [7-9, 25] have done in adopting the cloud technology. The external factors such as regulations of government, standards of IT industries and other institutions, cloud providers, partners of the business, competitors etc. Internal factors such as the willingness of invertors to invest in the cloud architecture, employer's prior experiences, Size of the firm, employees from the IT side etc. should also to be considered.

Authors in [7]proposed a trusted model for third party. Their architecture is framed in order to provide security, integrity and the confidentiality to the cloud user. Two factors such as the external factors and the internal factors should be considered before adopting new cloud architecture. Authors in [9] depicts how to secure files and various documents in a cloud environment which is maintained by a trusted third party. Various researchers in [10, 11, 12, 13, 14] have proposed different models for security models to secure the cloud architecture. But none of them mentioned the combination of two existing services to secure the present cloud data more efficiently.

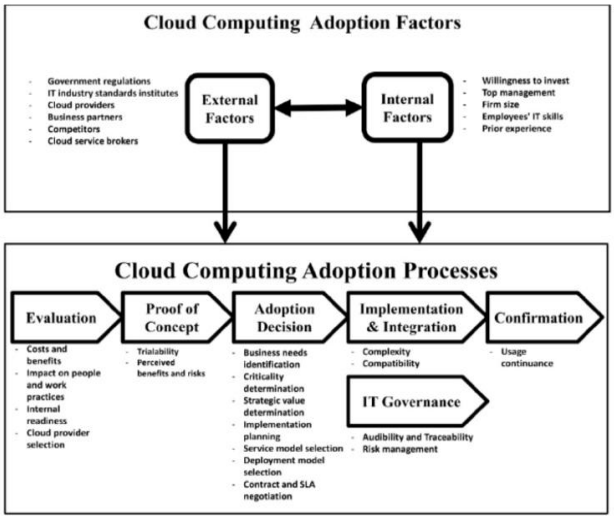

Fig 1. Various Adoption Factors for Cloud Computing

A. Methodology of cloud Adoption

Basic process behind the cloud adoption has various steps and techniques. Main stages for adopting new cloud architecture is as follows:

- **Analyze the existing issues by reviewing the already available methodologies and architectures:** This process analyzes the various issues present in the existing methods, methodologies present in the cloud adoption process.
- **Identify the problem:** A detailed research and its application should be performed in order to identify the real issues present in the adoption of cloud computing. In order to do this, smallscale organizations which implemented the cloud environment should be identified and analyzed so that all the necessary information can be gathered. Interviews can also be performed to identify the problem.
- **Analysis of collected data:**A well-used approach called as the content analysis can be used to analyze the collected data through interviews. Various charts and graphs can also be created to classify the problems identified.
- **Generating Guidelines:**Guidelines can be prepared based on the problems and solutions can be proposed for its effective implementation in small scale organizations.
- **Verification and Validation:** This process comprises of verifying the facts proposed and the implemented results. The proposed framework which is going to be adopted should also be validated. Various workshops should be conducted for this validation process.
- **Implementation:** After checking the accuracy of the proposed framework, it can be adopted effectively in small scale organizations.

III. SECURITY IN CLOUD COMPUTING

Security id defined as the ability of creating a situation where all the threats which are possible can be removed or kept in control [20]. Security in cloud computing data is an important issue in the cloud technology and its architecture since the cloud computing can be deployed using the help of various resources such as the networks, operating systems, agent based systems etc. Providing the trust for users in cloud is also an important issue in the cloud based computing. Trust for the cloud users can be improved by providing various security measures and various processes to convince them. Cloud architecture is considered as providing the trust environment to the user when he believes that his data stored and handled by the cloud service or the provider with a maximum security level. For this, initially, a cloud developer should analyze the various requirements. Every attack is assumed and all the requirements which are required are tested with the assumed attacks. Various vulnerabilities and threats to the security of data stored in a cloud environment are classified in table 1. Various categories of requirements such as the management based, credential based, network based, user based and provider based are there for providing the security in cloud systems. These categories can be applied for protecting the system from unauthorized logging in, management of various policies for the usability of the system, administrating the overall system, detection of various intruders etc. Data requirement such as storing the data securely, removal of redundancy, increasing the authorization should be also monitored. User requirements such as maintaining the flexibility in authentication process among the known users, usability of the resources and maintaining trust in the platform used.

A Security Requirements in Cloud Storage

Requirements to design a secure system are to identify the requirements of security. It is the foremost process. This is used to identify whether which requirement has to be prioritized for the development. For example, authentication is one of the requirements for the cloud storage development. This Process will also identify the necessary terms for developing those requirements. Performance is one of the terms that are necessary for developing the requirements. A new methodology called Asset Table [1] is used by various researchers for identifying the various assets which are required for the development process. The assets such as the networking components, protocols, devices, services, information regarding the users etc. were analyzed. A table is generated based on the above mentioned assets.

TABLE 1. SECURITY REQUIREMENTS IN CLOUD STORAGE SYSTEMS

Category	Applied for Particular Requirements
Category	Interoperability in the Protocol used, Scalability in the protocol, Performance of the software and hardware, Availability in the resources to users.
Management	Accountability (logging protection), Policy Management (usability), Simple Administration (constraints), Auditing (intrusion detection systems)
Data	Storing the data securely, Removal of redundancy, increasing the authorization
Credential	Creating and maintaining the user credentials
Network	Network Confidentiality, Integrity of different protocols, User authentication, and resource availability
User	Flexibility in authentication, Resource usability, Platform Trust
External	External Security for the software and the hardware used.

IV. CLASSIFICATIONS OF RISKS AND MAJOR SECURITY THREATS IN CLOUD STORAGE

Various requirements for the cloud storage system depicted in the section III paves the way for a cloud designer to know about various issues which can affect the security of cloud based data storage. In order to find the necessary requirements for cloud storage, the process of risk management derives the reasons for various security attacks [3]. Initially, a cloud developer should analyze the various requirements. Every attack is assumed and all the requirements which are required are tested with the assumed attacks. Values are generated and based on the analysis results are combined to form a list of most important security attacks. Various analyses had been done by recent researchers [4] and the findings from the analysis are as follows.

1) Logging in the System: Thisaction helps the administrators of the system to understand the various states such as its current and past of the system.
2) Authorization and Authentication of the User: This process helps the cloud provider to authenticate and authorize the user so that the data present in the cloud can be secure. It also ensures that only authorized user can access the data.
3) Authorization and Authentication of the Device: This process helps the cloud provider to authenticate and authorize the device so that all the communication devices belong to a particular infrastructure. It also ensures that only authorized device can access the data.
4) Protection of Data: This mechanism should protect the entire data where ever it is stored in the cloud.
5) Storage of user Credentials. All the credentials of user are stored and managed securely.
6) Service Extension: An open interface mechanism should be provided by the cloud storage system forextended mechanisms and it should also supportother integrated storage.
7) Administration of Policies: All the policies which are used in the entire system should be manages and administered. Managerial tasks such as the administration of user, service provider, etc. can also be managed.

TABLE 2: CLASSIFICATIONS OF VARIOUS THREATS IN CLOUD COMPUTING

Threat ID	Threat Name	Description of the Threat
T01	Hijacking the Account or Services	Hijacking or stealing an account can be done by various methods. Many social engineering based methods can be utilized for this purpose. If the attacker gets all the credentials of a user, the he can easily access the data, modify it and he can also change the sender address of the data [21].
T02	Scavenging of data	All the data cannot be completely erased or removed from the device by either destroying it. In this case, it is easy for the attackers to steal or recover the data [22,23,24].
T03	Leakage of Data	Leakage of data can be done when it is got in to a hacker. There is a possibility of transfer of this data to another service provider and it can also be processed [21,23,].
T04	Service Denial	Service denial can be done when a hacker or an attacker had hacked all the data which were present in the cloud. This can be possible when an attacker or a hacker hacked all the resources from the cloud. Since the data is not available, the system cannot satisfy the user's further request.
T05	Manipulating the data of Customer	Web based applications are hacked or attacked by users by the process of manipulating or changing it. It can be altered based on the server application. Example, injection techniques such as the SQL, command, and the cross site, cross references etc.
T06	Escaping the Virtual Machine	Escaping the virtual machine leads to exploit the overall machine for taking the entire control of that particular machine [31,5].
T07	Hoping the Virtual Machine	When a virtual machine is able to get the access of other virtual machine, the process of hoping is performed [23,8]
T08	Malicious creation of Virtual Machine	Malicious code can be used to create another virtual machine (VM) when a user tries to create a valid account in a virtual machine with virtual image and virtual account. Trojans and viruses can perform these operations
T09	Insecure migration of Virtual machine	Continuous migration of the VM Can bring all the contents and files present in it. By doing the continuous migration, an attacker can access the data in an illegal manner. He can transfer one VM to another through untrusted operations. General virtual machines can be migrated to various virtual machines by creating a disturbance in the overall cloud environment.

All the above mentioned security threats and vulnerabilities are a part of the paper. The proposal of a novel hybrid framework by combining the Iaas and the Paas service models in order to obtain the security in cloud storage comprises the second part.

V. PROPOSED FRAMEWORK:

In this section, a novel methodology of depicting a hybrid framework by combining the Iaas and the Paas service models in order to obtain the highest security in cloud storage is proposed. In general, the IaaS and PaaS service has various resources such as the Application, Data, Runtime, Middleware, Operating System, Virtualization, Servers, Storage and Networking. These services comprises of the cloud architecture. It is shown in figure 2.

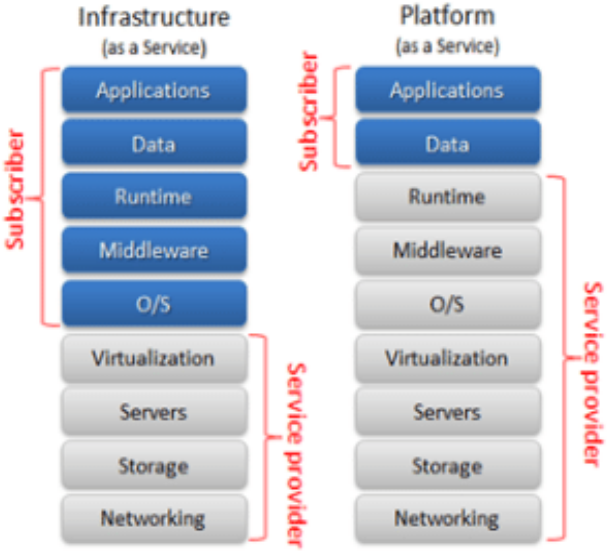

Fig 2. Services of cloud computing

In general, the cloud services have various resources which are provided by the subscriber and the service provider. In IaaS, the resources such as Application, Data, Runtime, Middleware were handled by the subscriber. Meanwhile, the hardware services such as the Virtualization, Servers, Storage and the Networking were handled by the service provider. In the Application and Data services were handled by the service provider.

In the proposed methodology, a novel framework combining IaaS and PaaS service as IPaaS called the Infrastructure and the Platform as a Service. In this framework, Application, Data and the Runtime tasks are carried out by the subscriber and the remaining services are executed by the service provider. The proposed security framework is shown in figure 3. Since the Middleware is managed by the service provider, it will be more efficient in providing the security in cloud storage.

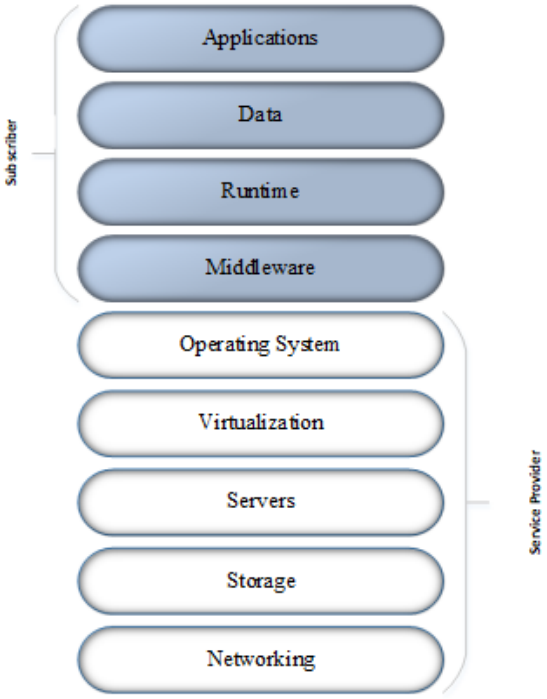

Fig 3. Proposed Service model

VI. CONCLUSION AND FUTURE ENHANCEMENTS

Cloud Computing is a new concept for storing huge data. Many advantages are there for the users because of this cloud computing. However, the security threats and various issues present in this cloud storage make it un-trustable to some users.Understanding the types of issues and vulnerabilities present in this Cloud storage will help organizations and various users in order to divert their focus towards the cloud computing have been used in this storage based on the cloud computing, the security issues will also be inherited towards these technologies. This paper focused on various security issues for the existing cloud based models depends on the types of model. As explained in this paper, the middleware and the security system should be focused. a novel methodology of depicting a hybrid framework by combining the Iaas and the Paas service models in order to obtain the highest security in cloud storage is proposed. Future works could be the implementation and testing of the proposed model to overcome the security threats in the cloud storage.

REFERENCES

1. Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed:15-Jul-2011
2. Cloud Security Alliance, Security guidance for critical areas of focus in Cloud Computing, V3.0, 2011.
3. Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, pp 93–97
4. Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0, Available: https://cloudsecurityalliance.org/ guidance/csaguide.v3.0.pdf
5. Wang C, Wang Q, Ren K, Lou W (2009) Ensuring data Storage Security in Cloud Computing. In: The 17th International workshop on quality of service. IEEE Computer Society, pp 1–9
6. GiljeJaatun M, Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, Proceedings, December 1-4, 2009.Springer
7. Anne Thomas M, Cloud Computing: the Gap between Hype and Reality, presentation by VP and Research Director Burton Group ECAR Symposium December 5, 2008.
8. Jasti A, Shah P, Nagaraj R, Pendse R (2010) Security in multi-tenancy cloud. In: IEEE International Carnahan Conference on Security Technology (ICCST), KS, USA. IEEE Computer Society, pp 35–41
9. Reuben JS (2007) A survey on virtual machine Security. Seminar on Network Security. Technical report, Helsinki University of Technology, October 2007
10. Hendre A, Joshi KP, A Semantic Approach to Cloud Security and Compliance, 2015 IEEE 8th International Conference on Cloud Computing", New York City, June 27- July 2, 2015.
11. Al-Ayyoub, Mahmoud, Jararweh Y, Benkhelifa E, Vouk M, Rindos A, SDSecurity: a software defined security experimental framework, In Communication Workshop (ICCW), 2015 IEEE International Conference on, pp. 1871-1876. IEEE, 2015.
12. Damenu TK, Balakrishna C, Cloud Security Risk Management: A Critical Review , 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, 9-11 September.
13. Singh LV, Bole AV, Yadav SK, Security Issues of Cloud Computing-A Survey, International Journal of Advance Research in Computer Science and Management Studies, Volume 3, Issue 1, January 2015.
14. Varsha Wadhwa A, Gupta S, Study of Security Issues in Cloud Computing, International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 6, June 2015, pg.230 – 234.
15. Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. Available: https://cloudsecurityalliance.org/research/top-threats
16. Mather T, Kumaraswamy S, Latif S (2009) Cloud Security and Privacy. O'Reilly Media, Inc., Sebastopol, CA
17. ENISA (2009) Cloud Computing: benefits, risks and recommendations for information Security. Available: http://www.enisa.europa.eu/activities/riskmanagement/ files/deliverables/cloud-computing-risk-assessment
18. Jansen WA (2011) Cloud Hooks: Security and Privacy Issues in Cloud Computing. In: Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, Kauai, HI. IEEE Computer Society, Washington, DC, USA, pp 1–10
19. Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. Available: https://cloudsecurityalliance.org/research/top-threats
20. ENISA (2009) Cloud Computing: benefits, risks and recommendations for information Security. Available: http://www.enisa.europa.eu/activities/riskmanagement/ files/deliverables/cloud-computing-risk-assessment
21. Grobauer B, Walloschek T, Stocker E (2011) Understanding Cloud Computing vulnerabilities. IEEE Security Privacy 9(2):50–57
22. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA. ACM New York, NY, USA,pp 199–212
23. Zhang Y, Liu S, Meng X (2009) Towards high level SaaS maturity model: methods and case study. In: Services Computing conference. APSCC, IEEE Asia-Pacific, pp 273–278
24. Morsy MA, Grundy J, Müller I (2010) An analysis of the Cloud Computing Security problem. In: Proceedings of APSEC 2010 Cloud Workshop. APSEC, Sydney, Australia
25. El-Gazzar R.F. (2014) A Literature Review on Cloud Computing Adoption Issues in Enterprises. In: Bergvall-Kåreborn B., Nielsen P.A. (eds) Creating Value for All Through IT. TDIT 2014. IFIP Advances in Information and Communication Technology, vol 429. Springer.