Security Threats in Cloud Computing

Engr: Farhan Bashir Shaikh
Department of Computing & Technlogy
SZABIST
Islamabad, Pakistan
Shaikh.farhan@live.com

Sajjad Haider
IT Department
NUML
Islamabad, Pakistan
Sajjadhyder@hotmail.com

Abstract— **Abstract— Cloud computing is set of resources and services offered through the Internet. Cloud services are delivered from data centers located throughout the world. Cloud computing facilitates its consumers by providing virtual resources via internet. General example of cloud services is Google apps, provided by Google and Microsoft SharePoint. The rapid growth in field of "cloud computing" also increases severe security concerns. Security has remained a constant issue for Open Systems and internet, when we are talking about security cloud really suffers. Lack of security is the only hurdle in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. The wide acceptance www has raised security risks along with the uncountable benefits, so is the case with cloud computing. The boom in cloud computing has brought lots of security challenges for the consumers and service providers. How the end users of cloud computing know that their information is not having any availability and security issues? Every one poses, Is their information secure? This study aims to identify the most vulnerable security threats in cloud computing, which will enable both end users and vendors to know about the key security threats associated with cloud computing. Our work will enable researchers and security professionals to know about users and vendors concerns and critical analysis about the different security models and tools proposed.**

Keyword: Cloud Computing; Cloud Computing Security; Security Survey of Cloud Computing; Security threats; Secure Cloud computing

I. INTRODUCTION

"Cloud computing" simply means "Internet computing ", generally the internet is seen as collection of clouds; thus the word cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. Cloud computing enables consumers to access resources online through the internet, from anywhere at any time without worrying about technical/physical management and maintenance issues of the original resources. Besides, Resources of cloud computing are dynamic and scalable. Cloud computing is independent computing it is totally different from grid and utility computing. Google Apps is the paramount example of Cloud computing, it enables to access services via the browser and deployed on millions of machines over the Internet. Resources are accessible from the cloud atany time and from any place across the globe using the internet. Cloud computing is cheaper than other computing models; zero maintenance cost is involved since the service provider is responsible for the availability of services and clients are free from maintenance and management problems of the resource machines. Due to this feature, cloud computing is also known as utility computing, or 'IT on demand'. Scalability is key attribute of cloud computing and is achieved through server virtualization. This fresh, web-based generation of computing uses remote servers placed in extremely safe and secure data centers for storage of data and management, so organizations do not need to pay for and look after their internal IT solutions. After creation of a cloud, Deployment of cloud computing differs with reference to the requirements and for the purpose it will be used. The principal service models being deployed are:

Software as a Service (SaaS): Software's are provided as a service to the consumers according to their requirement, enables consumers to use the services that are hosted on the cloud server.

Platform as a Service (PaaS): Clients are provided platforms access, which enables them to put their own customized software's and other applications on the clouds.

Infrastructure as a Service (IaaS): Rent processing, storage, network capacity, and other basic computing resources are granted, enables consumers to manage the operating systems, applications, storage, and network connectivity.

II. LITERATURE REVIEW

Rongxing et al [1] in this paper gave a new security and provenance proposal for dataforensics and post examination in cloud computing. According to them their proposed system is typified, the proposed system can provide the privacy and security on secret documents/files that are piled up in the cloud. It also provides secure authentication mechanism to control unauthorized user access, and provides track mechanism to resolves disputes of data. Their proposed secure provenance scheme is working on the bilinear pairing method and they have claimed it as the necessary building blocks of data forensics and post examination in cloud computing environment. Using provable security techniques, they have formally verified that there proposed scheme is safe and sound in the standard model. There proposed secure

provenance system for cloud computing includes five parts: [1] "Setup, KGen, AnonyAuth, AuthAccess, and ProveTrack". Due to theample security features, the scheme proposed produces reliable facts for data forensics in cloud computing. They claim that their proposed system can be a cause to move forward for the wide recognition of cloud computing.
The strength of their work is the proposed secure provenance system and limitation of their work is that their proposed scheme is difficult to implement as it is based on complex mathematical model which is very difficult to understand.

La'Quata Sumter et al. [2] says: The rise in the scope of "cloud computing" has brought fear about the "Internet Security" and the threat of security in "cloud computing" is continuously increasing. Consumers of the cloud computing services have serious concerns about the availability of their data when required. Users have server concern about the security and access mechanism in cloud computing environment. To assure users that there information is secure, safe not accessible to unauthorized people, they have proposed the design of a system that will capture the movement and processing of the information kept on the cloud. They have identified there is need of security capture device on the cloud, which will definitely ensure users that their information is secure and safe from security threats and attacks. The proposed implementation is based on a case study and is implemented in a small cloud computing environment. They have claimed that there proposed security model for cloud computing is a practical model cloud computing.
The advantage of their work is assurance of security to the end users of cloud. The limitation of this study is there proposed framework is not feasible for large scale cloud computing environments.

Mladen [3] states that "Cloud" computing is a recent field, which came into existence after Years of research in networking and different types of computing. It uses a SOA, that minimized the information technology operating and maintenance cost for the clients, it offers greater flexibility, reduces capital costs, provides required services are along with many other characteristics. This study discusses issues associated with cloud computing along with Virtualization, Cyber infrastructure; Service oriented Architecture and end users. Implementation, research and security issues are studied in detail and key concerns have been identified. The study ranked security as the primary challenge in cloud computing. It is being observed that the users of cloud computing services are not satisfied with the current security mechanism in cloud computing. Service providers must assure the availability and reliability of services to the consumers available anytime, anywhere using internet, plus security, safety, data protection and Privacy is also exercised. The study further emphasizes that further research on security of cloud computing is required.
The benefit of this study is the identification of issues related with security and implementation. The drawback of this work is the study is based on theoretical concepts nothing practical found in this study. This work could have contributed more if practical things were discussed.

Wenchao et al. [4] in this paper have taken alternative perspective and proposed data centric view of cloud security. They have explored the security properties of secure data sharing among the applications hosted on clouds. They have discussed the data management issues in distributed query processing, Forensic and system analysis and query correction assurance. They have proposed a new security platform for cloud computing, which is named as Declarative Secure Distributed Systems (DS2). According to them the DS2 platform includes the functionality essential for their proposed data security methods. In DS2, the network protocol and security policies are specified Via Secure Network Data log (SeNDlog) a Language which is normally rooted in Datalog that merges declarative networking and logic-based access control Specifications. In this paper they have developed DS2 prototype using the Rapid Net declarative networking engine They have added provenance support to the DS2 platform because they believe that the distributed Provenance is significant step towards a secure cloud data management infrastructure.
The strength of their work is the proposed tool for data centric security which provides secure query processing, seamless integration of declarative access control policies, system analysis and forensics, efficient end-to-end verification of data. Limitations are not worth mentioning. There work needs to be validated from cloud computing vendors.

Soren et al [5] in this paper have mentioned that benefits of clouds are shadowed with the security, safety and privacy challenges and due to these challenges the adoption of cloud computing has been inhibited to a great extent. It is stated that highly flexible but very complex cloud computing services are configured using web interface by users but wrong configuring of cloud computing by users may lead to vulnerable security threats and can cause security incidents. In this paper an approach has been presented for analyzing security at client side and server side. Amazon's Elastic Compute Cloud (EC2) has been chosen for this assessment. The primary aim is to focus on the accessibility, vulnerabilities in the entire cloud infrastructure. They have implemented the security analysis model & weigh up it for realistic environments. A specialized query policy language for assessment has been proposed in this paper, which is used to get handy into the arrangement and to state required and not required configurations. They claim that their approach they have used effectively allows remediate current security issues by validating configurations of complex cloud Infrastructures. Security assessment has been implemented in Python and weigh up was calculated on Amazon EC2. Breaches in the weaknesses of securitypolicies are Identified and probable

attack trails are informed to the administrators of the system in order to ensure concerned services are checked and action is taken to make them secure.
The advantage of this work is their proposed tool which provides.Strong analysis of security attacks and vulnerabilities, this analysis helps vendors to improve their security policies the drawback is that their proposed framework is specific to Amazon. This work would have contributed more if it would have been general instead of specific to Amazon.

Flavi and Roberto [6] stated that clouds are being targeted increasingly day by day. In this paper integrity protection problem in the clouds, sketches a novel Architecture and Transparent Cloud Protection System (TCPS) for improved security of cloud services has been discussed. They claim that they have identified the integrity safety problem in clouds .To address the integrity issues, they have proposed a system, and the system is named as Transparent Cloud Protection System (TCPS) for increased security of cloud resources. According to them their proposed system, TCPS can be used to observe the guests integration and keeping the transparency and virtualization.
The strength of their work is their proposed tool which provides improved security, transparency and intrusion detection mechanism. The limitation of their work is that they haven't validated their work nor they have deployed in professional cloud computing scenario.

Wayne [7]: In this paper benefits of cloud computing are highlighted along with the basic security issues that are still associated with cloud services. Shaping the security of critical systems is very important. Addressing the security issues faced by end users is extremely mandatory, Researchers and professionals must work on the security issues associated with cloud computing. Strong security policies must be designed to ensure data is safe and prevented from unauthorized access, in both corporate data centers and in the cloud servers. This research brings primary problems in terms of cloud security, which are alleged to cloud computing security and privacy issues. Further the study gazes primary security and privacy Problems. It mainly focuses public clouds that needs significant consideration and presents required facts and figures to make organizations data security decisions. Key security issues identified and addressed in this paper are end user trust, Insider Access, Visibility, Risk Management, Client-Side Protection, Server-Side Protection, Access Control and Identity management.
The strengths of their work is identification and discussion on cloud computing security issues which educates end users about security and private risks associated with cloud services. The weakness is that they haven't proposed any tool or framework to address identifies issues.

As per Jinpeng et al [8] said that: Cloud computing poses many new security threats. In this paper they have evaluated these threats in depth from an image repository side. They have also analyzed the risks faced by the system administrators and end users of a cloud's image repository. An image management system design has been presented to address the associated risks. They claimed that their proposed design addresses those risks and according to them the proposed design is implementable and proficient. The filters of the system in first step finds malicious stuff and in next step sensitive information like passwords etc are removed. Provenance tracking and access control enable publishers to decide which images are available to which users. Users are able to find their required images. The repository maintenance services decrease the risk of executing vulnerable or illegal software. The preliminary results in this paper showed that the filters are working correctly at the repository, similarities among images are explored. They are expecting that such type of other services can also be implemented efficiently in their image management system.
The strength of their work is the proposed image management system which provides image filters and scanners to detect malicious images. The weakness is that image filters are not accurate and sometimes legitimate images may also be detected as malicious image and their virus scanner is also not efficient. The scanner is not capable to detect all types of viruses, virus scanner validation is not provided by the authors.

Miranda and Siani [9]: In this paper states that most important obstacle to wide acceptance of "cloud computing" services security and privacy issues in cloud computing, users have serious concerns about confidential data seepage. Privacy is not observed while critical data is being processed in the public accessible cloud. Some practical scenarios has been discussed in this paper, based on these scenarios it is recommended strongly that use of sensitive information must be minimized when data is processed on clouds and privacy to end users must be assured. To address this issue, a client-based privacy manager tool has been proposed in this paper. The proposed reduces security issues, and provides added privacy features. The tool has been tested accordingly in different cloud computing environments. The entire structure of their developed privacy manager tool is shown in Figure 1[9].

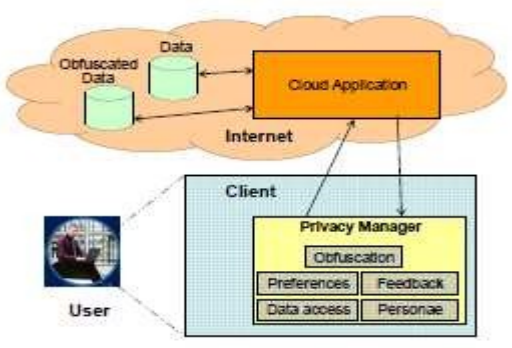

Figure: 1 [9] overview of their proposed solution

The theme of proposed Privacy Manager Tool is to ensure on privacy when cloud computing services are accessed on client machine. The premium aspect of Privacy Manager Software is providing obfuscation & de-obfuscation Service. This feature helps reducing critical user information placed on the cloud and fields of data are obfuscated prior to sending data on the cloud server for further action. Once data is obfuscated the output is de-obfuscated in the cloud. This process of obfuscation and de-obfuscation uses a key selected by the user of cloud services and selected key is not publicized. Even service providers are not aware of the key used. Further, the Privacy Manager also facilitates End users to customize privacy of their personal information, using multiple qualities, it also enables end users to reassess and then rectify their private information that is stored inside cloud. The features of privacy manager software like Obfuscation, Preference setting, Data access, Feedback and Personae are discussed in detail. They claim that privacy of users can be assured by simply minimizing the quantity of confidential data sent off to the cloud.
The strength of their work is that their proposed privacy manager tools is providing data minimization, access control, Purpose limitation, user-centric design and feedback facility to the consumer of cloud services. The drawback of their work is that it is not generalized and it cannot be implemented in all scenarios.
In this paper security concerns that occur in cloud computing services from user point of view are discussed briefly.

Rituik et al [10] have focused on the metering issue or verification of job, the users of cloud services can verify the cost charged by the service providers with respect to services they availed. Different types of security attacks are discussed and solutions are proposed for each type of attack. Numerous serious security problems faced by users of cloud services are reviewed in depth specially the metering issue and backup of user data. These issues are addressed in attacker model and solutions for each problem are also proposed. A simulation program is developed for eBay model. The results of simulation showed that proposed solutions attain sensible detection rate with inexpensive operating cost. The simulation software developed was deployed on a normal Intel core 2duo machine having 1GB ram. The simulation program is coded JAVA, the program is able to simulate 1000 online shops, using different parameters deeds of the cloud computing server and online merchants are simulated. During the process of simulation It was observed that the cloud computing server misses few inventory parts.
The strength of their work is the framework proposed to address metering issue. Their proposed tool enables users to verify billing details by service provider and prevention of security attacks. The weakness is that it is only applicable to sales applications.

According to Dan and Anna [11] Cloud computing provides highly scalable resources accessed via Internet. since cloud computing is growing quickly day by day used by individuals and companies throughout the world, data protection problems in the cloud computing have not been tackled currently. In the cloud, users of cloud services have serious threat of losing confidential data. To address data privacy issues of users, they have proposed data protection framework. According to them the proposed data protection framework addresses the challenges throughout the cloud services life cycle. Their proposed framework comprises of three key components: policy ranking, policy integration and policy enforcement. For each component, they have presented various models and analyzed properties of each component. This paper includes a discussion on general guidelines for weighing up designed systems based on such kind of framework. They have also presented several data protection models and defined cost functions. The proposed model is shown in figure 3[11]

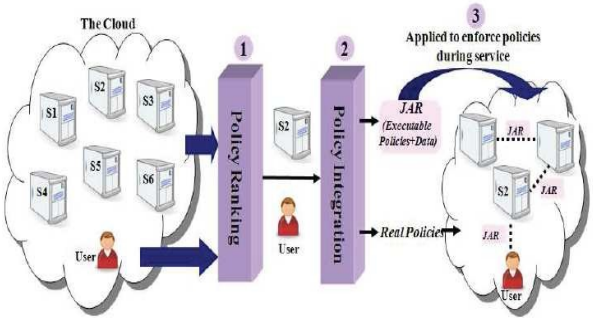

Figure: 2 [11] Overview of their proposed framework

The advantage of this work is that their proposed tool provides Correctness,Time-Efficiency, Scalability, Security, Robustness and Reliability. The weakness is that their proposed model is not validated.

III. CRITICAL EVALUATION

Before you begin to format your paper, first write and save We have studied research papers related with security and privacy threats in cloud computing. In some papers tools and models are proposed to address security and privacy in cloud computing while in others some more security and privacy issues are identified. After review we have summarized in the following compare and contrast table (table 1)

Lit. Ref	Context of Research	Problem Discussed	Technique Used	Model/ Tool/ Proposed
1	Secure Provenance in Cloud Computing	Data forensics and post investigation in cloud computing	Bilinear pairing method	Yes

Lit. Ref	Context of Research	Problem Discussed	Technique Used	Model/ Tool/ Proposed
2	Trusted Cloud Computing	Security Risk and Security assurance to cloud users	Trusted Cloud Computing Platform (TCCP)	Yes
3	Implementation and research issues in cloud computing	SSH tunnels and VLANs, verifiable integrity and end-to-end service isolation through VPN	Virtual Computing Laboratory (VCL) Technology, open source	No
4	Data-centric cloud security	Secure Query Processing and Data Sharing. System Analysis and Forensics, Query Correctness Assurance.	DS 2 Platform	Yes
5	Security audit in public infrastructure Clouds	Reachability Audit of Amazon Security Groups & Security Graphs.	Amazon's Elastic Compute Cloud (EC2)	Yes
6	Transparent Cloud Security	Cloud Security vulnerabilities and Security Attacks	The Transparent Cloud Protection System (TCPS)	Yes
7	Security & Privacy in Cloud Computing	End user trust, Insider Access, Visibility, Risk Management, Client-Side Protection, Server-Side Protection, Access Control and Identity management	Theoretical Research	No
8	Security Management of Virtual Machines	Managing virtual machine Images securely, Security Risks in image repository.	Image Management System that uses access control frame work, filters and scanners.	yes
9	Privacy Manager for Cloud Computing	Security, Privacy and user concerns.	Privacy Manger tool developed to address security issues at user level.	Yes
10	Addressing security issues in cloud computing.	Metering problem, Proof of work, Attack scenarios & data Backups	A simulation program that is coded JAVA, the program is able to simulate 1000 online shops, using different parameters deeds of the cloud computing server and online merchants are simulated. During the process of simulation It was observed that the cloud computing server misses few inventory parts.	yes
11	Data Protection Models for Service Provisioning in the cloud	Users Concerns regarding privacy and security of Data	Data Protection Framework	Yes

IV. FUTURE WORK

Cloud computing is not fully mature and still lot needs to be explored. After our current work we are claiming that security is the most important threat to both the users and the vendors of cloud computing. Vendors, Researchers and IT security professionals are working on security issues associated with cloud computing. Different models and tools have been proposed but still nothing fruitful found. While doing research on security issues of cloud computing we came to know that there are no security standards available for secure cloud computing. In our future work we will work on security standards for secure cloud computing.

V. CONCLUSION

In this study different security and privacy related research papers were studied briefly. Cloud services are used by both larger and smaller scale organizations. Advantages of Cloud computing are huge. But it's a global phenomenon that everything in this world has advantages as well as disadvantages. Cloud computing is suffering from severe security threats from user point of view, one can say that lack of security is the only worth mentioning disadvantage of cloud computing. Both the Service providers and the clients must work together to ensure safety and security of cloud and data on clouds. Mutual understanding between service providers and users is extremely necessary for providing better cloud security. In this paper we have identified that security is biggest hurdle in wide acceptance of cloud computing. Users of cloud services are in fear of data loss and privacy. Researchers and IT security professionals must come forward and do more to ensure security and privacy to users. Our study identifies top security concerns of cloud computing, these concerns are Data loss, Leakage of Data, Client's trust, User's Authentication, Malicious users handling, Wrong usage of Cloud computing and its services, Hijacking of sessions while accessing data. We propose to use[12] The Cloud Security Alliance (CSA) release of a new governance, risk management, and compliance stack for cloud computing. The suite of cloud security tools, available for free download, is meant to help organizations create public and private clouds that comply with industry standards for accepted governance, risk, and compliance (GRC) best practices. The GRC stack has three components: a technical foundation, a controls framework, and a questionnaire for assessing what the CSA calls "industry-accepted ways to document what security controls exist" for infrastructure-, platform-, and software-as-a-service offerings.

REFERENCES

[1] Rongxing et al, "Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing", ASIACCS'10, Beijing, China..

[2] R. La'Quata Sumter, "Cloud Computing: Security Risk Classification", ACMSE 2010, Oxford, USA

[3] Mladen A. Vouch, "Cloud Computing Issues, Research and Implementations", Journal of Computing and Information Technology - CIT 16, 2008, 4, 235–246

[4] Wenchaoet al, "Towards a Data-centric View of Cloud Security", CloudDB 2010, Toronto, Canada

[5] Soren Bleikertz et al, "Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds", CCSW 2010, Chicago, USA.

[6] Flavio Lombardi& Roberto Di Pietro, "Transparent Security for Cloud", SAC'10 March 22-26, 2010, Sierre, Switzerland.

[7] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", 44th Hawaii International Conference on System Sciesnces 2011.

[8] Jinpeng et al, "Managing Security of Virtual Machine Images in a Cloud Environment", CCSW, 2009, Chicago, USA

[9] Miranda & Siani, "A Client-Based Privacy Manager for Cloud Computing", COMSWARE'09, 2009, Dublin, Ireland

[10] Dan Lin & Anna Squicciarini, "Data Protection Models for Service Provisioning in the Cloud", SACMAT'10, 2010, Pittsburgh, Pennsylvania, USA

[11] en.wikipedia.org/wiki/Locality_of_reference.

[12] informationweek.com/news/storage/security/228300050