Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Security and Privacy Issues in Cloud Computing

M.Angel Jasmine Shirley,
M.C.A., M.Phil., M.Ed., Ph.D Research Scholar, JJT University, Rajasthan, India

Abstract-- Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Fast and reliable connectivity is a must for the existence of cloud computing. Cloud computing is clearly one of the most enticing technology areas of the current times due to its cost-efficiency and flexibility. However, despite the surge in activity and interest, there are significant, persistent concerns about cloud computing that are impeding the momentum and will eventually compromise the vision of cloud computing as a new IT procurement model. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Cloud computing raises privacy and confidentiality concerns because the service provider necessarily has access to all the data, and could accidentally or deliberately disclose it or use it for unauthorized purposes. The complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In this regard, the war for the future of security and privacy issues in the cloud is just beginning. Tough analysts of cloud security are gaining new credibility. For instance, a new way of auditing specifically designed for the cloud industry is evolving. Overall, it is fair to say that privacy and security issues related to the cloud industry are undergoing political, social, and psychological metamorphosis. This paper discusses the types, layers, data security and privacy issues and some propositions for security in cloud.

Keywords-- *Cloud Computing, security and privacy, virtualization, standardization, encryption.*

I. INTRODUCTION

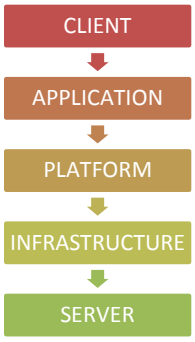
Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software and information are provided to computers and other devices as a utility a network . Cloud computing provides computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Example of cloud computing is Yahoo email or Gmail etc. We don't need software or a server to use them. All a consumer would need is just an internet connection and we can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc. The consumer gets to use the software alone and enjoy the benefits.

Cloud computing exhibits the following key characteristics:

1. Agility improves with users' ability to re-provision technological infrastructure resources.
2. Application programming interface (API) accessibility to software that enables machines to interact with cloud software in the same way the user interface facilitates interaction between humans and computers.
3. Cost is claimed to be reduced and in a public cloud delivery model capital expenditure is converted to operational expenditure.
4. Device and location independence enable users to access systems using a web browser regardless of their location or what device they are using (PC, mobile phone). As infrastructure is off-site and accessed via the Internet, users can connect from anywhere.
5. Multi-tenancy enables sharing of resources and costs across a large pool of users thus allowing for:
   1. Centralization of infrastructure in locations with lower costs
   2. Peak-load capacity increases
   3. Utilization and efficiency improvements for systems that are often only 10–20% utilized.
6. Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for continuity and disaster recovery.
7. Scalability and Elasticity via dynamic provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads.
8. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
9. Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels.
10. Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer.

II. LAYERS OF CLOUD COMPUTING

Once an internet protocol connection is established among several computers, it is possible to share services within any one of the following layers.



1. **Client:** A cloud client consists of computer hardware and/or computer software that relies on cloud computing for application delivery and that is in essence useless without it. Examples are computers, phones and other devices, operating systems, and browsers.
2. **Application:** Cloud application services or "Software as a Service (SaaS)" deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support.
3. **Platform:** Cloud platform services, also known as platform as a service (PaaS), deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud application.
4. **Infrastructure:** Cloud infrastructure services, also known as "infrastructure as a service" (IaaS), deliver computer infrastructure – typically a platform virtualization environment – as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients instead buy those resources as a fully outsourced service. Suppliers typically bill such services on a utility computing basis.
5. **Server:** The server's layer consists of computer hardware and/or computer software products that are specifically designed for the delivery of cloud services, including multi-core processors, cloud-specific operating systems and combined offerings.

III. CLOUD COMPUTING TYPES

A. Private cloud

Private cloud is infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.

B. Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned to the general public on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who bills on a fine-grained utility computing basis.

C. Community cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

D. Hybrid cloud

Hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.

Some Cloud Computing Service Providers are Amazon, Microsoft windows Azure, Savvis, Google AppEngine, VMware cloud, Rack space, Verizon, Go grid, AppNexus

IV. CLOUD COMPUTING SECURITY AND PRIVACY ISSUES

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. The network that interconnects the systems in a cloud has to be secure. Virtualization paradigm in cloud computing leads to several security concerns. Mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable for malware detection in the clouds. Cloud computing raises privacy and confidentiality concerns because the service provider necessarily has access to all the data, and could accidentally or deliberately disclose it or use it for unauthorized purposes. The complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users.

V. TYPES OF ATTACKERS IN CLOUD COMPUTING

A. Internal attackers

An internal attacker has the following characteristics:

- Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service.
- May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role.
- Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service.

B. External attackers

An external attacker has the following characteristics:

- Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service.
- Has no authorized access to cloud services, customer data or supporting infrastructure and applications.
- Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service.

In the cloud environment, attackers can be categorized into four types: random, weak, strong, and substantial

VI. PRIVACY AND SECURITY ISSUES

A. Conference management systems

Conference management systems based on cloud computing represent an example of these problems within the academic research community. A privacy concern with cloud-computing-based conference management systems such as EDAS and Easy Chair arises because the system administrators are custodians of a huge quantity of data about the submission and reviewing behavior of thousands of researchers, aggregated across multiple conferences. This data could be deliberately or accidentally disclosed, Reviewer anonymity could be compromised, as well as the confidentiality of PC discussions, the aggregated reviewing profile (fair/unfair, thorough/scant, harsh/undiscerning, prompt/late) of researchers could be disclosed. The data could be abused by hiring or promotions committees, funding and

award committees, and more generally by researchers choosing collaborators and associates. The mere existence of the data makes the system administrators vulnerable to bribery, coercion, and/or cracking attempts. Cloud computing solutions allow data to be aggregated across thousands of conferences over decades, presenting tremendous opportunities for abuse if the data gets into the wrong hands.

Certain cloud computing applications may be primarily storage applications, and might not require a great deal of processing to be performed on the server side. In that case, encrypting the data before sending it to the cloud may be realistic. It would require keys to be managed and shared among users in a practical and efficient way, and the necessary computations to be done in a browser plug-in

B. The cloud's newness and unique vulnerabilities

The cloud's newness and uniqueness present special problems. With the evolution and popularity of virtualization technology, new bugs, vulnerabilities and security issues are being found. One problem found in network virtualization is that a user may be able to access to the provider's sensitive portions of infrastructure as well as resources of other users. The cloud is also forensically challenging in the case of a data breach.

C. Nature of the architecture

a. Virtual and dynamic

The shared and dynamic resources of the cloud such as CPU and networking reduce control for the user and tend to pose new security issues not faced by on-premise computing. These characteristics of the cloud allow data and information to distribute widely across many jurisdictions. The locations where data are stored may vary in laws regarding security, privacy, data theft, and protection of intellectual property. Virtualization is the primary security mechanism in the cloud. Virtualization environments are not necessarily bug-free.

b. Sophistication and complexity

The cloud's security related problems can also be linked to its sophisticated and complex architecture. Clouds provide criminals and espionage networks with convenient cover, tiered defenses, redundancy, cheap hosting and conveniently distributed command and control architectures. Another problem concerns the cloud's complexity.

D. Attractiveness and vulnerabilities of the cloud as a cyber crime target

a. Value of data in the cloud

Target attractiveness depends on offenders' perceptions of victims. Crime opportunity is a function of target attractiveness, which is measured in monetary or symbolic value and portability. It is also related to accessibility—visibility, ease of physical access, and lack of surveillance. Large companies' networks offer more targets to hackers. Cloud suppliers, which often are bigger than their clients, are attractive targets. Thus information stored in clouds is a potential goldmine for cyber-criminals

b. Criminal-controlled clouds

The cloud is potentially most vulnerable, especially when viewed against the backdrop of criminal owned-clouds operating in parallel**.** Just like diamond is the only material hard enough to cut diamond effectively, criminal-owned clouds may be employed to effectively steal data stored in clouds. The cloud may provide many of the same benefits to criminals as for legitimate businesses.

c. Perception of vendor's integrity and capability

Cloud providers must guard against theft or denial-of-service attacks by users. Users need to be protected from one another. Cloud providers may use insecure ways to delete data once services have been provided. Data theft, denial-of-service attacks by users, threats from other users, and bugs are some of the biggest-problems associated with the cloud. The cloud may also increase exposure to organizational vulnerabilities to insider risks. Intellectual property and other sensitive information stored in the cloud could be stolen. Worse still, cloud providers may not notify their clients about security breaches. An organization's data in the cloud may be stolen but it may not ever be aware that such incidents had happened. Cloud users don't have access to the hardware and other resources that store and process their data. There is no physical control over data and information in the cloud.

VII. STANDARDIZATION ACTIVITIES IN CLOUD COMPUTING

Various activities are being undertaken by different standard development organizations (SDOs) in the domain of cloud application and service deployments particularly with regards to security and privacy issues.

- NIST Cloud Standards
- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- Storage Networking Industry Association (SNIA)
- Open Grid Forum (OGF)
- Open Cloud Consortium (OCC)
- Organization for the Advancement of Structured Information Standards (OASIS)
- TM Forum
- International Telecommunication Union (ITU)
- The European Telecommunications Standards Institute (ETSI)
- Object Management Group (OMG)
- Association for Retail Technology Standards (ARTS)
- Institute of Electrical and Electronics Engineers (IEEE)
- Alliance for Telecommunications Industry Solutions (ATIS)
- Internet Engineering Task Force (IETF)

These organizations have made efforts to address security and privacy concerns in the cloud industry.

VIII. SOME PROPOSITIONS FOR SECURITY IN CLOUD COMPUTING

A. Information-centric security

In order for enterprises to extend control of data in the cloud, it may be worthwhile to take an approach of protecting data from within. This approach is known as information centric security. This self-protection technique requires intelligence be put in the data itself. Data needs to be self-describing and defending, regardless of its environment. When accessed, data consults its policy and attempts to recreate a secure environment that is verified as trustworthy using the framework of trusted computing (TC).

B. High-assurance remote server attestation

Data owners wish to audit how their data is being handled at the cloud, and ensure that their data is not being abused or leaked, or have an unalterable audit trail. An approach to address this problem is based on trusted computing. In a trusted computing environment, a trusted monitor is installed

at the cloud server that can monitor or audit the operations of the cloud server. The trusted monitor can provide proof of compliance to the data owner, guaranteeing that certain access policies have not been violated. To ensure integrity of the monitor, trusted computing also allows secure bootstrapping of this monitor to run beside the operating system and applications. The monitor can enforce access control policies and perform monitoring/auditing tasks. To produce a proof of compliance, the code of the monitor is signed, as well as a statement of compliance produced by the monitor. When the data owner receives this proof of compliance, it can verify that the correct monitor code is run, and that the cloud server has complied with access control policies.

C. Privacy-enhanced business intelligence

A different approach for retaining control of data is to require the encryption of all cloud data. The problem in this approach is that encryption limits data use. In particular, searching and indexing the data becomes problematic. For example, if data is stored in clear-text form, one can efficiently search for a document by specifying a keyword. This is impossible to do with traditional, randomized encryption schemes. The state-of-the-art cryptographic mechanisms may offer new tools to solve these problems. Cryptographers have invented versatile encryption schemes that allow for operations and computations on the cipher-texts. For example,searchable encryption (predicate encryption) allows the data owner to compute a capability from his secret key. A capability encodes a search query, and the cloud can use this capability to decide which documents match the search query. The cloud can use this capability to decide which documents match the search query, without learning any additional information. Other cryptographic primitives such as homomorphic encryption and private information retrieval (PIR) perform computations on encrypted source data without decrypting them

CONCLUSION

Cloud computing means having a server firm that can host the services for users connected to it by the network. Technology has moved in this direction because of the advancement in computing, communication and networking technologies. Cloud computing is clearly one of the most enticing technology areas of the current times due to its cost-efficiency and flexibility. Virtualized resources in the cloud lower upfront investment and product development costs. However, the low cost comes with a trade-off. Legitimate as well as illegitimate organizations and entities are gaining access to data on the cloud through illegal, extralegal, and quasi-legal means. The cloud's diffusion and that of social media have superimposed onto organizations' rapid digitization in a complex manner that allows cyber-criminals and cyber-espionage networks to exploit the cloud's weaknesses. The above analysis thus indicates that ensuring that both technological and behavioral/perceptual factors are given equal consideration in the design and implementation of a cloud network is thus crucial. In this regard, the war for the future of security and privacy issues in the cloud is just beginning. Overall, it is fair to say that privacy and security issues related to the cloud industry are undergoing political, social, and psychological metamorphosis.

References

[1] Jaydip Sen, "Security and Privacy Issues in Cloud Computing", Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.

[2] Siani Pearson "Privacy, Security and Trust in Cloud Computing", HP Laboratories HPL-2012-80R1

[3] Nir Kshetri, "Privacy and Security issues in cloudcomputing, PTC'11 Proceedings Page 1 of 23

[4] Mark D. Ryan "Cloud Computing Privacy Concerns on our doorstep", communications of the ACM journal, january 2011, vol. 54, no. 1

[5] Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinsky, A., Lee, G., Patterson, D.,Rabkin, A., Stoica, I., & Zaharia, M (2009), "Above the Clouds: A Berkley View of Cloud Computing",Technical Report No. UCB/EECS-2009-28, Department of Electrical Engineering and Computer Sciences, University of California at Berkley. February 10, 2009.

[6] Chen, Y., Paxson, V., & Katz, R.H. (2010). "What's New About Cloud Computing Security?" Technical Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley, 2010. Available Online at: http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html.

[7] Sen, J. (2011a). "A Robust Mechanism for Defending Distributed Denial of Service Attacks on Web Servers". International Journal of Network Security and its Applications, Vol 3, No 2, pp. 162-179, March 2011.

[8] Kaufman, L. M. (2009). "Data Security in the World of Cloud Computing". IEEE Security & Privacy, Vol 7, Issue 4, pp. 61-64, July-August 2009.

[9] Ricardo puttini, zaigham mahmood "Cloud Computing: Concepts, Technology & Architecture" (The Prentice Hall Service Technology Series from Thomas Erl) Kindle Edition.