ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

*Website: www.ijircce.com*

Vol. 5, Issue 7, July 2017

# A Survey on Security and Privacy Issues In Cloud Computing

G.Praveen Kumar, S.Kavitha

PG Scholar, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India

Assistant Professor, Dept. of Computer Technology, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India

**ABSTRACT:** Cloud computing is a new enlargement of grid, parallel, and distributed computing with visualization techniques. It is shifting the IT trade in a notorious way. Cloud computing has grown-up due to its recompense like storage capacity, resources pooling and multi-tenancy. On the other hand, the cloud is an open environs and since all the services are vacant over the Internet, there is a grand deal of uncertainty about security and privacy at diverse levels. This paper aims to address security and privacy issues threatening the cloud computing adoption by end users. Cloud providers are mindful of cloud security and privacy issues and are working hardly to address them. Few of these threats have been addressed, but many more threats still unsolved. This paper focused on cloud computing security and privacy threats, challenges, and issues. Furthermore, some of the countermeasures to these threats will be discussed and synthesized. Finally, possible solutions for each type of threats will be introduced before we end with conclusions and future work

**KEYWORDS**: Cloud computing, architecture, security issues, privacy issues, challenges, solution methods, privacy laws, privacy challenges, security challenges.

## I .INTRODUCTION

As the Internet grew more popular, many new technologies such as a cloud computing appeared and caught the attention of many industries. Cloud computing (CC) became popular because of its unique features like dynamic massive scalability, elasticity, measured service and self-provisioning of resources, convenient and on demand network access, and a shared pool of resources. This means that the cloud is an open and shared environment, which makes the privacy and security of users' data a complex issue. CC exhibits a lot of security threats like sensitive data loss, cloning and data leakage. The cloud providers are mindful of the cloud security and privacy issues and are working on addressing them. Only few of those threats have been addressed, but many more threats still unsolved. Security is one of the most significant challenges that face the cloud, and privacy makes the cloud more complex to maintain. When we think about the benefits of cloud computing which revolves around sharing resources, information and applications by computer devices connected to the cloud.

## II.RELATED WORK

Many benefits are gained from using cloud computing, but it also has a lot of threats and issues. The following review will try to understand the concept of cloud computing (CC), explore security and privacy issues, and provide solutions for them. Nowadays, the cloud is commonly used by various users as they can easily connect using web service or web browsers. CC is characterized by its dynamic infrastructures, global access, massive scalability, fine grain pricing, standard platforms, and management services. It also provides high level services and produces new directions and trends in the IT sector with low cost and low IT resource complexity. The owner of the infrastructure (third party) has the responsibility of service delivery to the users and the maintenance of the infrastructure. It's a special type of IaaS; allowing the client to pay only for the used parts rather than paying for the entire data base (site license). DaaS has been used with the applications that retrieve a huge amount of data with very small timeframe, like: apache Hbase, Google big-table and the Amazon S3.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

## III. SECURITY OF CLOUD COMPUTING

The cloud as a social infrastructure is the fact that makes security a critical problem The main drawback of the cloud is building a secure environment for the implementation, business software's, web management and email service offered by cloud computing. It provides enormous potential for a reliable, available, and agile infrastructure in an autonomic, distributed and grid computing environments. The cloud providers are aware of the cloud security issues, where it turned into a competitive factor for CC. providers. Using a trusted network and platform may improve the cloud security and storage. In order to enhance the service provider's performance, the service security must be guaranteed. A secure cloud provides a reliable service by protecting data and its services available to the client with high performance.

A. *The cloud Security Challenges:*

Security plays the most important role in cloud computing acceptance prevention, users can't imagine putting their information and running their software on external hard disk and someone else's CPU, these dreading too many. Several security issues like phishing and data loss produce serious threats to data and software operated by the organization. Moving toward cloud computing environment generates tradeoffs between integrations and communication costs. CC may reduce the cost of infrastructure but it may increase data communication cost. Such issue can be notable if the user uses the combination of private and public cloud deployment (hybrid cloud) where the resources are distributed among a number of private and public clouds. The cost analysis of elastic resource collection is more complicated than the traditional data center, where the cost is computed based on static computing consumption. Also, the virtual machine is going to become a unit cost rather than physical server analysis item. Strategic charging is critical for profitability and sustainability of the SaaS providers.SLA (Service Level Agreement): The user doesn't have full control over the resources in the cloud, but when migrating to the cloud, they need to ensure the reliability, performance, availability and the quality of the resources provided by CC service providers. This will be done using SLA. SLA contains levels of granularity, expressiveness vs. complicatedness, and tradeoffs forcovering the user needs and expectations.

CLASSIFICATION OF SECURITY CONCERNS ACCORDING ON CLOUD TYPE

| *Personal Cloud* | *General Cloud* |
|---|---|
| -Identity and access management.<br>-Data protection.<br>-Security intelligence.<br>-Software, platform & infrastructure security. | -DOS attack.<br>-Attack on virtual machine.<br>-Placing malicious code.<br>-Attack on physical machine. |
| *Domain-Specific Cloud* | *Mixed cloud* |
| -Compliance and auditing.<br>-Firewall feature &<br>-Intrusion detection.<br>-Access controls<br>-Antimalware & antivirus protection. | -Multiple cloud tenants<br>-Ongoing compliance concern..<br>-Identity management & access control.<br>-Data slinging. |

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

B. *The Cloud Security Issues:*

The literature contained many classifications and typologies of CC security issues, where researchers and practitioners described these issues from diverse views. Classified cloud computing security issues into two main categories: security issues faced by the providers and security issues faced by the users. Security issues are holding back the growth of CC market. Some companies are returning back to their own platforms because they don't need to be exposed to security risks. Also, others defined the main cloud security issues as follows: wrapping XML signature, Browser Security, Cloud middleware attacks, and Flooding attacks. The attacks that may affect the web service can also affect cloud computing due to the fact that the user uses web services and web browsers in order to connect to the cloud. One of the well-known attacks is wrapping XML signature for web service, while the XML signature had been used by WS-security in order to protect the elements name, values and its attributes from unauthorized parties. Attackers can produce malicious messages that can be addressed by using XML signature with WS-Security. Browser security is that attack when users send a message, they must wait a cloud server to complete the computational processes, before this request, the client must be authenticated to use the cloud system. These can be done with the SSL/TLS process, where the browser has to use it in order to encrypt the cardinalities and uses hand shake 4-ways to authenticate the clients. When the attacker starts sniffing the package, he can use the cloud as an authorized user, for handling this issue, WS security on the message level is implemented.

## IV. PRIVACY CHALLENGES AND ISSUES IN CLOUD COMPUTING

One of the most important goals we want to achieve in cloud computing security is protecting data privacy. But as we discussed earlier, it is difficult to prevent threats in cloud computing because it is a shared environment that depend on a shared infrastructure. So information will be exposed to the risk of unauthorized access. In other word we face a big challenge when we talk about sharing a cloud computing resources with protecting customer privacy. The important step to solve this challenge is data isolation, where each customer's information is isolated from other users' information. Another difficult issue about cloud computing is the movement of data, where data may transfer between countries and face local regulations. Information anonymity is the solution in this case by ensuring customers' data privacy and security .One of the biggest challenges for business adoption of cloud computing is the lack of privacy and data security. As discussed earlier, data security risks are potent because of open environment of CC. Such issue raises more challenges related to privacy where it increases the risks of information confidentiality because of the density of data within common clouds. After all these issues, we still need to have a proper policy that defines the relations between the major three entities in the cloud: consumers, utilities and third parties involved. To reach an acceptable level of cloud privacy, many issues need to be addressed like: Insufficient user control over his data, information disclosure in movement across the cloud, unauthorized secondary storage of sensitive data, uncontrolled data proliferation, and dynamic provision legal challenges.

## V.PRIVACY CHALLENGES SOLUTIONS

Many methods were proposed to preserve privacy anytime and anywhere. In this review we will describe some of these methods and approaches (called Privacy Preserving Methods). Any approach or technique used must guarantee both preserving the privacy of data as well as assuring data correctness. Anonymity-based Method: The anonymity algorithm works in a very logical manner, firstly, processes the data and anonymizes all or some information before shooting it in the cloud environment. Often not always, the cloud service provider (CSP) uses the background knowledge it has and incorporates the details with the anonymous data to mine the needed knowledge. When studying the traditional approach for privacy preserving (i.e. cryptography technology) we will find that this technique differs from Anonymity-based because Anonymity-based method gets rid of key management and thus it stands simple and flexible. But Anonymity-based method is easier, the attributes that has to be made anonymous varies and it depends on the cloud service provider. Privacy Preserving Authorization System: Users can define their access policies and how to access their data to assure the controlled access of data in the cloud. Policy Decision Points (PDP) and Policy Enforcement Points (PEP) are used for making authorization decisions and enforcing these decisions respectively. Master Policy Decision Points are launched, which figure out and solve the conflicts among various decisions of different PDPs. Obligation service is provided as a part of the authorization infrastructure, by means of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

which the data owner is informed/stated about authorized or unauthorized access of their data. As the cloud provider is trusted, encryption of outsourced data is not done.

## VI. PRIVACY LAWS AND REGULATIONS

Realizing the difficulties facing cloud computing, we must control the cloud using legal constraints, which are important because privacy intrusions on the Web are so prevalent,. These difficulties may result from deregulation of Internet issues (government's responsibility), to sustain an acceptable privacy levels and encourage users to use cloud computing. Also, researchers are worried that could computing concept will jeopardize online advertising industry and other related sectors. Another important issue to be considered when we are dealing with cloud computing environment is the social direction to regulate the domain. There are two main options that can be used: addressing the issues of market and self-regulation or by regulating it by the government. Within the privacy context there are differences between a self-regulation versus the government regulation. Some users believe that government shouldn't control the legal directions in privacy, trying to avoid the standard view of the big brother role of government. Other users proclaimed that self-regulation is difficult as no available mechanism in the CC industry to select educated, significant, and logical policies to implement.

## VII. SOLUTIONS TO SECURITY ISSUES

Many security issues such as data segregation, authentication, privacy, policy integration, console security, recovery, and access sensitive data, may face it. Another solution is by using better enterprise infrastructure; it provides configuration and installation of the components, such as firewalls, routers, operating systems and proxy servers.

COUNTERMEASURES FOR CSA THREATS

| | Forced threat name | Counter measure name |
|---|---|---|
| 1 | Nefarious Use, Confronting Abuse. | Monitor public blacklists, initial registration and validation processes. |
| 2 | Malicious Application Interfaces. | Access controls and authentication with encrypted transmission. |
| 3 | Malicious Insiders. | Specify resource requirements, compliance reporting, supply chain management. |
| 4 | Technology Vulnerabilities. | SLA, security in installation/configuration, monitoring the application environment. |
| 5 | Data Leakage /Loss. | Using API access, protecting and encrypting integrity of data, retention strategies. |
| 6 | Traffic Hijacking. | Using the user and service account credentials, understanding SLA/ providers' policy. |

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

## VIII.CONCLUSION

In this paper we explored the cloud computing environment and tried to discuss security and privacy concerns related to cloud computing. Also, we investigated the different architectures and their requirements, applications and associated challenges and concerns. In this paper we described some models and solutions to create a simplified view of cloud computing and solve some of problems which face businesses in their work. Also, in this work, privacy concerns were identified as an associated concern with security flaws. Privacy issues were discussed and some solutions also were proposed. To achieve privacy goals, we distilled few proposed methods from the literature such as: anonymity-based method, privacy preserving authorization system, privacy-preserving architecture and Oruta. There are much research on ensuring the security of outsourced data in an untrusted cloud data center and how to achieve the privacy of users' data.

## REFERENCES

[1]Patidar, K., Gupta, M. R., Singh, G., Jain, M. M., &Shrivastava, M. P. (2012). Integrating the Trusted Computing Platform into the Security of Cloud Computing System. *International Journal of Advanced Research inComputer Science and Software Engineering*, Vol. 2(2), pp. 1-5.
[2] Madhavi, K. V., Tamilkodi, R., & Sudha, K. J. (2012). Cloud Computing: Security threats and Counter Measures. International Journal of Research in Computer and Communication technology, IJRCCT, Vol. 1(4), pp.125-128.
[3] Ashktorab, V., & Taghizadeh, S. R. (2012). Security Threats and Countermeasures in Cloud Computing. International Journal of Application or Innovation in Engineering & Management (IJAIEM) , Vol. 1(2), pp. 234-245.
[4] Tiwari, P. K., & Mishra, B. (2012). Cloud Computing Security Issues, Challenges and Solution. International Journal of Emerging Technology and Advanced Engineering, Vol. 2(8), pp. 306-310.
[5] Malik, A., & Nazir, M. (2012). Security Framework for Cloud Computing Environment: A Review. Journal of Emerging Trends in Computing and Information Sciences, Vol.3(3), pp. 390-394.
[6] Younis, Y., Merabti, M. & Kifayat, K. (2013). Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep.