JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Security and Privacy Protection in Cloud Computing Discussions and Challenges

Dr. Prafullkumar Ashokrao Ghuge, Dr. Haridas Janardhan Kharat
Shankarlal Khandelwal Arts, Science & Commerce College, Akola

Abstract:
Security and privacy are the two most crucial factors influencing cloud computing services' popularity. Access control, attribute-based encryption (ABE), trust, and reputation have all been the basis of numerous research plans for cloud computing privacy security in recent years, but they are dispersed and lack cogent reasoning. We carefully evaluate and analyze pertinent research accomplishments in this study. Prior to presenting a thorough framework for privacy security protection, we outline several privacy security risks associated with cloud computing. Next, we present and explore the advancements made in various technologies' research, including access control, multi-tenant, trust, ciphertext policy attribute-based encryption (CP-ABE), key policy attribute-based encryption (KP-ABE), trace mechanism, fine-grain, multi-authority, revocation mechanism, proxy re-encryption (PRE), hierarchical encryption, searchable encryption (SE), and a combination of multiple technologies. Finally, we examine and compare the features and range of applications of typical schemes. We will talk about in this essay. The challenges and discussions surrounding security and privacy protection in cloud computing.

Keywords:
Protection, Cloud Computing, Privacy, Security, Attribute-Based Encryption, Hierarchical Encryption, Storage, Software Resources, Private Cloud Storage, Hybrid, Environment, Data Integrity

Introduction:
Several computers, storage, and software resources are connected via cloud computing to create a sizable shared virtual resource pool from which customers can buy related services, like hydropower. Applications for cloud computing are becoming more and more common, and as a result, cloud computing is now used in a wide range of sectors including production, education, entertainment, and scientific research.
The field of cloud computing has grown to be quite influential in the IT industry. For data storage, security, accessibility, and dependability on expenses, it is regarded as one of the most important qualities. Improvements in technology have led to a wide range increase in internet usage and an increase in hardware and software costs. The cloud computing concept, which aims to reduce the cost of hardware and software by offering services on demand via the internet, has been tremendously successful and popular in a short amount of time. [1]
Data or information integrity, availability, and confidentiality are all aspects of **security**. Non-repudiation and authentication are two further aspects of security.
Regarding the right to a private life, **privacy** refers to how one expresses or upholds different legal and nonlegal standards. This is frequently interpreted in the European context as adherence to European data protection laws. While mapping cloud issues onto the entire spectrum of privacy and personal data protection regulatory architectures would be extremely difficult, the widely recognized privacy principles—consent, purpose restriction, legitimacy, transparency, data security, and data subject participation—provide a helpful framework. [2]
The success and popularity of cloud computing can be attributed to recent advancements. On-demand computing resources and storage are offered by this innovative computing and business strategy. The primary goal of cloud computing is to generate financial gains because it provides a practical means of lowering capital and operating expenses. One fundamental component of cloud computing architecture is cloud storage, which enables online data sharing and storing for users. Offsite backup, effective and safe file access, limitless data storage capacity, and minimal use costs are a few benefits of cloud computing. Cloud storage is typically categorized into five types:
(1) Private Cloud Storage,
(2) Personal Cloud Storage,
(3) Public Cloud Storage,
(4) Community Cloud Storage, and
(5) Hybrid Cloud Storage.
Cloud computing is subject to many legal and regulatory frameworks, which present a variety of issues. Among these are the practicality of legal frameworks that impose obligations according to the location of cloud computing data service models. the difficulty of determining the relevant law and jurisdiction, the efficiency of cybercrime legislation in deterring and penalizing

cybercrime in the cloud, the establishment of the data subject's consent, and the effectiveness of breach notification regulations. The study revealed operational concerns regarding the efficacy of current risk governance frameworks, the ability of cloud customers to fulfill legal obligations when data or applications are hosted, the need to be compliant and accountable in the event of an incident, whether data will be locked into particular providers, the difficulties involved in conducting audits and investigations, how to determine the right degree of transparency, and, lastly, how to measure cloud security. [3]

Compliance: A higher degree of privacy, security, and trust in cloud computing environments can be achieved by improved harmonization of pertinent legal and regulatory frameworks. For instance: expanding breach reporting procedures to include cloud computing providers and enacting more efficient regulations for accountability and transparency that support a high degree of privacy and security in the protection of information.

Accountability: Rules allowing cloud users, particularly consumers, to exercise their rights should be improved. Service Level Agreement (SLA) models should also be improved, as they serve as the main means of ensuring that security, privacy, and trust duties are met.

Transparency: Enhancing the ability to identify, quantify, and manage the security, privacy, or trust levels provided to cloud customers and end users. This includes conducting research on best practices for security, developing automated methods for citizens to exercise their rights, and creating incident response protocols.

Governance: As part of its e-Commission program, the European Commission may take the lead in implementing cloud computing solutions and so indirectly aiding in the enhancement of currently in place operational risk control frameworks. Among other things, research funds could be used to enhance cloud-based Security Event and Incident Monitoring. [4]

Review of Literature:

They discussed how important it is to develop strategies and regulations to protect IoT systems, which in turn protect critical private information in Alferidah (2020). Security and privacy issues with IoT systems have become more pressing. There are many levels of hazard associated with security and privacy issues. Certain attacks carry greater risk than others. The origins of attacks also vary; some originate internally, while others originate externally. Although attacks can vary, they always carry a certain degree of risk and have unfavorable consequences. This survey study provided a review of the IoT security and privacy literature. Furthermore, the layer-by-layer breakdown of privacy and security issues with IoT systems. [5]

Cloud computing is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" by the National Institute for Standards and Technology (NIST) (Badger et al., 2011). It symbolizes an information technology paradigm change that many of us will probably witness in our lifetimes. While customers are thrilled about the potential to cut capital costs, free themselves from infrastructure management to concentrate on core skills, and, most importantly, the flexibility provided by on-demand computing provisioning, there are problems and obstacles that must be resolved before a widespread adoption can take place. [6]

Cloud computing environments are multidomain settings where distinct processes, interfaces, and semantics may be used by each domain, each of which may have different security, privacy, and trust requirements. These domains might stand for additional application or infrastructure components, or they could represent independently enabled services. Technology that naturally supports such multidomain formation through service composition and orchestration is service-oriented architectures. Building a thorough policy-based management framework in cloud computing environments requires utilizing the research that has already been done on secure service composition and multidomain policy integration (Takabi et al., 2010). We list a few crucial cloud computing security and privacy issues below that require quick solution to ensure widespread use of this technology. [7]

Objectives:

- To Study Challenges of **Security and Privacy Protection in Cloud Computing.**
- Organization of data security and privacy in cloud computing
- Introduction to Cloud Computing

Research Methodology:

The overall design of this study was exploratory. The research paper is an effort that is based on secondary data that was gathered from credible publications, the internet, articles, textbooks, and newspapers. The study's research design is primarily descriptive in nature.

Result and Discussion:

This research aims to examine various security approaches and obstacles related to data storage security and privacy protection in cloud computing environments. As illustrated in Figure 1, this paper offers a comparative study analysis of previous research on cloud computing solutions through data security elements such as availability, confidentiality, and integrity. Because data security and privacy are typically associated, cloud computing technologies and privacy concerns are also researched. By protecting data in the cloud computing environment, comparative studies on data security and privacy may contribute to an increase in consumer trust.

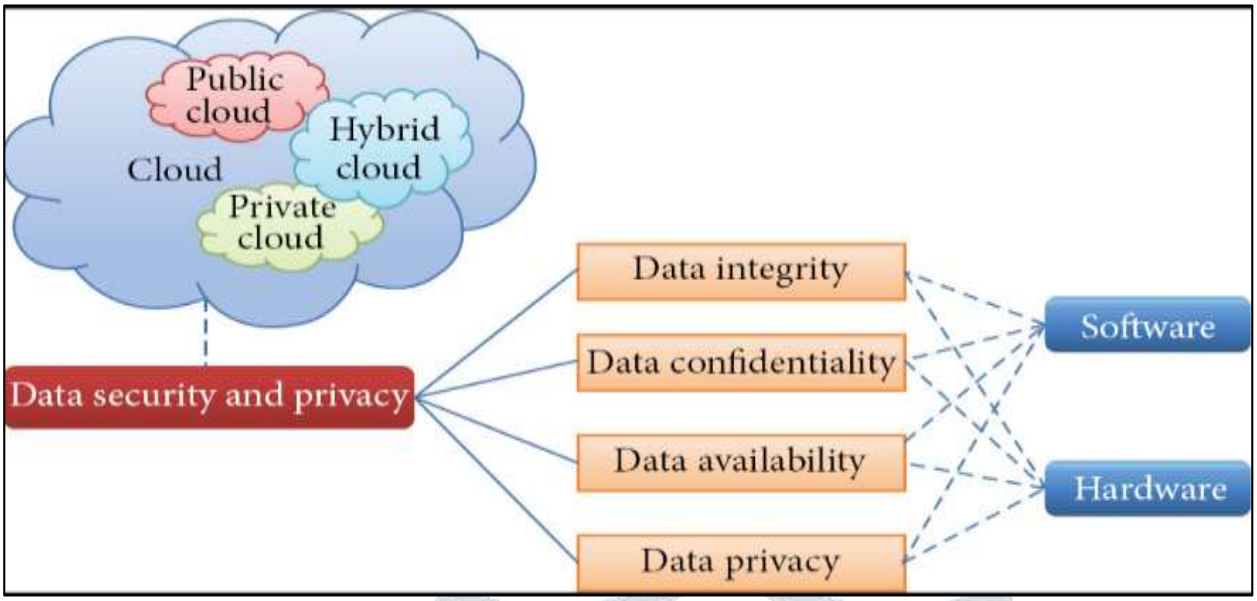

Figure 1: Organization of data security and privacy in cloud computing. [8]

- **Data Integrity**

In any information system, one of the most important components is data integrity. Data integrity generally refers to safeguarding data from illegal additions, deletions, or fabrications. Restricting access to certain enterprise resources and managing an entity's rights thereto guarantees that important information and services are not misused, pilfered, or destroyed.

In a standalone system with a single database, achieving data integrity is simple. A database management system (DBMS) typically completes database constraints and transactions, which are used to preserve data integrity in standalone systems. For data integrity to be guaranteed, transactions must adhere to the ACID (atomicity, consistency, isolation, and durability) criteria. Most databases are capable of maintaining data integrity and supporting ACID transactions. [9]

- **Data Confidentiality**

Users that save sensitive or private data on the cloud must ensure data confidentiality. Data confidentiality is ensured through the use of authentication and access control techniques. By enhancing the cloud's dependability and credibility, concerns about access control, authentication, and data secrecy could be resolved.

It is extremely risky for users to keep their sensitive data directly in cloud storage due to consumer mistrust of cloud providers and the near-impossibility of cloud storage service providers to completely eradicate insider threats. Complex requirements like inquiry, concurrent modification, and fine-grained authorization cannot be supported by simple encryption due to the key management issue.

- **Data Availability**

When an accident like hard drive damage, IDC fire, or network failure occurs, data availability refers to the following: the degree to which the user's data can be used or recovered; and the methods by which the user verifies their data independently of the cloud service provider's credit guarantee.

Customers have severe concerns about the issue of storing data on transborder servers since local laws regulate cloud companies, and clients need to be aware of these rules. Additionally, the cloud service provider is responsible for guaranteeing data security, specifically data integrity and confidentiality. Building a relationship of trust in this regard, the cloud provider should discuss all such concerns with the client.

- **Data Privacy**

The power to keep oneself or information about oneself private allows an individual or group to share certain aspects of themselves only. The components of privacy are as follows.

(i) When: Compared to information from the past, a subject's anxiety may be higher about information that will be revealed in the future or the present.

(ii) How: A user might feel more at ease if friends can ask for their information directly, but they might not like getting frequent, automated alerts.

(iii) Extent: Rather than an exact point, a user may prefer that his or her information be reported as an ambiguous region.

Cloud computing offers several services that forward three models: software as a service, platform as a service, and infrastructure as a service, as shown in Table I. Customers of cloud services can employ SaaS applications that are already operating on cloud infrastructure. These programs are available from any place. Salesforce.com, a CRM application, is an example of SaaS. In PaaS, the customer receives the platform as a service from the cloud provider, allowing him to use and manage its application without having to worry about managing cloud infrastructure. Example is Google Apps.IaaStype of service, cloud provider provide infrastructure where the consumer can manage its platform along with application for its purpose. Amazon Web Services is the finest illustration of IaaS. Public cloud, private cloud, and hybrid cloud are the three types of deployment methods mentioned in Table I by the NIST (2009). Private cloud refers to cloud infrastructure held for a specific purpose by an individual, corporation, or organization. The public is able to access the cloud infrastructure without restriction. A business, academic institution, governmental body, or a combination of these may own, administer, and run it. Public clouds are a type of cloud construction known as a hybrid cloud, which combines two or more different cloud infrastructures (private and public). [10]

Table 1. Introduction to Cloud Computing [11]

Five Essential Characteristics	1. On demand self-service 2. Broad network access 3. Resource pooling 4. Rapid elasticity 5. Measured Services
Three Service Models	1. Software as Service(Saas) 2. Platform as service(Paas) 3. Infrastructure as service(Iaas)
Deployment Models	1. Public Cloud 2. Private Cloud 3. Hybrid Cloud

The front end of a cloud architecture consists of various client types that utilize the cloud's services, while the cloud platform makes up the back end. The architecture is divided into layers, each of which is composed of a distinct cloud service model. Iaas, or infrastructure as a service, is the lowest tier of architecture and is responsible for managing network and storage resources both physically and virtually.

Security Issues, Challenges, and Methods:

Many security problems and obstacles can be found in cloud computing. A few security risks, difficulties, and threats related to cloud computing are covered in the section that follows, along with solutions. Figure 2: Secure cloud architecture.

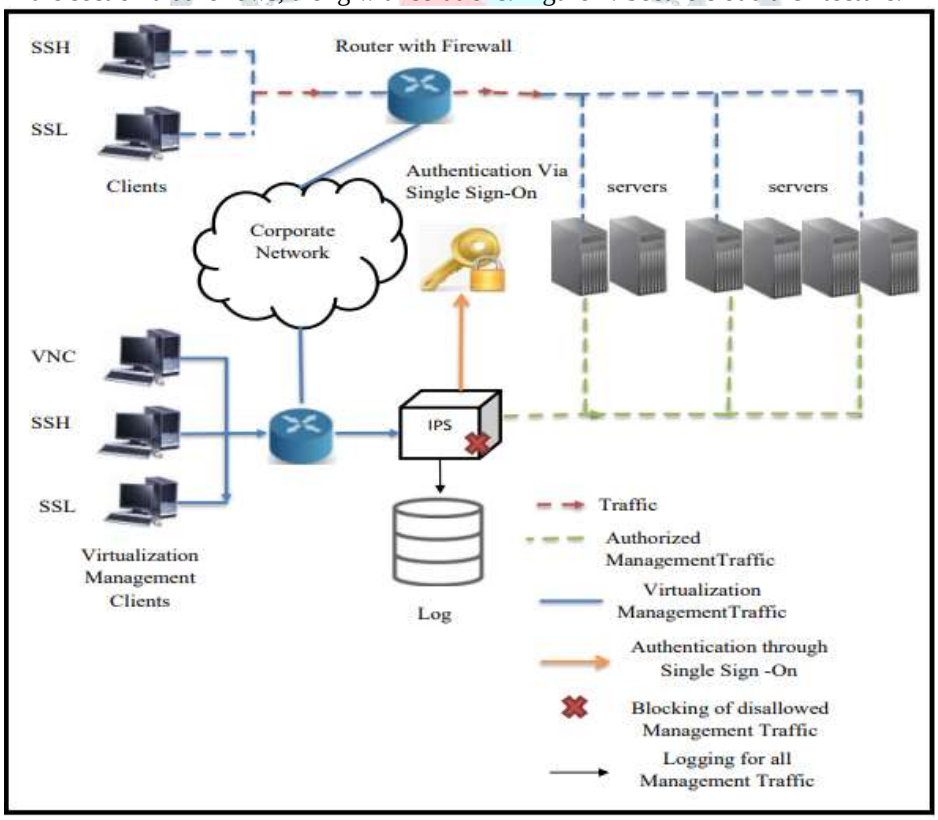

Figure 2: Secure Cloud Architecture [12]

Users of the cloud typically have a variety of login methods, but this leads to authentication issues. User level authentication is provided by Single Sign On. to use dynamic cloud storage servers inside the cloud infrastructure to improve data availability. To safeguard the cloud network, an appropriate virtual firewall and intrusion prevention system (IPS) should be deployed. Furthermore, the cloud network is secured via the single management console. Virtual Network Computing (VNC), Secure Shell (SSH) protocol, and Secure Sockets Layer (SSL) protocol are examples of virtual management clients.

Challenges to Security and Privacy:

It is the defense against passive attacks of transmitted data. Making sure that no unauthorized individual accesses or discloses sensitive customer data is the goal (Figure 2, The Privacy Issues of Cloud computing).

Figure 3: The Privacy issues of cloud computing.

The Internet of Things (IoT) is a networked, wireless system wherein smart nodes (IoT devices) exchange data via a communication channel with one another. Anybody who want to develop intelligent systems that rely on technology must now use IoT technologies. IoT made it possible to communicate with people more effectively. Nonetheless, the attackers let sensitive user data to be exploited by assaults on IoT systems.

Huge volumes of information about things like jeans, cancer, drugs, HIV, social networking sites, etc. can be described by the term "big data." In an effort to unravel mysteries surrounding biological systems, humans are trying to interpret biological data. Big data attracts people from a variety of industries. Big Data is becoming more and more prevalent in data scientists' biological streams, and it has more uses and applications than ever before. [13]

Conclusion:

This paper evaluates some of the most important privacy and security concerns associated with moving to cloud settings and lays out the foundation for a few strategies to deal with the problem. Many of these topics are expanded upon and investigated. New, forward-thinking methods based entirely on the increased value of personal information are made possible by cloud service delivery models and their carefully correlated capabilities for big data processing and extended statistics mining. Mechanisms must be provided so that both men and women may continue to manage this wider enterprise use of personal records, as it can be highly contentious. Among the technologies that hold the greatest promise for the upcoming generation of IT applications is cloud computing. Data security and privacy concerns are the main reasons for concern with the rapid expansion of cloud services. Any company's primary objective is to lower the cost of data storage.

References:

1. L. Teo and G.-J. Ahn, “Managing Heterogeneous Network Environments Using an Extensible Policy Framework,” Proc. Asian ACM Symp. Information, Computer and Communications Security, ACM Press, 2007, pp. 362–364.
2. H. Takabi et al., “An Architecture for Specification and Enforcement of Temporal Access Control Constraints using OWL,” Proc. 2009 ACM Workshop on Secure Web Services, ACM Press, 2009, pp. 21–28.
3. Mishra, S., S.K. Sharma, and M.A. Alowaidi, Analysis of security issues of cloud-based web applications. Journal of Ambient Intelligence and Humanized Computing, 2020: p. 1-12.
4. Mishra, Sambit Kumar, Sonali Mishra, Ahmed Alsayat, N. Z. Jhanjhi, Mamoona Humayun, Kshira Sagar Sahoo, and Ashish Kr Luhach. "Energy-Aware Task Allocation for Multi-Cloud Networks." IEEE Access (2020).
5. Alferidah, K. and Jhanjhi, N. (2020) A Review on Security and Privacy Issues and Challenges in Internet of Things. IJCSNS International Journal of Computer Science and Network Security, 20, 263-285.
6. Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2011). Draft Cloud Computing Synopsis and Recommendations. National Institute of Standards and Technology (NIST) Special Publication 800-146. US Department of Commerce. May 2011. Available online at: http://csrc.nist.gov/publications/drafts/800- 146/Draft-NIST-SP800-146.pdf (Accessed on: November 20, 2012).
7. Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010). Security and Privacy Challenges in Cloud Computing Environments. IEEE Security and Privacy, Vol 8, No 6, pp. 24-31, November-December 2010.
8. Arjun, U. and S. Vinay. A short review on data security and privacy issues in cloud computing. in 2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC). 2016. IEEE.
9. Yang, K.; Jia, X. Data storage auditing service in cloud computing: Challenges, methods and opportunities. World Wide Web 2012, 15, 409–428. [Google Scholar]
10. Arunarani, A.; Manjula, D.; Sugumaran, V. Task scheduling techniques in cloud computing: A literature survey. Future Gener. Comput. Syst. 2019, 91, 407–415. [Google Scholar]
11. Xiao, Z.; Xiao, Y. Security and privacy in cloud computing. IEEE Commun. Surv. Tutor. 2012, 15, 843–859.
12. Ryan, M. (2013). Cloud computing security: the scientific challenge, and a survey of solutions. J Syst Software. 86(9). 2263–2268.
13. Younis, A., Kashif, K. & Madjid, M. (2014). Cloud Computing Security & Privacy Challenges.