INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue6)

Available online at: www.Ijariit.com

A Review in Cloud Computing Security Using Steganography

Ataussamad
Dept.of Computer Science & Engineering
Madan Mohan Malaviya University of Technology
Gorakhpur (U.P.) INDIA
a.samad6387@gmail.com

Dr.Shiva Prakash
Dept.of Computer Science & Engineering
Madan Mohan Malaviya University of Technology
Gorakhpur (U.P.) INDIA
shiva.plko@gmail.com

Abstract: Cloud Computing is a flexible, cost-efficient, and authentic platform for providing business or consumer IT enabled services on the Internet. However, Cloud computing represents an added level of risk factors because important and essential services are often outsourced to a third party connected to cloud network, which makes it even harder to maintain the level of data security. Steganography is the technique of hiding or encapsulating information in digital media in order to prevent the existence of information. The digital media with hidden information within are called stego media and the data without hidden information are called cover media. Steganography can be used for hiding both the legal as well as illegal information. For example, civilians can use it for maintaining privacy while the government may use it for the security reasons of the country. In this paper we have discussed about the various techniques by which we can enhance the cloud service in relation to security and data privacy.

Keywords — Steganography, Security, CSP, Cryptography, Iaas, Paas, Saas.

I. Introduction

The importance of Cloud Computing is increasing day by day and it is getting a growing attention in industries as well as various scientific communities. A study by Gartner [1] considered Cloud Computing the first among the top ten most privileged technologies and has a better prospect in upcoming years by the companies and the organizations. Cloud Computing enables ubiquitous, flexible, on-demand network access to a shared pool of configured computing resources (i.e.., storage, application, server, network and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [2,3]. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [4-7]. Cloud Computing combines numbers of computing concepts and technology such as Service Oriented Architecture [SOA], Web 2.0, virtualization and there are various other technologies with confidence over the internet, providing online common business applications through browsers to satisfy the users need of computing, meanwhile their software as well as data are stored on the server [5]. In some aspects, Cloud Computing represents maturing of these available technologies and it's a marketing term to exhibit the maturity and the services they provides [6]. Although there are so many benefits of adopting to Cloud Computing, there are also few significant barriers to embracement. One of the most

significant barrier to adoption is security as well, followed by issues related to compliance, privacy and legal works [8]. Because Cloud Computing represented rather a fresh computing model, there is a great amount of uncertainty about how arrangements are done at all levels (e.g., network, host, application, and data levels) that can be achieved and how application and security is moved to Cloud Computing [9]. That uncertainty has consistently led information and data executives to state that security is their top concern with Cloud Computing [10]. Security concern relates to risky areas such as the external data storage, lack of control, dependency on the "public" internet, multi-tenancy as well as integration with internal security mechanism. As when compared to traditional technologies, the cloud contains many precise features, such as it is having a large scale and the case that resources which belongs to cloud providers are totally distributed, independent and fully virtualized. Various traditional security aspects such as authentication, identity, and authorization are not fully satisfactory for cloud in their current structure [11]. Security controls in Cloud Computing are, not much different than, security controls in an IT environment. Cloud Computing might present different type of risks to an organization than the classic IT solutions. Regrettably, integrating security mechanism into these solutions are often recognized as making them more rigorous [4]. Dragging sensitive data and critical applications to public cloud environment is of good concern for those various corporations that are moving behind their data center's networking structure under their control. To relieve these issues, Cloud solution provider should make sure that customers will still have the same security and privacy controls over their application and all the services, providing the proof to customers that their organization are safe and they can get their service level agreements, that they can approve compliance to auditors [12].A threat is a potential attack that may lead to a misuse of information or resources, and the term vulnerability refers to the flaws in a system that allows an attack to be successful. There are some surveys where they focus on one service model, or they focus on listing cloud security issues in general without distinguishing among vulnerabilities and threats. Here, we present a list of vulnerabilities and threats, and we also indicate what cloud service models can be affected by them. Furthermore, we describe the relationship between these vulnerabilities and threats; how these vulnerabilities can be exploited in order to perform an attack, and also present some countermeasures related to these threats which try to solve or improve the identified problems.

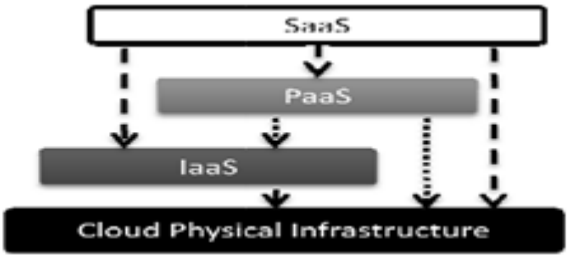

Figure 1: Cloud service delivery model

Some of the common issues related to security in the Cloud Despite the tremendous business and technical advantages of the cloud, the security and privacy concern has been one of the major hurdles preventing its widespread adoption. Especially for outsourced data services, the owners exclusive control over their data is ultimately relinquished to the CSPs [13]. For example, Google's recent privacy policy implies that they essentially own the right to arbitrarily handle the uploaded user data [14]. As a result, from the data owner's point of view, whenever their outsourced data contain sensitive personal information, such as financial and medical records, and social network profiles, it can no longer be considered as private as before.

Risks that is new and unique to cloud computing in respect of various security and privacy concerns [15].

•Outsourcing: Users may lose control of their data. Appropriate mechanisms needed to prevent cloud providers from using customer's data in a way that has not been agreed upon in the past.

• Extensibility and Shared Responsibility: There is a trade-off between extensibility and security responsibility for customers in different delivery models.

• Virtualization: There needs to be mechanisms to ensure strong isolation, mediated sharing and communications between virtual machines. This could be done using a flexible access control system to enforce access policies that govern the control and sharing capabilities of VMs within a cloud host.

• Multi-tenancy: Issues like access policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment.

• Service Level Agreement: The main goal is to build a new layer to create a negotiation mechanism for the contract between providers and consumers of services as well as the monitoring of its fulfillment at run-time.

• Heterogeneity: Different cloud providers may have different approaches to provide security and privacy mechanisms, thus generating integration challenges.

The remainder of the paper is organized as follows. In section 2 we have done the literature survey of the existing security mechanism.

II. Literature Survey

There are many different approached of storing data securely over the cloud, using mobile computing such as end-to-end encrypted data transmission, dynamic credential generation, steganography etc. The stored application or information on cloud raises security issues which are discussed in Bilogrevic [16]. To increase the storage capacity of mobile device, mobile users use cloud storage services. The mobile users do not have any control on the information store on the cloud which causes security and privacy issues [17][18][19].

Garima Saini et al. [20] research work titled "Triple Security of Data in Cloud Computing", in their proposed work they provide security by implementing three algorithms DSA, DES and steganography together to cloud network. To implement these three algorithms we use Asp.net as a platform. In proposed system for encryption first apply DSA for authentication of data. Then apply AES algorithm for encryption and then hiding data within audio file for provide maximum security to the data. Receiver can get original plain text by reversing the steganography, AES and DSA. They implements Digital signature Algorithm, Data Encryption Standard and Steganography to provide maximum security in cloud computing. By implementing these three algorithms provide authenticity, security and data integrity to the data. Then find that the time complexity is high because it is a one by one process but in future this time complexity could be reduced.

We classify cloud computing security related issues into the following five categories, which are summarized in Table 1. A similar approach to classify the issues is found in [21] but it is limited to small set of cloud security concerns.

No.	**Category**	**Description**
C1	Security Standards	Describes the standards required to take precaution measures in cloud computing in order to prevent attacks. It governs the policies of cloud computing for security without compromising reliability and performance.
C2	Network	Involves network attacks such as Connection Availability, Denial of Service (DoS),flooding attack, internet protocol vulnerabilities, *etc*.
C3	Access Control	Covers authentication and access control. It captures issues that affect privacy of user information and data storage.
C4	Cloud Infrastructure	Covers attacks that are specific to the cloud infrastructure (IaaS, PaaS and SaaS) such tampered binaries and privileged insiders.
C5	Data	Covers data related security issues including data migration, integrity, confidentiality, and data warehousing.

Table 1. Issues Relating to Security

The above table shows various categories which could probably are the most prone to security and must be protected through various mechanisms, some of which are discussed in this paper. C. Saravankumar and C. Arun [22] explain cloud computing issues and proposed new cloud computing security model. An important issue of the mobile cloud computing is to secure the user data is addressed in this

paper. There are many security standards and policies are available to secure the data such as data privacy, authenticated access to data, third party data protection, but these standards are exist only at the cloud end. It is a critical for the customer as well as provider to store, retrieve and transmit the data over the cloud network in a secure manner. To provide secure system, the authors have proposed the algorithm [22] to develop a customer owned security model. This algorithm is able to send the encrypted data to the provider. The provider can also apply the security by encryption over the customer's data by using the algorithm. The customer's data is secure at both the end. The proposed algorithm uses ASCII and BCD security with steganography that stores the encrypted data in an image file which will be send to the provider end. The security algorithm is using CDM (Common Deployment Model) which also provides an interoperable security services over the cloud. The main objective of the proposed algorithm is to control and send the data in an encrypted manner by the customer to the provider. The provider also maintains the data with a security algorithm to protect the data from unauthorized access.

Z. Al-Khanjari and A. Alani proposed a steganography scheme architectural model to protect data in cloud. Cloud computing systems needs to satisfy interoperability, security, safety, dependability, performance and many other parameters [23]. Security is one of the important issues, can be discussed and resolved using protected access control technique which can prevent security problems. Authors are proposing steganography to secure the data in cloud computing. The paper explains that how to hide the data through security pipeline channel. This provides protected access to the data. Steganography will provide safety, dependability, performance, integrity and confidentiality to the data for exchanging data over the network. It is hiding the data when data is requested and displayed. This steganography scheme uses text properties to hide the data, text properties includes font, font metrics, font styles, color and their RGB values, and the x, y location to display data. This steganography architecture supports cloud computing to provide security from unauthorized access. The architecture contains 3 layers physical Layer, data Layer, security Layer [23]. Security layer hides the data through security pipeline channel.

Here, we have explored various algorithms and their contribution in cloud data security various Symmetric Encryption algorithms are compared based on its techniques, description, concepts, security, issues addressed in table 2.

Author	**Technique Used**	**Description**	**Security Applied**	**Issue Addressed**
Padmapriya et al.[24]	Inverse Caesar Cipher	Classical Substitution cipher same key used for encryption and decryption	Cloud customer and Cloud provider	Data Security and Privacy
Sastry et al.[25]	Playfair Cipher	Classical substitution Cipher. Same key used for Encryption as well as Decryption	Cloud customer and Cloud provider	Data Security & privacy
Maha et al.[26]	Fully Homomorphic Encryption	The private key is used for Encryption (without Decryption)	Cloud Provider Site only	Data Security in cloud Scenario
Sugumaran et al.[27]	Block based Symmetric Cryptography	Symmetric layer inserted for encrypting the secure data using a symmetric algorithm	Cloud Customer Site	Data Security and Privacy
Monikandan et al.[28]	Classical Encryption	Both Substitution and Transposition. Same key used.	Customer site only	Data Security, Privacy and Authenticity

Neha Jain et al.[29]	DES Algorithm	The same key is used for Encryption and Decryption	Both Cloud customer and Cloud provider	Data Security
Wang, Cong, et al. [30]	Searchable Symmetric Encryption (SSE)	To prevent the cloud server learning the plaintext of either the data files or the search keywords	Both Cloud provider as well as Customer	Data Security over the cloud server
Abhishek Mohta[31]	Hash Algorithm	Store the root hash of the Tree to authenticate his received data	Cloud only	Not provide assurance about the correctness of Other outsourced data.
Giuseppe Ateniese[32]	RSA-based homomorphic authenticators	Ensure possession of data files on untrusted storage	Both Cloud provider as well as Customer	Security During Online Transfer of Data

Table 2. Comparison of various Security Techniques in cloud Security

III. Applications of Steganography

- In the business world audio data hiding, video data hiding and text data hiding can be used as a secret chemical formula or plans for a new invention. Audio data hiding can also be used in corporate world. Terrorists can also use audio data hiding to keep their communications secret and to co-ordinate attacks.
- Data hiding in video and audio is of interest for the protection of copyrighted [32] digital media and to the government for information system security and for covert communication.
- It can also be used in forensic application for inserting hidden data in to audio files for the authentication of spoken words and other sounds and in the music business for the monitoring of the songs over broadcast radio.
- For contracting firms, sending an authentic bedding letter with authorization signature and date, hand-written.
- In the stock market, to authorize the buying or selling of stocks [33]

IV. Conclusion

Here we have explored the various techniques proposed by several authors in various literature surveys. Steganography is the latest advancement as well as a very embellished technique of hiding the data in today's scenario where the cloud is mostly used by all users and their data keep synchronized to the cloud almost every time. This steganography application can be used on networks for data security

without using third party interference. The cloud computing application is able to embed only limited amounts of data into images. In the future, there is a scope of enhancing the capability from a few words to huge data files by replacing the steganography medium that is, images with audio or video files. In this literature Survey we have found that the proposed steganography techniques implemented by various authors will work perfectly as long as a user remembers the key, but if he loses the key, then the system does not have any provision for recovering or guessing the key, so in this case a user might lose the data in future there is a very vast scope of extending the steganography techniques by implementing it in more effective way it can also be used in the Mobile cloud data protection.

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. Zhao, Gansen, et al. "Cloud computing: A statistics aspect of users." IEEE International Conference on Cloud Computing. Springer Berlin Heidelberg, 2009.
3. Zhang, Shuai, et al. "Cloud computing research and development trend." Future Networks, 2010. ICFN'10. Second International Conference on. Ieee, 2010.
4. Jansen, Wayne, and Timothy Grance. "Guidelines on security and privacy in public cloud computing." NIST special publication 800.144 (2011): 10-11.
5. Jaatun, Martin Gilje, Gansen Zhao, and Chunming Rong, eds. Cloud Computing: First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009, Proceedings. Vol. 5931. Springer, 2009.
6. Rajasekaran, V., and M. Suganya. "An Analysis of SPI Security Issues for Cloud Computing." Biometrics and Bioinformatics 5.12 (2013):425.
7. Khalid, Ammar. "Cloud computing: Applying issues in small business." Signal Acquisition and Processing, 2010. ICSAP'10. International Conference on. IEEE, 2010.
8. Jung, Jae Un, and Hyun Soo Kim. "Deployment of Cloud Computing in Logistics Industry." Journal of Digital Convergence 12.2 (2014): 163-171.
9. Rosado, David G., et al. "Security analysis in the migration to cloud environments." Future Internet 4.2 (2012): 469-487.
10. Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.", 2009.
11. Li, Wenjuan, and Lingdi Ping. "Trust model to enhance security and interoperability of cloud environment." IEEE International Conference on Cloud Computing. Springer Berlin Heidelberg, 2009.
12. Rittinghouse, John W., and James F. Ransome. Cloud computing: implementation, management, and security. CRC press, 2016.
13. Li, Ming, et al. "Toward privacy-assured and searchable cloud data storage services." IEEE Network 27.4 (2013): 56-62.
14. Shahzad, Farrukh. "State-of-the-art survey on cloud computing security Challenges, approaches and solutions." Procedia Computer Science 37 (2014): 357-362.
15. Takabi, Hassan, James BD Joshi, and Gail-Joon Ahn. "Securecloud: Towards a comprehensive security framework for cloud computing environments." Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual. IEEE, 2010.
16. Bilogrevic, Igor, et al. "Meetings through the cloud: privacy-preserving scheduling on mobile devices." Journal of Systems and Software 84.11 (2011): 1910-1927.

17. Ren, Wei, et al. "Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing." Tsinghua Science & Technology 16.5 (2011): 520-528.

18. Yang, Jian, et al. "Provable data possession of resource-constrained mobile devices in cloud computing." Journal of networks 6.7 (2011): 1033-1040.

19. Tysowski, Piotr K., and M. Anwarul Hasan. "Re-Encryption-Based Key Management Towards Secure and Scalable Mobile Applications in Clouds." IACR Cryptology ePrint Archive 2011 (2011): 668.

20. Saini, Garima, and Naveen Sharma. "Triple Security of Data in Cloud Computing." International Journal of Computer Science & Information Technologies 5 (2014).

21. Sengupta, Shubhashis, Vikrant Kaulgud, and Vibhu Saujanya Sharma. "Cloud computing security--trends and research directions." 2011 IEEE World Congress on Services. IEEE, 2011.

22. Saravanakumar, and C. Arun. "AN EFFICIENT ASCII-BCD BASED STEGANOGRAPHY FOR CLOUD SECURITY USING COMMON DEPLOYMENT MODEL." Journal of Theoretical and Applied Information Technology 65.3 (2014).

23. Al-Khanjari, Z., and A. Alani. "Developing Secured Interoperable Cloud Computing Services." European Scientific Journal 10.24 (2014).

24. Praveenkumar, Padmapriya, et al. "Data puncturing in OFDM channel: A multicarrier stego." Information Technology Journal 13.12 (2014): 2037.

25. Herzog, S., et al. COPS usage for RSVP. No. RFC 2749. 1999.

26. Tebaa, Maha, and Said El Hajji. "Secure cloud computing through homomorphic encryption." arXiv preprint arXiv:1409.0829 (2014).

27. Sugumaran, M., B. Bala Murugan, and D. Kamalraj. "An architecture for data security in cloud computing." Computing and Communication Technologies (WCCCT), 2014 World Congress on. IEEE, 2014.

28. Arockiam, L., and S. Monikandan. "Data security and privacy in cloud storage using hybrid symmetric encryption algorithm." International Journal of Advanced Research in Computer and Communication Engineering 2.8 (2013): 3064-3070.

29. Anton, Annie I., et al. "HIPAA's Effect on Web Site Privacy Policies." IEEE Security & Privacy 5.1 (2007): 45-52.

30. Wang, Cong, et al. "Secure ranked keyword search over encrypted cloud data." Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010.

31. Mohta, Abhishek, Ravi Kant Sahu, and Lalit Kumar Awasthi. "Robust data security for cloud while using third party auditor." International journal of advanced research in computer science and software engineering 2.2 (2012).

32. Ateniese, Giuseppe, et al. "Provable data possession at untrusted stores." Proceedings of the 14th ACM conference on Computer and communications security. Acm, 2007.

33. Bender, Walter, et al. "Techniques for data hiding." IBM systems journal 35.3.4 (1996): 313-336.

34. Balaji, R., and Garewal Naveen. "Secure data transmission using video Steganography." Electro/Information Technology (EIT), 2011 IEEE International Conference on. IEEE, 2011.

