Designing Secure Architectures for Data Storage in Cloud Environments

Arslan Shahid[1], Sharjeel Imtiaz[2]

[1]Information Technology University of the Punjab, Pakistan
[2]Tallin University of Technology, Estonia

Correspondence:
Arslan Shahid: Arslan.shahid@itu.edu.pk

Article Link: https://www.brainetwork.org/index.php/jcai/article/view/17

DOI: https://doi.org/10.69591/jcai.1.2.1

JCAI
ISSN (P):3007-3049
ISSN (E):3007-3057
JOURNAL OF COMPUTING AND ARTIFICIAL INTELLIGENCE
ARTIFICIAL INTELLIGENCE
Published by
Beyond Research Advancement and Innovation Network

Citation: Shahid, A. & Imtiaz, S., (2023). Designing Secure Architectures for Data Storage in Cloud Environments, *Journal of Computing and Artificial Intelligence*, *1*(2), 1-10.

Conflict of Interest: Authors declared no Conflict of Interest

Acknowledgment: No administrative and technical support was taken for this research

Article History

Submitted: Sep 11, 2023
Last Revised: Oct 12, 2023
Accepted: Nov 28, 2023

Volume 1, Issue 2, 2023

Funding
No

An official Publication of
Beyond Research Advancement & Innovation Network, Islamabad, Pakistan

Designing Secure Architectures for Data Storage in Cloud Environments

Arslan Shahid[1]*, Sharjeel Imtiaz[2]

[1]Information Technology University of the Punjab, Pakistan

[2]Tallin University of Technology, Estonia

Abstract

Popularity of cloud computing is increasing day by day in the domain of information technology. It provides a lot of services utilizing resources that are dynamic and scalable. It enables users to cut their costs and also ease of utilization. Small as well as large enterprises are now inclined towards cloud solutions to enhance their services and businesses and also to easily integration with other enterprises. Even there are a lot of benefits that businesses achieve with cloud computing, however still some of the users are not comfortable to place their sensitive and private data on cloud due to security issues. The type of sensitive information may contain any personal identification information, government data, personal health information or emails etc. Because of that there is a need that cloud computing addresses the security issues during data transmission of sensitive information when shared on public environments. The type of security issues cloud computing is dealing with include; data privacy, data misuse, cyber-attacks or any other malicious attacks resulting in security breach. The intent of this paper is to highlight the issues in cloud computing related to security and to discuss the solution to deal with security issues. A secure architecture is presented in this paper that when applied secures not only the data transmission over cloud but also secure the data storage and enables authorized access.

Keywords: cloud computing, cyber-attacks, data privacy, malicious activity, secure architecture.

Introduction

The Cloud Service Provider provides security on cloud computing by employing solutions likes firewall and also virtualization. Although these mechanisms provide a level of security, but data cannot be considered completely protected. Another solution is encrypting the private data.

* Corresponding Author: Arslan.shahid@itu.edu.pk

However, with encryption there is an issue because of increased overheads in communication to access cloud. These are the reasons that cloud requires secure mechanisms for management of data and its storage so that authorized and controlled access of data can be maintained and the issues related to confidentiality and privacy [1].

A. *Cloud Data Storage Challenges & Issues*

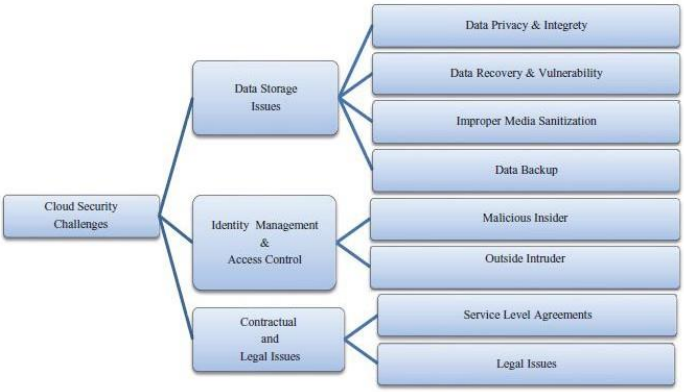
The service providers of cloud computing are able to access any data saved on cloud, they can manipulate data and also perform malicious activity like delete data, change, or make a local copy of any client data. Lack of control on data lead to many security issues. Figure 1 explains all the security issues faced by users working with cloud computing [2].

B. Data Recoverability

In cloud computing, there is dynamic on request resource assignment given to users through resource pooling. Due to that the resource that is assigned to one user can be at a later point of time be assigned to any other user. A malicious user can utilize data recovery techniques to access the data of the previous user from memory [3].

Figure 1

Security Issues in Cloud Computing


Cloud Security Challenges
Data Storage Issues
Identity Management & Access Control
Contractual and Legal Issues
Data Privacy & Integrety
Data Recovery & Vulnerability
Improper Media Sanitization
Data Backup
Malicious Insider
Outside Intruder
Service Level Agreements
Legal Issues

C. Data Backup

Keeping backup of data is also important in cloud computing. The service providers regularly take backups from cloud data storage to be utilized in case of any disaster. Backup of data should also have applied security guidelines so that any malicious user does not perform any data tampering on the data backups or get unauthorized access [4].

D. Data Privacy and Integrity

As it is discussed that there is need for cloud computing to make sure that the data integrity is maintained along with the privacy of data and confidentiality. Due to ease of use of cloud computing, the number of applications hosted on cloud is increasing as well as users accessing data. Because of this exponential growth in cloud computing, there are chances of increased security threats too. Even if there is security breach on a single data entity, then the entire data on cloud becomes at risk and can have unauthorized access [5]. This violation of data integrity loses the cloud computing multi-tenant feature. In addition to these issues, access of data is also a concern because of data transformation among multi-tenants. Also, virtualizations lead to sharing of physical resources in between different users. That is how the malicious insider attacks can be targeted by CSP. So, the malicious user is very easily able to access and compromise any other user data when accessing their own data. The security risk is increased even more when a third party is outsourcing the user's data by CSP. Encrypting data on cloud using public/private key is also not up to the mark [6].

Background

A. *Cloud Security Issues*

Cloud computing allows users to have on request access of network and data and shared resources like applications, services and storage. These resources are provided to users with much convenience and much less interaction of service provider [7]. Following are the security issues being faced by service providers and the users access cloud:

1. Data Storage is an issue where the CSP might scan or access user's data for commercial interests.

2. Selling private and sensitive data to third parties without taking any consent from users [8].

3. Accessing data is also an issue as the cloud servers and the users do not belong to the single trusted domain [9,10]. This makes it easier for the hackers to breach into the system. The server cannot be fully trusted to enforce and manage access and user information.

4. Another issue is the law issue, where government bodies can very easily access information from third parties without the consent of data owner. CSP can share user’s data to these agencies to identify any fugitives, violations of copyrights or any other required information by such agencies [11].

B. *Mimesis Aegis (M-Aegis)*

Mimesis Aegis (MAegis) is a preserving system for privacy that is intended to provide better protection of privacy for the user’s data on cloud. MAegis is regarded as the newer approach that is applied to maintain data privacy and preserving the user experience. This is achieved by creating a new conceptual layer Layer 7.5. This conceptual layer is actually introduced between the application layer, with is Layer 7 and the user layer which is the Layer 8. This conceptual layer 7.5 acts as a transparent layer operating on top of the application UIs. It intercepts the plain text from user input and after that transforms it to the application layer. Similarly, the output from the application is first transformed by this layer before converting it into plain text and presenting it to user [12]. This way an end-to-end encryption can be achieved through MAegis by completely segregating the data and the business logic from unauthenticated bodies. E2EE is also another solution to solve such data privacy issue. However, the law issue and storage issue in cloud computing still exists even with the implementation of MAegis [13,14].

C. *Controlled Functional Encryption*

Controlled Functional Encryption (CFE) is fresh and new technology in the cloud computing. The basic model of CFE uses the authorization key of the user (client) to access the encrypted data on the cloud. But in the advance computing whenever user (client) request for access the data needs a new key every time. This key has encrypted data which used to access to the information on the cloud. For the records holder, they subsidize their information with attached access policy restrictions [15] (e.g., number of periods it can be recycled in a calculation) to the structure only once and go disconnected [16].

Proposed Solution

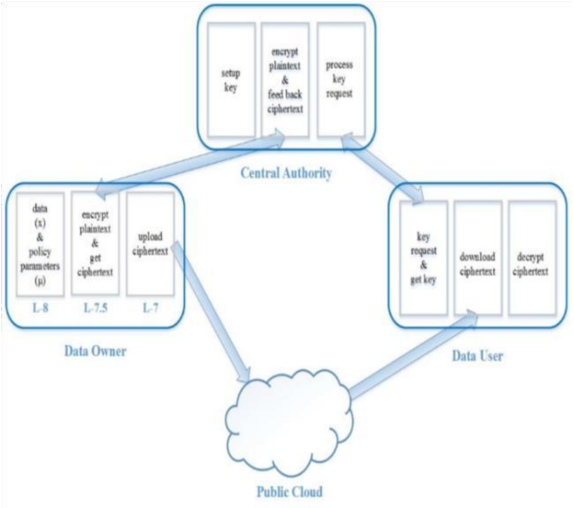
We are using different components in our purposed architecture like a public cloud, central authority, data user and the owner of data. In case the user wants to perform any operation, function or evaluate the data in the public cloud of any data owner, first the data uploads on the public cloud with specific parameters defining authorized users to access data with frequency of how many times data can be accessed. System central authority plays an important role and is fully trusted. The owner of data trusts on central authority for controlling access and enforce policies that are applied on cloud data. Central authority ensures what type of operation can be performed on cloud data.

A. Flow of the Architecture

Data owner has three layers like conceptual layer (L7.5) which communicates among the user and application layer (L7), (L8). When data is uploaded by data owner with different specifications/parameters the conceptual layer intercepts and transfers this plain text data to the central authority. When central authority gets this plain text and encrypt it and convert it to the cipher text. Then this central authority sends this data-to-data owner and data owner send this cipher text to cloud using the

Figure 2.

Secure Architecture for Cloud Computing



application layer. So, data user first request to the central authority. This request is called ‘Key request’. Then central authority checks from parameters which is sent by data owner with data and ensure that is the key issued to this user or not. And if key is issued user can download descriptive data and process it. First user decrypt it and then can use.

B. Cryptographic Modules

1. Key Manager

This key manager in central authority is responsible for the whole key process that is specified by the data owner through policy parameters. In these policy parameters, data owner defines access protocol that what type of user can access data and how many times. In this key manager there are different types of schemes. Complex password scheme and a simple password base KDF (key derivation function) are two such schemes.

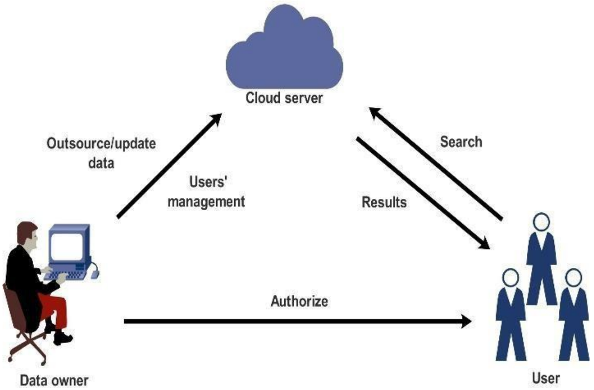
Complicated password base scheme ensures the authenticity of a user. Simple password base KDF are used to create symmetric keys as the default.

2. Searchable Encryption

Searchable encryption is of many types. In proposed secure architecture for cloud computing, we are proposing searchable encryption in cloud computing. The type of searchable encryption used in proposed solution is mSSE (multi-user symmetric searchable encryption). mSSE is beneficial as it is efficient and secure. In mSSE owner of data outsource their files to cloud. The data user or group of users authorized by data owner can download files and perform any data processing by generating search token. User decrypt files by using decrypt key and unique key. Cloud sever authenticates the token and present requested results to user.

Figure 3

Searchable Encryption in Cloud Computing



Conclusion

In this paper issues of cloud computing related to security are discussed with the possible solution in the form of secure architecture for cloud computing. With this secure architecture data owner can outsource their files or data to cloud without worrying about security and data privacy. Only authorized users would be able to access their data, download and manipulate it. This way any malicious user even if get access to cloud would not be able to access other user’s data. This way the integrity, confidentiality and privacy of data storage on cloud can be maintained.

References

[1] B. R. Kandukuri and A. Rakshit, “Cloud security issues,” in *2009 IEEE International Conference on Services Computing*, IEEE, 2009, pp. 517–520. Available: https://ieeexplore.ieee.org/abstract/document/5283911/

[2] B. Lau, S. Chung, C. Song, Y. Jang, W. Lee, and A. Boldyreva, “Mimesis Aegis: A Mimicry Privacy {Shield–A}{System’s} Approach to Data Privacy on Public Cloud,” in *23rd usenix security symposium (USENIX Security 14)*, 2014, pp. 33–48. Available: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/lau

[3] G. Forecast, “Cisco visual networking index: global mobile data traffic forecast update, 2017–2022,” *Update*, vol. 2017, p. 2022, 2019.

[4] S. Fahl, M. Harbach, T. Muders, and M. Smith, “TrustSplit: usable confidentiality for social network messaging,” in *Proceedings of the 23rd ACM conference on Hypertext and social media*, Milwaukee Wisconsin USA: ACM, Jun. 2012, pp. 145–154. doi: 10.1145/2309996.2310022.

[5] M. Naveed *et al.*, “Controlled Functional Encryption,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Scottsdale Arizona USA: ACM, Nov. 2014, pp. 1280–1291. doi: 10.1145/2660267.2660291.

[6] M. Nabeel and E. Bertino, “Privacy preserving delegated access control in public clouds,” *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2268–2280, 2013.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in *2010 proceedings ieee infocom*, Ieee, 2010, pp. 1–9. Available: https://ieeexplore.ieee.org/abstract/document/5462173/

[8] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” in *Financial Cryptography and Data Security*, vol. 6054, R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. M. Miret, K. Sako, and F. Sebé,

Eds., in Lecture Notes in Computer Science, vol. 6054. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 136–149. doi: 10.1007/978-3-642-14992-4_13.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in *Proceedings of the 13th ACM conference on Computer and communications security*, Alexandria Virginia USA: ACM, Oct. 2006, pp. 79–88. doi: 10.1145/1180405.1180417.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring data storage security in cloud computing," in *2009 17th International Workshop on Quality of Service*, Ieee, 2009, pp. 1–9. Available: https://ieeexplore.ieee.org/abstract/document/5201385/

[11] M. Aazam, P. P. Hung, and E.-N. Huh, "Smart gateway based communication for cloud of things," in *2014 IEEE ninth international conference on intelligent sensors, sensor networks and information processing (ISSNIP)*, IEEE, 2014, pp. 1–6. Accessed: May 15, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6827673/

[12] S. Vinoski, "Advanced message queuing protocol," *IEEE Internet Comput.*, vol. 10, no. 6, pp. 87–89, 2006.

[13] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Cooperative private searching in clouds," *J. Parallel Distrib. Comput.*, vol. 72, no. 8, pp. 1019–1031, 2012.

[14] A. S. Rao *et al.*, "A Secured Cloud Architecture for Storing Image Data using Steganography," in *2024 2nd International Conference on Computer, Communication and Control (IC4)*, IEEE, 2024, pp. 1–6. Accessed: May 15, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10486495/

[15] I. Bouleghlimat, S. Boudouda, and S. Hacini, "PPSecS: Privacy-Preserving Secure Big Data Storage in a Cloud Environment," *Arab. J. Sci. Eng.*, vol. 49, no. 3, pp. 3225–3239, Mar. 2024, doi: 10.1007/s13369-023-07924-4.

[16] S. Guan, C. Zhang, Y. Wang, and W. Liu, "Hadoop-based secure storage solution for big data in cloud computing environment," *Digit. Commun. Netw.*, vol. 10, no. 1, pp. 227–236, 2024.

[17] N. Jain and P. Singhal, "Securely Cloud Data Storage and Sharing," *J. Inform. Electr. Electron. Eng. JIEEE*, vol. 5, no. 1, pp. 1–12, 2024.

[18] E. M. Mohammed and E. H. Ziyati, "Novel Approach for Protecting Personal Sensitive Information in a Cloud Storage Environment," *Int. J. Comput. Digit. Syst.*, vol. 16, no. 1, pp. 1–10, 2024.

[19] M. Kuštelega and R. Mekovec, "Migrating data to the cloud: An analysis of cloud storage privacy and security issues and solutions," *CroDiM Int. J. Mark. Sci.*, vol. 7, no. 1, pp. 89–98, 2024.

[20] N. I. Ali, A. G. Memon, and A. Jamali, "Architectural Design for Data Security in Cloud-based Big Data Systems," *Baghdad Sci. J.*, 2024, Accessed: May 15, 2024. [Online]. Available: https://www.bsj.uobaghdad.edu.iq/index.php/BSJ/article/view/8722

[21] V. Bande, B. D. Raju, K. P. Rao, S. Joshi, S. H. Bajaj, and V. Sarala, "Designing Confidential Cloud Computing for Multi-Dimensional Threats and Safeguarding Data Security in a Robust Framework," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 11s, pp. 246–255, 2024.

[22] S. R. Vulapula and H. B. Valiveti, "Secure and efficient data storage scheme for unstructured data in hybrid cloud environment," *Soft Comput.*, vol. 26, no. 23, pp. 13145–13152, 2022.

[23] M. I. Reddy, P. V. Rao, T. S. Kumar, and S. R. K, "Encryption with access policy and cloud data selection for secure and energy-efficient cloud computing," *Multimed. Tools Appl.*, vol. 83, no. 6, pp. 15649–15675, Jul. 2023, doi: 10.1007/s11042-023-16082-6.