IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 10, October 2021

DOI: 10.17148/IJARCCE.2021.101018

# An In-Depth Look at the Issues around Data Security and Privacy in Cloud Computing

**Sheikh Md Zubair Md Zahoor**

Former Research Scholar, Computer Science, OPJS University, Churu, Rajasthan, India

**Abstract**: In the field of information technology, cloud computing is swiftly becoming a hotspot. Nevertheless, when we look at its ease of use and high data processing capabilities, we find that it also poses significant issues in terms of data security and privacy information protection. The current security and privacy information concerns have been evaluated in this study. Second, a summary of current security measures is provided.

**Keywords**: Cloud Computing; Data Security; Privacy Information; Cloud Computing Provider.

## I. INTRODUCTION

Unlike traditional computing models, cloud computing (Iosup et al., 2011; Prasad and Rao, 2014; Li et al., 2015; Yuriyama and Kushida, 2011; Mori et al., 2012; Raekow et al., 2013; Yao et al., 2013; Ye and Khoussainov, 2013; Zhu et al., 2013; Ronald et al., 2013 merge many new components, such as remote computing and virtualization, have come together to create a novel system that can be managed and dynamically expanded.

Cloud computing security encompasses all areas of cloud computing protection. Many of these issues aren't specific to the cloud: data is vulnerable to assault regardless of where it's kept. As a result, cloud computing security covers all aspects of computing security, including security architecture design. Cloud computing, on the other hand, offers a number of unique features (Ryan, 2013; Chen et al., 2010; Kumar, 2010; Christodorescu et al., 2009):

a Because the cloud is really a shared resource, we can't ensure that other users won't be dangerous. To put it another way, we can't verify the veracity of other sources.
b Insecure APIs and protocols may be given permission to access cloud data.
c Once the security mechanism fails, the illegal cloud provider has access to the data in the cloud and can edit or destroy it.
d It's acceptable for cloud data to be accessible, but only to a certain level.

To tackle the above possible shortcomings, references (Chang et al., 2016; Ali et al., 2015; Naser et al., 20015; Xiang et al., 2015; Oscar et al., 2015; Rasheed, 2014; Feng et al., 2011; Lin et al., 2013; Wlodarczyk et al., 2009; Ai and Mukaidono, 2011; Hsu et al., 2011; Kryvinska et al., 2010; Siemens IT Solutions and Services, 2011) several unique models or approaches have been presented. Virtual computers, for example, can be deployed in the cloud to isolate operations. In terms of data security, deploying a viable and feasible backup method is an option. Naturally, different models are built to detect the incorrect alterations.

This paper gives a summary of cloud computing and related security concerns, as well as potential options in the sector, based on the information indicated above. The following is a breakdown of the paper's structure.

The classic cloud computing theory is introduced in Section 2. Section 3 discusses potential answers or proposals for the current difficulties in cloud computing. Finally, Section 4 brings the paper to a close.

## II. CLASSIC THEORY OF CLOUD COMPUTING

Cloud computing has the capability of handling big batches of task requests for a large number of clients at the same time. When cloud service providers receive service requests, they distribute matching computer resources based on the varied requests from customers or the dispenses of the cloud computing resources that the clients pay for. Figure 1 depicts the standard cloud computing model.

Private, public, communal, and hybrid clouds are the four forms of cloud computing available (Wlodarczyk et al., 2009).

a An organization owns or rents a private cloud. The entire cloud resource is reserved for that organization's exclusive usage. A cloud constructed by a company to service its mission-critical applications is an example of this model.
b A service provider owns a public cloud, and its resources are sold to the general public. End-users can rent portions of the resources and scale their resource consumption to meet their needs.

Public cloud providers include Amazon, Google, Rackspace, Salesforce, and Microsoft.

c A community cloud is comparable to a private cloud, except the cloud resource is shared among members of a small group of people who share similar interests. The media cloud set up by Siemens IT Solutions and Services (2011) for the media sector is an example of a community cloud. A community cloud can be managed by a third party (as in Siemens' example) or collaboratively controlled and operated (as in the grid computing paradigm).

d The term "hybrid cloud" refers to a cloud infrastructure that combines two or more cloud infrastructures, which can be private, public, or community clouds. The fundamental goal of a hybrid cloud is to provide additional resources in times of high demand, such as allowing some processing jobs to be transferred from a private cloud to a public cloud.

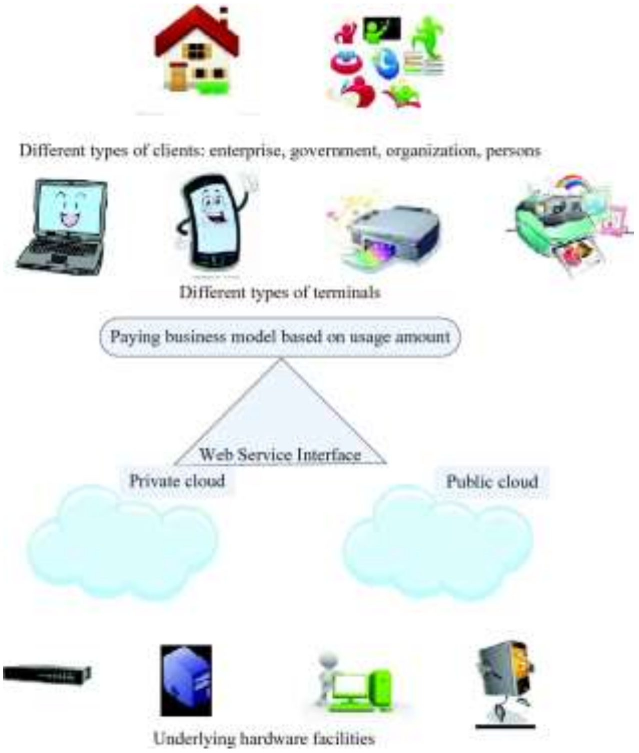
Different types of clients: enterprise, government, organization, persons
Different types of terminals
Paying business model based on usage amount
Web Service Interface
Private cloud
Public cloud
Underlying hardware facilities

**Figure 1** Traditional cloud computing model (see online versionfor colours)

### III.3 CURRENTLY USED SECURITY MEASURES

The current security measures are summarized below in order to address the issues described above.

*Privacy data access processing*

The community cloud is made up of two or more clouds that run independently and allow data and applications to be transferred between them. The community cloud, which is made up of both private and public clouds, has both advantages: it has the privacy of the private cloud as well as the reduced computing costs of the public cloud. As a result, many firms and organizations have adopted the community cloud as their preferred model, and it is widely recognized as the primary paradigm of future cloud computing.

Although combining public and private clouds is a fair approach for dealing with cloud computing security and privacy, integrating the two types of clouds properly remains a difficult subject. There are two parts to the perfect item. On the one hand, we can take advantage of the public cloud's extensive computational and storage resources. Client private information, on the other hand, must be effectively protected.

Several researchers presented a novel community cloud mode that included a privacy protection module based on the Hadoop MapReduce paradigm, allowing for the realization of privacy-sensing-based community cloud computing. The basic concept is to divide computing chores, with sensitive privacy data being stored in the private cloud and non-sensitive data being stored in the public cloud. The limitation is that the sensitive data must be assigned by the client, therefore the aforementioned mode could do nothing with the unknown sensitive data.

*Data encoding and search*

As a result of the encoding, the original ordering, comparability, and other qualities may be lost, making data searches more difficult. The following is a direct searching technique for cloud storage. The data owner must first obtain the encrypted text from the cloud server. The plaintext is then decoded from the encrypted text. Finally, let the machine look for plaintext data. Clearly, the procedure described above is inefficient.

Early references mentioned a feasible encrypt data searching algorithm that uses a symmetric encryption algorithm to encapsulate the text and its keywords. The server can look up which texts include the keywords provided by the clients, but it can't get any practical information about the text's content. Furthermore, the existing search strategy can only complete searches for a single keyword, but it does not meet the needs of most clients. To ensure that public-key encryption with keyword searching is more appropriate to cloud computing environments, we need develop a new public-key encryption scheme that can provide privacy protection as well as complicated logic expression.

*Encoding data computing*

With the rapid development of cloud computing, data owners can now upload large amounts of data to a cloud server for computing and searching, which helps to reduce storage, calculation, and maintenance costs. Property encryption and homomorphic encryption have recently been used to address the problem of encoding data computation.

The cipher text and plaintext are conducted concurrently and directly in homomorphic encryption. Even if the plaintext is unknown, the cipher text can still be generated using this procedure. The data is initially encoded by the clients, then the cipher text is uploaded to the cloud server. The server can carry out the data cipher text according to the clients' specifications and return the computed result to them. The clients can use the private key to decode the encrypted text and obtain the plaintext computed result. Clients, on the other hand, are unable to verify the accuracy of the cloud server's computed result.

## IV. CONCLUSION

Cloud computing has become a widely accepted and universal paradigm for service-oriented computing, in which computing infrastructure and solutions are provided as a service. The classic theory of cloud computing is initially introduced in this work. The potential security and privacy data concerns are then discussed. The current metrics are also summarized at the end.

## REFERENCES

[1]. Ai, L.A.P. and Mukaidono, M. (2011) ‘Selection of model in developing information security criteria for smart grid security system’, *Journal of Convergence*, Vol. 2, No. 1, pp.39–46.

[2]. Ali, M., Khan, S.U. and Vasilakos, A.V. (2015) ‘Security in cloud computing: opportunities and challenges’, *InformationSciences*, Vol. 305, No. 3, pp.357–383.

[3]. Baek, S.J., Park, S.M., Yang, S.H. et al. (2010) ‘Efficient server virtualization using grid service infrastructure’, *Journal of Information Processing Systems*, Vol. 6, No. 4, pp.553–562.

[4]. Chang, V., Kuo, Y.H. and Ramachandran, M. (2016) ‘Cloud computing adoption framework: a security framework for business clouds’, *Future Generation Computer Systems*, Vol. 57, No. 1, pp.24–41.

[5]. Chen, Y., Paxson, V. and Katz, R.H. (2010) *What’s New About Cloud Computing Security?*, Technical Report UCB/EECS-2010-5, Electrical Engineering and Computer Sciences, University of California at Berkeley.

[6]. Christodorescu, M., Sailer, R., Schales, D.L. et al. (2009) ‘Cloud security is not (just) virtualization security: a short paper’, in *Proceedings of the ACM Workshop on Cloud Computing Security*, pp.97–102.

[7]. Feng, D.G., Zhang, M., Zhang, Y. et al. (2011) ‘Study on cloud computing security’, *Journal of Software*, Vol. 22, No. 1,pp.71–83.

[8]. Hsu, P.H., Tang, W.S., Tsai, C. et al. (2011) ‘Two-layer security scheme for AMI system’, *Journal of Convergence*, Vol. 2,No. 1, pp.47–52.

[9]. Iosup, A., Ostermann, S., Yigitbasi, M.N. et al. (2011) ‘Performance analysis of cloud computing services formany-tasks scientific computing’, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 6, pp.931–945.

[10]. Kong, W.W., Lei, Y. and Ma, J. (2016) ‘Virtual machine resource scheduling algorithm for cloud computing based on auction mechanism’, *Optik*, Vol. 127, No. 12, pp.5099–5104.

[11]. Kryvinska, N., Thanh, D.V. and Strauss, C. (2010) ‘Integratedmanagement platform for seamless services provisioning in converged network’, *International Journal of Information Technology Communications & Convergence*, Vol. 1, No. 1, pp.77–91.

[12]. Kumar, S.N. (2010) *Top Threats to Cloud Computing v1.0*, Cloud Security Alliance [online] http://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[13]. Li, J., Tan, X., Chen, X.F. et al. (2015) ‘OPoR: enabling proof of retrievability in cloud computing with resource-constrained devices’, *IEEE Transactions on Cloud Computing*, Vol. 3,No. 2, pp.195–205.

[14]. Lin, C., Su, W.B., Meng, K. et al. (2013) ‘Cloud computing security: architecture, mechanism and modeling’, *Chinese Journal of Computers*, Vol. 36, No. 9, pp.1765–1784.

[15]. Mori, T., Nakashima, M. and Ito, T. (2012) ‘SpACCE: a sophisticated ad hoc cloud computing environment built by server migration to facilitate distributed collaboration’, *International Journal of Space-Based and Situated Computing*, Vol. 2, No. 4, pp.230–239.

[16]. Narayana, I.N.C.S., Gopinath, G., Mogan, K.P.C. et al. (2014) ‘A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment’, *International Journal of Grid and Utility Computing*, Vol. 5, No. 4, pp.236–248.

[17]. Naser, S., Kamil, S. and Thomas, N. (2015) 'A case study ininspecting the cost of security in cloud computing', *Electronic Notes in Theoretical Computer Science*, Vol. 318, No. 11, pp.179–196.
[18]. Oscar, R., Daniel, M., Eduardo, F.M. et al. (2015) 'Empirical evaluation of a cloud computing information security governance framework', *Information and Software Technology*, Vol. 58, No. 2, pp.44–57.
[19]. Prasad, A.S. and Rao, S. (2014) 'A mechanism design approachto resource procurement in cloud computing', *IEEE Transactions on Computers*, Vol. 63, No. 1, pp.17–30.
[20]. Raekow, Y., Simmendinger, C., Jenz, D. et al. (2013) 'On-demand software licence provisioning in grid and cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4, No. 1, pp.10–20.
[21]. Rasheed, H. (2014) 'Data and infrastructure security auditing in cloud computing environments', *International Journal of Information Management*, Vol. 34, No. 3, pp.364–368.
[22]. Ronald, P., Stephan, S. and Christoph, S. (2013) 'A
[23]. privacy-friendly architecture for future cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4,No. 4, pp.265–277.
[24]. Ryan, M.D. (2013) 'Cloud computing security: the scientific challenge, and a survey of solutions', *The Journal of Systems and Software*, Vol. 86, No. 9, pp.2263–2268.
[25]. Siemens IT Solutions and Services (2011) *Community Clouds: Supporting Business Ecosystems with Cloud Computing* [online] http://docplayer.net/1234732-Community-clouds-supporting-business-ecosystems-with-cloud-computing.html.
[26]. Wlodarczyk, T., Rong, C.M. and Thorsen, K.A. (2009) 'Industrial cloud: toward inter-enterprise integration', *Cloud Computing, Lecture Notes in Computer Science*, Vol. 5931, pp.460–471, Springer, Berlin/Heidelberg.
[27]. Xiang, Y., Martino, B.D., Wang, G.L. et al. (2015) 'Cloud computing: security, privacy and practice', *Future Generation Computer Systems*, Vol. 52, No. 11, pp.59–60.
[28]. Yao, Z.Q., Xiong, J.B., Ma, J.F. et al. (2013) 'Access controlrequirements for structured document in cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4, Nos. 2–3, pp.95–102.
[29]. Ye, X.F. and Khoussainov, B. (2013) 'Fine-grained access control for cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4, Nos. 2–3, pp.160–168.
[30]. Yuriyama, M. and Kushida, T. (2011) 'Integrated cloud computing environment with IT resources and sensor devices', *International Journal of Space-Based and Situated Computing*, Vol. 1, Nos. 2–3, pp.163–173.
[31]. Zhu, X.D., Li, H. and Li, F.H. (2013) 'Privacy-preserving logistic regression outsourcing in cloud computing', *International Journal of Grid and Utility Computing*, Vol. 4, Nos. 2–3, pp.144–150.