Review Article

International Journal of Advanced Technology and Engineering Exploration, Vol 7(73)
ISSN (Print): 2394-5443 ISSN (Online): 2394-7454
http://dx.doi.org/10.19101/IJATEE.2020.762181

An analytical review and analysis for the data control and security in cloud computing

Makrand Samvatsar[1*] and Priyesh Kanungo[2]
Research Scholar, School of Computer Science and Information Technology Devi Ahilya Vishwavidyalaya, Indore, Madhya Pradesh, India[1]
Professor & Senior System Engineer, DAVV (SCS), Indore, Madhya Pradesh, India [2]

Received: 03-October-2020; Revised: 27-December-2020; Accepted: 29-December-2020

Abstract
In this paper an analytical review and analysis for the data control and security in cloud computing was presented and analysed. This review and analysis covers three aspects. First is the study of the wide acceptability of cloud computing and its areas of applicability. Second is the security aspect in terms of data handling and data sharing. Third aspect is the interdisciplinary areas like Internet of Things (IoT) and big data in terms of collaboration with cloud computing environment. These components were discussed and analysed with the parametric evaluation along with the analytical variations. This paper presented an analytical view with the exploration of authenticity and data integrity. It also shows the result analysis with the performance measures. It also highlights the gaps along with the solution methodology with insightful discussion. This paper also highlights the problem statements with the suggested solutions and the future work in the same direction.

Keywords
Cloud computing, IoT, Big data, Data integrity, Data security.

1.Introduction
Cloud computing facilities the resources on-demand. It has been processed generally over the internet [1]. The processing incorporates several applications to storage and processing it through the internet [2−4]. So, it is like a rent for the computing infrastructure based on the user demand [5]. This includes all the resources from the applications to the complete storage. The providers are called the cloud service providers. It is beneficial for the business enterprises and firms to avoid several complexities, reducing the upfront cost and saving it from the self-maintenance [6, 7].

It can be elaborated in two different aspects. The first aspect is to control the workload remotely. It is processes over the internet [8]. It is possible on the commercial data center. It is also called public clouds [9]. The famous providers for the same are Amazon Web Services (AWS), Salesforce's CRM system, and Microsoft Azure.

In general, the enterprises use the multi-cloud concept today [10]. Means to adopt many public clouds simultaneously.

The second aspect shows the complete working scenario. It shows how it works and the data sharing mechanism [11]. As we have a pool of resources or virtualized pool. It has been available on demand with the capability of computing to the application functionality [12]. The computing supports the automation for the processing which is relay advanced in terms of computing power. It provides the agility advantage. It will work with the capability of computing, storage and other network resources. The application functionality provides the interconnection for the data sharing and efficacy to monitor with the server and user [13, 14].

Now the major threat comes in the mind is the data security and the storage when the data is shared among several workstation remotely. So, the control on the data and the communication aspect is the major concern now days.

*Author for correspondence

The major security threats are data breaches, data loss, inside threats, denial of service attacks, and usage of API which are insecure and advance persistent threats. Data breaches in terms of cloud customer are the major aspect and there is the need of applying different computation applicability for the prevention and detection. The permanent loss of the customer data is another challenge so data cloning for the working procedure or regular data backup mechanism is needed. Then denial of service attacks especially in terms of distributed attack is the major concern which includes the data damage and exposure of customer data. API should be tested before use otherwise it may be the door for the attackers. Then finally the persistent threats which may target the public services of cloud for their attacks.

The service model encompasses the organization and it serves as a framework and provides the ease in resource sharing [14]. The major issues can be classified as the issues by the source means the providers who provides the clouds and the other side is the huge customers. It should be organized in such a way that the security concern should be fulfilling in the two-way direction [15]. It is exceptionally flaw tolerant through excess and conveyance of information [16−20]. *Figure 1and 2* show the cloud computing system and security applicability respectively. It clearly shows the communication and storage aspects.

The interdisciplinary aspects have also been included in terms of big data and internet of things (IoT).

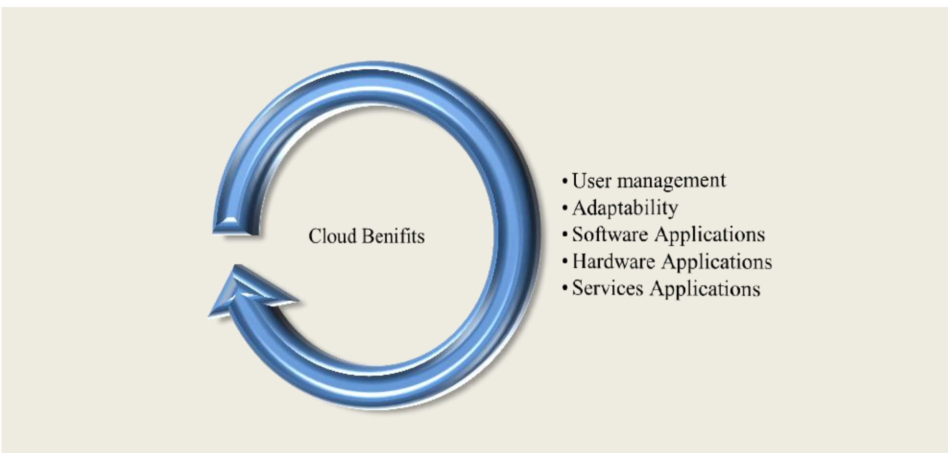

Figure 1 Cloud computing system

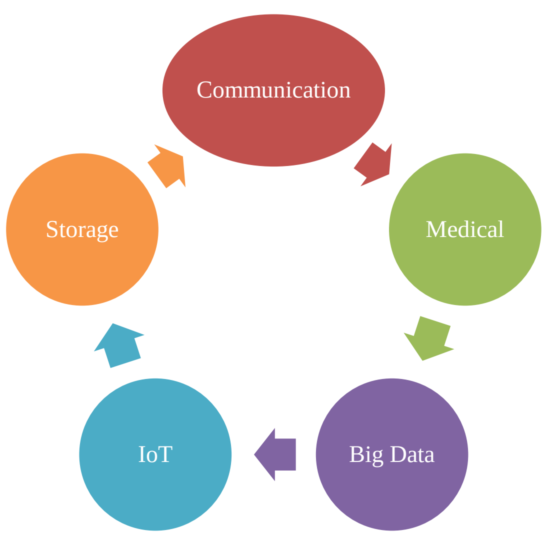

Figure 2 Cloud computing security applicability

The main motivations of this paper are as follows:
1. Analysing the applicability of security mechanism for the prevention of data breaches.
2. Discussing the resource sharing mechanism applicability and computability for the ease of resource distribution.
3. Analysis of the mechanism inside threat identification.
4. Discuss and analysis of hierarchal security applicability and synchronization time processing for achieving high end security in less time.

The objectives of this paper are as follows:
1. To explore the previous literature analytically and computationally for the security prospect and data sharing.
2. To explore empirically for the security prospect and data sharing.
3. To analyse and discuss the mechanism of cloud computing in terms of different domains for the same security aspect.

2.Related work

In 2020 Ismail and Islam [21] developed a security transparency and audit tool. It has the capability of automatic assessment and collection. They validated the tool through the real world cases. Their complete approach is also beneficial for the cloud computing security.

In 2020, Ahamad et al. [22] discussed about data violation, unprotected sensitive data and the public access in terms of cloud computing. They have discussed regarding the privacy preservation challenges in the cloud. For the challenges they have developed a privacy preservation model in the cloud environment. It has been developed by using the advancements of artificial intelligent techniques. They have combined Shark Smell Optimization and Jaya Algorithm (JA) and formed as Jaya-based Shark Smell Optimization (J-SSO). Their model found to be efficient in enhancing cloud security.

In 2020, Prasath et al. [23] discussed about the web application based cloud administration experiences. They have discussed regarding the loss of data along with the security aspects. They have shown the applicability of elliptical curve cryptography in the web application based cloud administration. Their applied strategies are found to be efficient in terms of encryption time, decoding time, and computational expense.

In 2020, Prajapati and Shah [24] discussed regarding the efficient data storage and cloud service providers. They have used convergent encryption and proof of ownership (PoW) for the data protection and integrity. They have also discussed several other security approaches.

In 2020, Kelf [25] discussed about the security concern in cloud migration. They have discussed the aspects of tremendous upsides in terms of traditional methods. The main basis of this study is to explore the risk arises during the migration process.

In 2020, Fan et al. [26] discussed cloud computing environment in terms of data security and IoT. They have also discussed complex deployment process and usage environment of the IoT in terms of security risk. They suggested blockchain technology for the data security of in terms of cloud to data consumer's performance.

In 2020, Mondal et al. [27] discussed about the cloud computing as the latest developments in the IT industry. The major advantages suggested were throughput, scalability and easy access. They have reviewed different security and privacy issues. They have mainly discussed the trust, authenticity, confidentiality, encryption, key management, multitenancy, data splitting and virtual machine security.

In 2020, Mohiuddin and Almogren [28] discussed IoT and its adaptation in terms of cloud computing. They have analyses and performed a study in the direction of investigation of safe transition in cloud computing environment to facilitate safe transition. It has been discussed and analyzed in terms of IoT in cloud application.

In 2020, Saran et al. [29] discussed the latest trends in cloud computing. It was discussed in terms of medical field. They covered the storage aspects, computation and cost in the medical domain in terms of cloud computing usage. They have also elaborated the security concern in the same through the network communication and data storage.

3.Problem statements

Based on the related work discussed above the following gap statements have been identified.
1. There is the need of intelligent data grouping with data tracking and handling mechanism.
2. There is the need of secure data transaction and log mapping in the cloud computing environment.
3. There is the need of automation in security identification.

4. Analysis

In case of public cloud, the data should be secured in such a manner that unauthorized access should be prevented [17]. There should be some prevention mechanism so that it can be prevented on time. There should be some precaution mechanism in case of any malicious node as it may result in complete cloud processing risky and attack prone. There should be some mechanism for the prevention of the failure situation where the data can be backup and it can be used at the time of the need [18−20]. In this section result based analysis was presented and discussed in terms of security and interdisciplinary collaboration with cloud computing. Table 1 shows the result analysis.

Table 1 Result analysis

S.No	Authors	Approach	Findings
1	[30]	Cloud-edge based data security architecture	Their cloud-edge infrastructure is helpful in the confidential data sharing.
2	[31]	Security strategy for virtual machine allocation	The result finding of this paper are as follows: 1.Their allocation strategy is efficient in VM co-resident attack. 2.It is cabaple in the reduction of energy consumption.
3	[32]	DNA based data security	The finding of this paper are as follows: 1.1024-bit secret key is generated based on DNA computing. 2.Secret key was generated based on media access control, decimal encoding rule, American Standard Code for Information Interchange (ASCII) value.
4	[33]	Implementing Hy-IDS	The finding of this paper are as follows: 1.Access security implementation. 2.Ease of resources management using mobile agents. 3.Reliable structure with lower cost.
5	[34]	Periodical key change for cloud mutable security protocol	The finding of this paper are as follows: 1.Access security implementation. 2.Ease of resources management using mobile agents. 3.Reliable structure with lower cost.

5. Conclusion

This paper provides a study and analysis of security aspects in the cloud computing environment. It provides a proper collaboration of different interdisciplinary aspects like big data and IoT. It shows a systematic analysis of data security in terms of cloud data, data storage, communication and data integrity. It also covers the aspects with big data and IoT based on security and confidentiality. In future a collaborative framework can be designed with security framework for the computational improvement.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Kumar R, Bhatia MP. A systematic review of the security in cloud computing: data integrity, confidentiality and availability. In international conference on computing, power and communication technologies 2020 (pp. 334-7). IEEE.

[2] Kumar R, Goyal R. On cloud security requirements, threats, vulnerabilities and countermeasures: a survey. Computer Science Review. 2019; 33:1-48.

[3] Sun PJ. Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications. 2020:102642.

[4] Sasubilli SM, Dubey AK, Kumar A. A computational and analytical approach for cloud computing security with user data management. In international conference on advances in computing and communication engineering 2020 (pp. 1-5). IEEE.

[5] Divya J, Shivagami S. A study of Secure cryptographic based Hardware security module in a cloud environment. In international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) 2020 (pp. 1273-9). IEEE.

[6] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI sixth international conference on software engineering 2012 (pp. 1-8). IEEE.

[7] Zheng X, Martin P, Brohman K, Da Xu L. Cloudqual: A quality model for cloud services. IEEE Transactions on Industrial Informatics. 2014; 10(2):1527-36.

[8] Jagli D, Purohit S, Chandra NS. SaaS CloudQual:a Quality Model for Evaluating Software as a Service on the cloud computing environment. In innovations in computer science and engineering 2017 (pp. 73-80). Springer, Singapore.

[9] Sasubilli SM, Dubey AK, Kumar A. Hybrid security analysis based on intelligent adaptive learning in Big Data. In international conference on advances in computing and communication engineering 2020 (pp. 1-5). IEEE.

[10] Singh A, Chatterjee K. Cloud security issues and challenges: a survey. Journal of Network and Computer Applications. 2017; 79:88-115.

[11] Choi SW, Kim SD. A quality model for evaluating reusability of services in SOA. In conference on e-commerce technology and the fifth IEEE conference on enterprise computing, e-commerce and e-services 2008 (pp. 293-8). IEEE.

[12] Choudhary AR. Baseline requirements and architecture for cloud computing services. International Journal of Advanced Computer Research. 2012; 2(7):1-7.

[13] Luo HY, Lv P, Liu LZ, Yang X. Enterprises trust comprehensive evaluation based on fussy rough AHP in cloud computing. J Shandong Univ (Nat Sci). 2014; 49:111-7.

[14] Alotaibi MB. Antecedents of software-as-a-service (SaaS) adoption: a structural equation model. International Journal of Advanced Computer Research. 2016; 6(25):114-29.

[15] Bhupendra Kumar, Jayshree Boaddh. A meta-analysis on secure cloud computing. International Journal of Advanced Technology and Engineering Exploration. 2016; 3(15): 15-20.

[16] Zisman A, Spanoudakis G, Dooley J. A framework for dynamic service discovery. In 2008 23rd IEEE/ACM International conference on automated software engineering 2008 (pp. 158-67). IEEE.

[17] Soni A, Hasan M. Pricing schemes in cloud computing: a review. International Journal of Advanced Computer Research. 2017; 7(29):60-70.

[18] https://www.globaldots.com/cloud-computing-types-of-cloud/. Accessed 26 October 2020.

[19] Shrimali B, Bhadka H, Patel H. A fuzzy-based approach to evaluate multi-objective optimization for resource allocation in cloud. International Journal of Advanced Technology and Engineering Exploration. 2018; 5(43):140-50.

[20] Kalangi RR, Rao MC. A novel multi-user fingerprint minutiae based encryption and integrity verification for cloud data. International Journal of Advanced Computer Research. 2018; 8(37):161-70.

[21] Ismail UM, Islam S. A unified framework for cloud security transparency and audit. Journal of Information Security and Applications. 2020; 54:102594.

[22] Ahamad D, Hameed SA, Akhtar M. A multi-objective privacy preservation model for cloud security using hybrid Jaya-based shark smell optimization. Journal of King Saud University-Computer and Information Sciences. 2020.

[23] Prasath R, Santhosh GT, Ratchnayaraj IA, Jemiline E. The security in web application of cloud and IoT service. Materials Today: Proceedings. 2020.

[24] Prajapati P, Shah P. Review on secure data deduplication: cloud storage security issue. Journal of King Saud University-Computer and Information Sciences. 2020.

[25] Kelf S. The security risks created by cloud migration and how to overcome them. Network Security. 2020; 2020(4):14-6.

[26] Fan Y, Zhao G, Shang W, Shang J, Lin W, Wang Z. A preliminary design for authenticity of IoT Big data in cloud computing. In international conference on computer communications and networks 2020 (pp. 1-2). IEEE.

[27] Mondal A, Paul S, Goswami RT, Nath S. Cloud computing security issues & challenges: a review. In international conference on computer communication and informatics 2020 (pp. 1-5). IEEE.

[28] Mohiuddin I, Almogren A. Security challenges and strategies for the IoT in cloud computing. In international conference on information and communication systems 2020 (pp. 367-72). IEEE.

[29] Saran P, Rajesh D, Pamnani H, Kumar S, Sai TH, Shridevi S. A survey on health care facilities by cloud computing. In international conference on emerging trends in information technology and engineering 2020 (pp. 1-5). IEEE.

[30] Chadwick DW, Fan W, Costantino G, De Lemos R, Di Cerbo F, Herwono I, et al. A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future Generation Computer Systems. 2020; 102:710-22.

[31] Jia H, Liu X, Di X, Qi H, Cong L, Li J, Yang H. Security strategy for virtual machine allocation in cloud computing. Procedia Computer Science. 2019; 147:140-4.

[32] Namasudra S, Devi D, Kadry S, Sundarasekar R, Shanthini A. Towards DNA based data security in the cloud computing environment. Computer Communications. 2020; 151:539-47.

[33] Toumi H, Fagroud FZ, Zakouni A, Talea M. Implementing Hy-IDS, mobiles agents and virtual firewall to enhance the security in IaaS Cloud. Procedia Computer Science. 2019; 160:819-24.

[34] Kayed A, Omar S. Periodical key change for cloud mutable security protocol. Microprocessors and Microsystems. 2019; 69:152-8.

Mr. Makrand Samvatsar is currently working as Assistant Professor in the School of Computer Science and Information Technology at Symbiosis University of Applied Sciences, Indore. He is Pursuing Ph.D. from Devi Ahilya VishwaVidhyalaya Indore. He has done M.Tech (CS) from DAVV, Indore. His area of interest are as follows:-Critically review the different solutions available for cloud computing and study the different virtualization solutions for both Open-Source and commercial vendors that can be used with cloud computing. Design will be to be able to measure the performances of both public and private cloud and also to be able to test the performance of a private cloud. Implementing the different scenario to be able to evaluate the performances of public and private cloud as well as the implementation of the private cloud. In addition to this he has Successfully organized many Conferences, Seminar, workshops and guided M. Tech thesis for more than 10 students.
Email: makrand111@gmail.com

Dr Priyesh Kanungo has got vast knowledge of research in the field of computer science and engineering his key interest area are Distributed Computing, Cloud Computing, Artificial Intelligence, Operating systems in Ph D Coursework (at SCSIT, IET, IMS, SoC, School of Data Analytics) M Tech, MCA, MSc, MBA, BE etc. He has done Ph.D.(Computer Engineering), B.E., M.E.(Comp. Engg.), M.Phil.(Comp.Sc.) from DAVV and SGSITS respectively. He has received M.K.Kulkarni Award in Higher Secondary, II Position in B.E from SGSITS., National merit Scholarship, GATE Scholarship for M.E. Currently he is working as a Professor & Sr. System Engineer in DAVV (SCS), Indore. In addition to this he is also the Member of DAVV college Inspection Committee, UGC Expert.