Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 285-290, 2016
ISSN 1990-9233;

DOI: 10.5829/idosi.mejsr.2016.24.TAET23539

Information Security Issues and Challenges in Cloud Computing

[1]S. Ramasamy, [2]R.K. Gnanamurthy and [3]R. Thilagavathi

[1]Assistant Professor, Department of Computer Science and Engineering,
VCEW, Namakkal, TN, India
[2]Professor, Department of Computer Science and Engineering, SKP, Tiruvannamalai, TN, India
[3]PG Scholar, Department of Computer Science and Engineering, VCEW, Namakkal, TN, India

Abstract: Cloud computing is a rapidly increasing emerging technology in IT services. The cloud computing offers various services as required for the cloud users such as software, platform and infrastructure. The cloud service provider offers a wide range of storage for their cloud users. The cloud users may store and retrieve the information from their registered cloud servers, while storing and retrieving the information from the servers may cause information leakage. So providing information security in cloud computing is a major anxiety to the remote server over the web. To be addressed first security issues before implementation cloud computing in an organization. In this paper, we emphasize information interrelated security issues in cloud based domain and challenges to overcome.

Key words: Cloud computing · Information security · Data access · Issues · Challenges

INTRODUCTION

Cloud computing is the next generation of web based computing system which provides trouble-free and adapt services to the users for accessing with various cloud applications. Cloud computing provides a way to store and access cloud information from wherever by connecting the cloud application using web. The survey of information correlated security challenges in cloud based environs and solutions to overcome are highlighted [1]. In remote information server, the users are able to store their local information by choosing the cloud services [2].The cloud service providers provide the cloud services to access stored information in remote information centre. Hence the information stored in remote information centre for information processing should be done with most extreme care.

Cloud computing security is the most important anxiety to be addressed at the present time. The information is at high risk when the security measures are not provided accurately for information operations and transmission [3]. As cloud computing provides a capability for a group of users to access the stored information there is prospect of having high information risk. By implementing strongest security measures to identify security issues and challenges to manage these issues.

Literature Survey: Several of the proposed techniques has been conversed in the literature survey for managing security issues and challenges in cloud computing. Popovi and Hocenski, conversed about the security issues, requirements and challenges that are appearance by cloud service providers for the period of cloud engineering [4]. Behl surveys the security issues correlated to the cloud domain. He besides conversed regarding existing security approaches to protect the cloud transportation and applications and their limitations [5]. Sabahi conversed regarding security issues, reliability and availability for cloud computing technology. He besides proposed a sufficient solution for a small amount of security issues [6].

E.M. Mohamed *et al.,* presented the information security representation of cloud computing based on the learning of cloud structural design. They besides realized software to improve the effort in information security representation for cloud computing [7]. Wentao Liu initiated a various cloud computing systems and

Corresponding Author: S. Ramasamy, Assistant Professor, Department of Computer Science and Engineering, VCEW, Namakkal, TN, India.

investigates cloud computing security issues and its policies according to the cloud computing notion [8]. Mathisen, E conversed regarding several of the key security issues that cloud computing are bounce to be tackled with, in addition to present achievements that offer a resolutions to these susceptibility [9]. Farrukh Shahzad survey several researches works on cloud computing related to privacy issues and security challenges [10]. Selvamani k, Jayanthi s surveyed to point out several techniques to solve the security issues and privacy of the information in public auditing scheme cloud domain [11].

Services in Cloud Computing: Cloud computing can be accessed through a set of cloud computing services such as SaaS, PaaS, IaaS. Software as a Service (SaaS) as the ability for a user to use the provider's consequence operating on a cloud transportation. The relevance's are available from a variety of client devices through a thin client interface like an internet browser (e.g., internet-based email). The user does not handle the underlying cloud transportation. These applications can be accessed via internet browser. Providers are more responsible for the protection and confidentiality of application services, more so in public than private clouds anywhere the client association might have strict protection necessities and offer the desirable enforcement services.

Platform as a Service (PaaS) offers the cloud user with the ability to organize the applications using programming languages into the cloud platform and tools that are sustained by the cloud provider. The cloud user does not handle the underlying cloud transportation. The service delivery model permits the customer to charge virtualized servers and associated services for executing existing applications and developing new ones. Though, the cloud user can manage the deployed applications and probably the application hosting atmosphere configurations.

Infrastructure as a Service (IaaS) gives the cloud user the most control of the three types of clouds. It is mainly extensible liberation model and offers only some, but one, application-like features. It's expected that the clients protect the operating systems, applications and substance. Though the cloud user has managed in excess of the operating system, storage and deployed applications, the cloud provider is tranquil dependable for the control of the fundamental cloud transportation. However businesses by means of the IaaS cloud service representation are usually dependable for protecting their individual virtual machines and the applications and information that live on them.

Information Security Issues in Cloud Computing: Since we are stirring into web based cloud model, it requires enormous importance on information security and privacy. Information failure or information outflow can have rigorous collision on big business, variety and hope of an association.

Threats: There is a threat of information exploitation when several associations distribute resources. Hence, to avoid threats it is obligatory to protect the information repositories and besides the information that rivet storage space development. Security of information is the major significant challenges in cloud computing. To improve the security in cloud computing it is significant to grant authentication, authorization, access control for information stored in cloud computing.

Locality: In cloud computing the information is share out more than the number of areas and to determine the location of information is complicated. While the information is simulated to various geographic sites the rules governing on the information as well as change. Hence, In cloud computing there is an issue of compliance and information protection laws, client must be familiar with their information sites and it is to be informed by the service provider.

Integrity: The system must preserve security such that information is able to customize only by the authorized personality. Information integrity should be maintained properly to avoid the information failure in cloud based domain. In common each transactions in cloud computing should trail ACID properties to preserver information integrity. The majority of the internet services using HTTP services to face group of issues with the transaction organization regularly. HTTP service does not sustain transaction or assurance deliverance. It can be handled by executing transaction organization in the API itself.

Access: Information access mostly refers to the information security strategy. In an association, the client will be given access to the part of information based on their company security strategy. In the same association, the other worker cannot be accessed by the same

information. Different encryption techniques and key management mechanisms are used to guarantee that information are distributed merely with the exact client. The key is shared merely to the authorized personality using a variety of key distribution mechanisms. The information security strategy should be severely followed to protect the information from the unauthorized person. As access is prearranged through the web for all cloud clients, it is required to give restricted client access. Customers can use information encryption and fortification mechanisms to avoid the security threats.

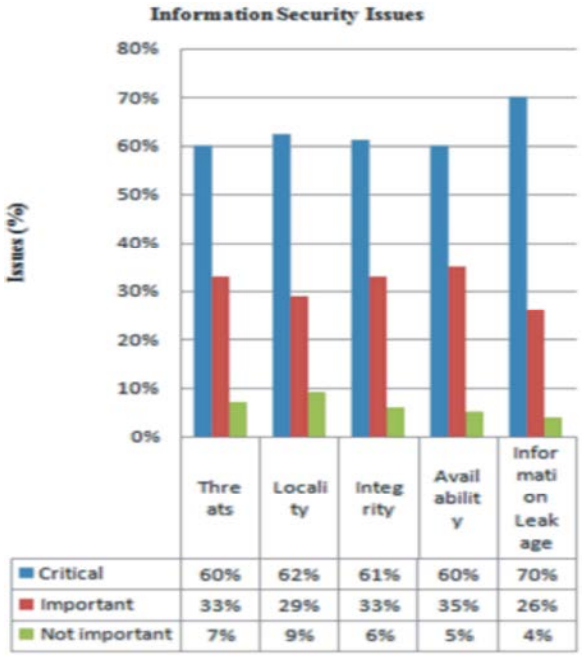

Fig. 1: Cloud Security Issues

Availability: Since the cloud provider has growing responsibility for revolutionize organization contained by all cloud deliverance models, there is a risk that modify could establish unenthusiastic possessions. These could be reigned by software or hardware modified to obtainable cloud services.

Breaches: Information breaches are one more significant security issue to be deliberated in cloud. Because large information from a range of clients consumes are stored in the cloud, there is a chance of malicious client penetrate the cloud such that the whole cloud domain is level to a high importance attack. The information breach at aim, resulting in the failure of individual and credit card information of up to 110 million persons, was single of a sequence of unexpected thefts that took place during the usual processing and storage of information.

Information Management at Respite: Businesses should ask particular issues to verify the cloud service provider's (CSP's) information storage life cycle and security strategy.

Businesses should find out if:

- Multitenant storage is being used and if it is, find out what partition mechanism is being used between tenants.
- Mechanisms such as tagging are utilized to avoid information being simulated to particular country or provinces.
- Storage used for archive and backup is encrypted and if the key management policies consist of a strong personality and access management strategy to control access within sure authorities.

Information Leakage: A threat from prevalent information leakage between many, potentially participator associations, via the identical cloud provider could be caused by human being mistake or faulty hardware that will escort to information cooperation.

Long-Term Viability: Request eventual providers how you would get your information back if they were to fail or be obtained and find out if the information would be in a layout that you could without issues import into a substitution application.

Information Security Challenges in Cloud Computing: Cloud computing environs are multi-domain environs in which each area can utilize different security, privacy and hope necessities and po-tentially use various mechanisms, edges and semantics. In conventional information centres, IT administrators locate actions and controls in set to construct a toughened boundary about the transportation and information they need to protect. This pattern is moderately trouble-free to handle, because associations contain control of their servers' site and make use of the physical hardware completely for themselves.

Information Isolation and Security: One of the most important characteristics of cloud computing is multi-tenancy. As multi-tenancy permit to store information by several clients on cloud servers there is a chance of information interruption. Through injecting a user code or functions, information can be interrupted. Hence there is obligation to store information individually from residual clients can consumer's information. Exposure with information separation can be discover or

identify using the investigations such as SQL injection AWS, information validation and insecure storage. Cloud computing consumers distribute physical assets with others during general software virtualization levels.

Information Failure Avoidance: Information failure avoidance is a approach for creating confident that end consumers do not send perceptive or important information remote the commercial network. The term is besides used to explain software products that facilitate a network manager control what information end consumers can transmit. Information failure avoidance software products utilize business regulations to categorize and protect secret and vital information so that unauthorized end consumers cannot inadvertently or maliciously distribute information whose exposé could put the association at threat. For example, if a worker aimed to promote a big business email remote the commercial environment or upload a commercial file to a consumer cloud storage service similar to Drop box, the worker would be deprived of consent. Implementation of information failure avoidance is being motivated by insider risk and by extra accurate state privacy rules, a lot of which have inflexible information protection or access apparatus.

Information Mobility and Control: Stirring information starting stagnant physical servers onto virtual dimensions constructs it extraordinarily cellular phone and information stored in the cloud be able to live wherever in the virtual globe. Storage space managers can simply convey or reproduce users' information diagonally information centres to help server maintenance, HA/DR or capability preparation, with tiny or no service disruption or detect to information proprietors. This makes a amount of official difficulties for cloud consumers. Suspicious controls must be useful to information in cloud computing environs to make sure cloud contributors do not accidentally break these regulations by roaming geographically responsive information diagonally political margins.

Authentication and Identity Management: By using cloud services, consumers can simply access their private information and create it obtainable to a variety of services across the web. An identity management (IDM) mechanism can facilitate authenticate consumers and services based on recommendations and characteristics. A key issue regarding IDM in clouds is interoperability problems that could outcome from using different identity indications and identity cooperation protocols. Existing password-based certifications has an inher-ited restriction and create important threats. An IDM system must be able to secure private and tactful information connected to clients and processes.

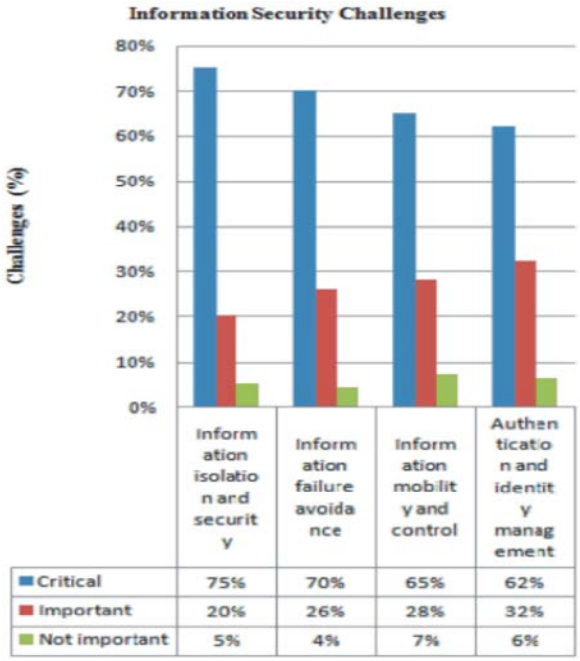

Fig. 2: Cloud Security Challenges

Secure-Service Management: In cloud computing environs, cloud service providers and service integrators make services for their consumers. The service integrator offers a raised area that permits self-sufficient service providers orchestrate and interwork services and kindly provide extra services that meet consumers' protection necessities. While several cloud service providers utilize the Web Services Description Language (WSDL), the conventional WSDL can't entirely meet up the necessities of cloud computing services explanation. In clouds, issues for instance eminence of service, cost and SLAs are serious in service explore and composition. These issues must be tackled to depict services and begin their features, discover the greatest interoperable choices, combine them not including violating the service proprietor's strategies and make sure that SLAs are satisfied. In concentrate, an involuntary and systematic service provisioning and composition structure that considers security and privacy issues is essential.

CONCLUSION

Cloud computing is a most emerging IT trend. It offers more benefits to the users. Cloud computing faces number of security issues and challenges. To provide security in cloud computing we can use various advanced encryption techniques for encrypting the information before it stored, to avoid this security issues and challenges. In addition we can also use proper key management techniques to distribute the key to cloud users such that only dispensation persons can access the information.

ACKNOWLEDGEMENTS

I owe my deep gratitude to my respected guide Prof. Dr. R.K. GNANAMURTHY who gives me the valuable guidelines with a touch of inspiration and motivation to progress my way through quite substantial barrier between early problem statement and something that resembled a fine work.

REFERENCES

1. Velumadhava Rao, R. and K. Selvamani, Data 2015. security Challenges and Its Solutions in Cloud computing, in: Procedia Computer Science, 48: 204-209.
2. Mollah, M.B., K.R. Islam and S.S. Islam, 2012. Next generation of computing through cloud computing technology, 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012. pp: 1-6.
3. Shucheng Yu, Cong Wang, Kui Ren and Wenjing Lou, 2010. Achieving secure, scalable and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010, pp: 1-9.
4. Kresimir Popovic and Zeljko Hocenski, 2010. Cloud computing security issues and challenges, in: MIPRO, 2010 Proceedings of the 33rd International Convention, pp: 344-349.
5. Akhil Bhel, 2011. Emerging Security Challenges in Cloud Computing. Information and Communication Technologies, in: 2011 World Congress on, Mumbai, pp: 217-222.
6. Farzad Sabahi, 2011. Cloud Computing Security Threats and Responses, in: IEEE 3rd International Conference on Communication software and Networks (ICCSN), May 2011. pp: 245-249.
7. Eman M. Mohamed, Hatem S. Abdelkader and Sherif EI Etriby, 2012. Enhanced Data Security Model for Cloud Computing, in: 8th International Conference on Informatics and Systems (INFOS), Cairo, May 2012. pp: 12-17.
8. Wentao Liu, 2012. Research on Cloud Computing Security Problem and Strategy, in: 2nd International Conference on Consumer Electronics. Communications and Networks (CECNet), April 2012. pp: 1216-1219.
9. Eystein Mathisen, 2011. Security Challenges and Solutions in Cloud Computing, in: International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 2011. pp: 208-212.
10. Farrukh Shahzad, 2014. State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions, in: Procedia Computer Science, 37: 357-362.
11. Selvamani, K. and S. Jayanthi, 2015. A Review on Cloud Data Security and its Mitigation Techniques, in: Procedia Computer Science, 48: 347-352.
12. Gnanamurthy, R.K and L. Malathi, 2012. "A novel routing protocol with lifetime maximizing clustering algorithm for WSN India Conference (INDICON), 2012 Annual IEEE925-930, December 2012.
13. Gnanamurthy, R.K., V. Babyvennila and B. Bshuvaneswari, 2012. "Wireless sensor network for forest fire sensing and detection in tamilnadu", Engineering Science and Technology: An International Journal (ESTIJ), 2(2): 306-309, April 2012.
14. Arulkumaran, G. and R.K. Gnanamurthy, 2014. "Improving Reliability against Security Attacks by Identifying Reliance Node in MANET", Journal of Advances in Computer Networks, 2(2): 96-99, June 2014.
15. Gnanamurthy, R.K K Sankaranarayanan, "Secured Group Communication Protocol INDICON, 2005 Annual IEEE 267-271, December 2005.
16. RK. Gnanamurthy, L. Malathi, "Cluster Based Hierarchical Routing Protocol for WSN with Energy Efficiency", International Journal of Machine Learning and Computing, Volume 4, Issue 5, Pages 474, October 2014.
17. Gnanamurthy, R.K., L. Malathi and M.K. Chandrasekaran, 2013. "A novel cluster-chain based routing protocol to prolong the lifetime of WSN", International Journal of Computer Applications, 61(22): 43-47, January 2013.

18. Gnanamurthy, R.K. and L. Malathi, 2015. "Hybrid Node Deployment Algorithm to Mitigate the Coverage Whole Problem in Wireless Sensor Network", Middle-East Journal of Scientific Research, 23(10): 2500-2506.
19. Gnanamurthy, R.K., 2014. "Design and implementation of quality of service and security in group Communication over mobile Adhoc networks".
20. R.K. Gnanamurthy, L. Malathi and M.K. Chandrasekaran, 2015. "Energy efficient data collection through hybrid unequal clustering for wireless sensor networks", Computers and Electrical Engineering, 48: 358-370, November 2015.