JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REVIEW ON DATA SECURITY IN CLOUD COMPUTING

Rashmi Dagde (Assistant Professor) Computer Science And Engineering Priyadarshini Bhagwati College Of Engineering Nagpur, India	Sanskruti Tiwari (Research Scholar) Computer Science And Engineering Priyadarshini Bhagwati College Of Engineering Nagpur, India	Rugveda Dhok (Research Scholar) Computer Science And Engineering Priyadarshini Bhagwati College Of Engineering Nagpur, India
Janhavi Choudhari (Research Scholar) Computer Science And Engineering Priyadarshini Bhagwati College Of Engineering Nagpur, India	Nikita Sonkusare (Research Scholar) Computer Science And Engineering Priyadarshini Bhagwati College Of Engineering Nagpur, India	Chanchal Mate (Research Scholar) Computer Science And Engineering Priyadarshini Bhagwati College Of Engineering Nagpur, India

Abstract : Human life nowadays has reached a stage where the internet has become an indivisible part of our life. New technologies are taking place of old technologies on a large scale, bringing great profits to mankind. On the other hand these same technologies being the data storehouses leading to multiple data security vulnerabilities.

In this study, an overview of the concept of data security in cloud computing has been presented. Availability of data in the cloud is beneficial for applications leads to reliable outcomes of the operation performed over them but ion the other hand it also poses risks by exposing data to applications which might already have security loopholes in them. This document is firstly providing the basic introduction to the concept of data security in cloud computing.

The causes of data security vulnerabilities in an organization and the challenging factors of protecting an organization from data phishing are discussed in brief. Then a few common data-phishing acts and the ways to protect from them are specified. The paper will also provide an overview on data security aspects for Data-in-Transit and Data-at-Rest.

I. INTRODUCTION

In the modern digital era, the significance of ensuring robust data security is widely recognized. This research paper is dedicated to exploring and enhancing data security within the realm of cloud computing. Cloud computing has gained immense prominence as a revolutionary technological advancement, making it imperative to address data security comprehensively.

Presently, cloud computing stands as a paramount computing service, transforming the technological landscape. In this context, safeguarding data assumes a pivotal role. This paper meticulously delves into five crucial facets of data security inherent to cloud computing: the establishment of a secure architecture, meticulous enforcement of compliance, vigilant practice of due diligence, continuous network monitoring, and the integration of a robust authentication protocol. Centralizing data security is a key tenet of cloud computing, consolidating various security functions into a cohesive framework.

The methodology expounded within this research paper delineates a comprehensive approach to fortify data security within cloud computing. This methodological framework serves as a bulwark against potential threats posed by hackers, online scams, and cyber attacks. Through exhaustive examination, we have explored a myriad of data security techniques inherent to cloud computing, thereby devising effective strategies to safeguard valuable information.

As we delve deeper into the realm of cloud computing, the importance of data security becomes even more pronounced. This paper embarks on a journey to uncover innovative methodologies and techniques that contribute to the preservation of data integrity, thereby fostering a secure cloud computing environment.

II. METHODOLOGY

Cloud computing comes with its fair share of risks and security concerns that require careful attention. This exploration focuses on three key areas: virtualization, public cloud storage, and multitenancy, all of which relate to safeguarding data in cloud computing

A. Virtualization-

Virtualization is like a trick where one operating system is wrapped up within another. It's like using the resources of a computer inside another computer. To make this work, there's a special tool called a hypervisor that helps different operating systems work together. But, there are some risks with this. The hypervisor can become a target for attacks. If it's compromised, the entire system,along with the data, could be in danger. Another issue is with managing resources. If data from one operation is not properly cleared before another one starts, private info might end up where it shouldn't. To handle these risks, careful planning and strong security measures are needed.

B. Storing Data in Public Cloud-

When you put your data in a public cloud, there's a risk that bad actors might try to get at it. Public clouds have big storage systems that can attract unwanted attention. To avoid this, for really important stuff, it's better to use a private cloud that you control.

C. Multitenancy

Sharing resources in cloud computing, called multitenancy, has its own risks. Imagine different people using the same computer parts at the same time. Sometimes,data from one user could accidentally end up with another user. It's like a mix-up.This is a problem because private info might end up where it's not supposed to be. To fix this, strong user checks and safeguards are needed.

ENSURING DATA SECURITY IN CLOUD COMPUTING

Securing data within the realm of cloud computing encompasses far more than the simple act of encryption. The vital requisites for data security diverge based on the trio of service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Within this landscape, two pivotal data states emerge, each vulnerable to potential threats: Data at Rest, representing data nestled within the cloud's confines, and Data in Transit, signifying the continuous movement of data in and out of the cloud ecosystem. The foundational principles of confidentiality and data integrity are intricately woven into the fabric of data protection mechanisms, procedural measures, and systematic processes. Singularly significant is the question of how data exposure manifests within these two critical states.

A. Safeguarding Data at Rest

Data at rest refers to the data resting inside the cloud, including both active information and important backups. Protecting this data can be tough in some cases, especially if you don't have your own private cloud with physical control. However, creating a private cloud setup can effectively solve this challenge. It involves carefully arranging a system that allows controlled access and strong security measures.

B. Protecting Data in Transit

The flux of data in transit alludes to the ceaseless journey of data to and from the cloud. This flux may take the form of files or databases securely stored within the cloud's repository, subsequently sought and accessed from diverse locales. As data is ushered into the cloud's embrace, it enters the realm of data in transit. The spectrum of this data encompasses highly sensitive elements like user

credentials, which, on occasion, are shrouded in encryption for added protection. Yet, it is essential to recognize that data can also traverse in an unencrypted state .

Vulnerable by its very nature, data in transit faces heightened risks in comparison to its dormant counterpart, data at rest. The transitional voyage exposes data to lurking threats, where intermediary software may clandestinely eavesdrop on the discourse or even manipulate the data's trajectory en route to its intended haven. Encryption emerges as a vanguard strategy, fortifying data in transit and forming an impregnable shield against potential breaches.

In summation, the quest to ensure data security in the domain of cloud computing navigates through a nuanced terrain, far beyond the realm of encryption. Our exploration sheds light on the divergent requisites for data protection across various service models, contemplates the intricacies of data at rest and in transit, and underscores the paramount role of encryption as a steadfast guardian of data integrity.

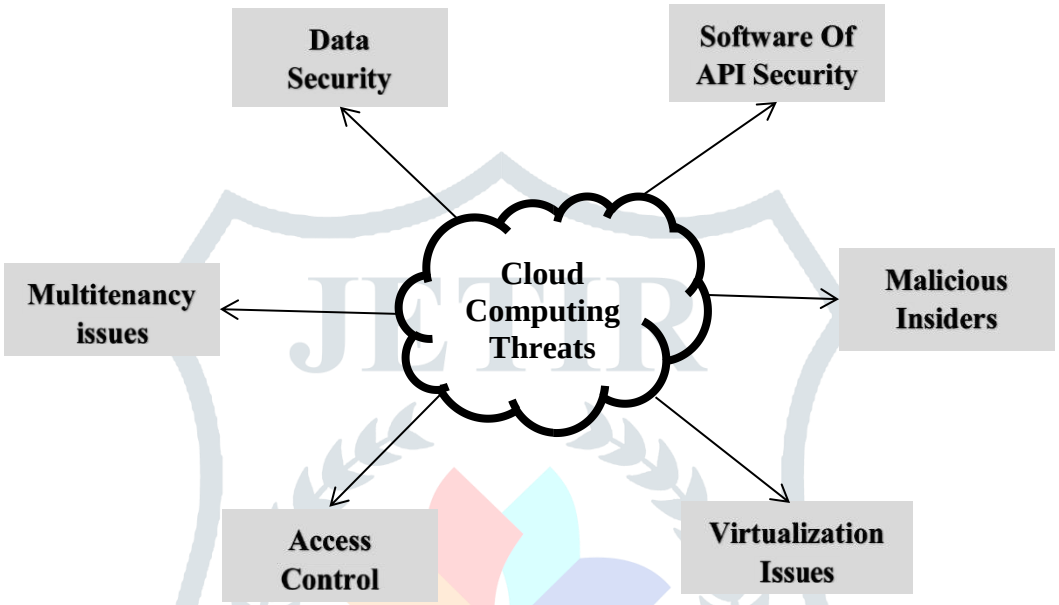

Fig 2.1: Data Security Threats

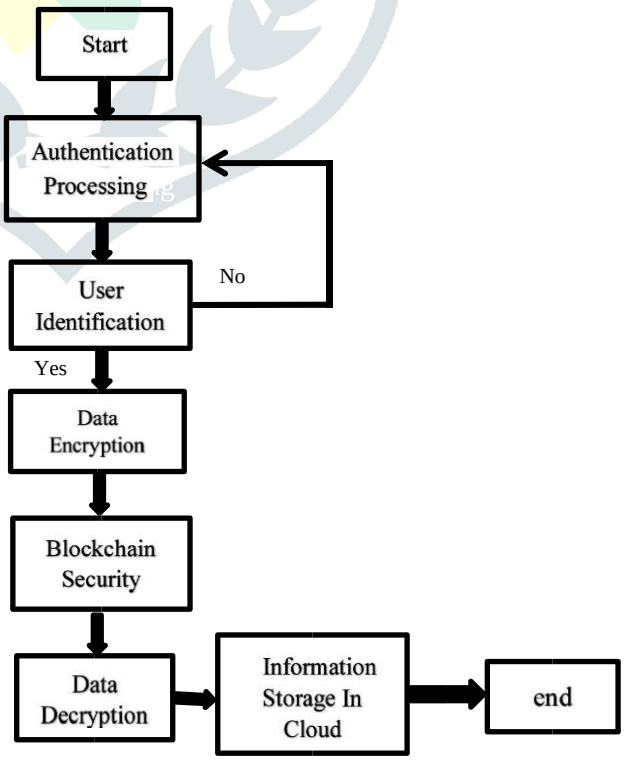

Fig 2.2 : Flowchart Of Data Security

III. LITERATURE SURVEY

To acquire a foundational grasp of cloud computing and the secure storage of data within cloud environments, an extensive array of resources has been consulted. This literature review serves as the cornerstone for discussing diverse facets of data security.

[1] Abdelkader and Etriby introduce a data security model for cloud computing that is intricately woven into the cloud architecture. Their contributions extend to the development of supplementary software, enhancing the efficacy of the Data Security model for cloud computing.

[2] Hu and A. Klein present a standardized approach to secure data-in-transit within the cloud. Their discourse encompasses a benchmark for encryption, a critical shield during data migration. While bolstering security requires additional encryption, it comes at the cost of heightened computation. The benchmark proposed by their study strikes a delicate equilibrium between security and encryption overhead.

[3] Haralambos Mouratidis presents a security framework for the meticulous selection of a cloud provider, grounded in pertinent security prerequisites. This framework relies on a modeling language and leverages the Open Models Initiative (OMI) Platform, with an underlying foundation in the principles of security and privacy.

[4] L. Malina contributes a security model for the cloud, harnessing group signatures to ensure authentication and user privacy. This innovative paradigm simultaneously guarantees the confidentiality and integrity of transmitted data.

[5] Sultan Aldossary delves into the intricacies of cloud data storage, addressing issues such as virtualization, data integrity, availability, and confidentiality. Their survey extends beyond these data security concerns to encompass a comprehensive inventory of potential threats within the realm of cloud computing.

[6] Ulrich Greveler et al [18] architect a revolutionary cloud database structure that effectively counters unauthorized access to uploaded data, spanning both internal and external administrators. This architecture ingeniously employs the XACML structure for articulating the access control policy, further fortifying the database's contents through the use of an Encryption Proxy.

[7] Entao Luo introduces a novel hierarchical multi-authority and CB-ABE based friend discovery system, integrating character attribute subsets to mitigate risks of single point failure and performance bottlenecks. However, it is essential to note that this scheme does not explicitly address the realm of data integrity.

IV. CONCLUSION

In this paper we have described various security concerns with cloud computing .More and More people are using cloud computing to store data pushing the need to make storing data in the cloud better .As cloud computing is becoming more popular in data storage it is prompting efforts to further enhance how data is stored within the cloud .

The paper outlines the causes of data security vulnerabilities within organizations, along with the complexities of guarding against data phishing attempts. Moreover, it delves into common data-phishing behaviors and provides insights into protective measures. Additionally, the document sheds light on data security considerations for both Data-in-Transit and Data-at-Rest scenarios.

In summary, this research underscores the critical importance of data security in cloud computing, offering valuable insights into its multifaceted nature and providing a foundation for robust protective measures. As technology continues to advance, it is imperative that we remain steadfast in our commitment to securing our digital landscape.

REFERENCES

[1] M.Joshi, S. Budhani, N. Tewari and S. Prakash, "Analytical Review of Data Security in Cloud Computing," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2021, pp. 362-366, doi: 10.1109/ICIEM51511.2021.9445355.

[2] A. Albugmi, M. O. Alassafi, R. Walters and G. Wills, "Data security in cloud computing," 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), London, UK, 2016, pp. 55-59, doi: 10.1109/FGCT.2016.7605062.

[3] S. Rajeswari and R. Kalaiselvi, "Survey of data and storage security in cloud computing," 2017 IEEE International Conference on Circuits and Systems (ICCS), Thiruvananthapuram, India, 2017, pp. 76-81, doi: 10.1109/ICCS1.2017.8325966.

[4] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing," 2017

3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall), Dehradun, India, 2017, pp. 1-7, doi:
10.1109/ICACCAF.2017.8344738.

[5] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 2012, pp. 647-651, doi: 10.1109/ICCSEE.2012.193.

[6] U. Somani, K. Lakhani and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), Solan, India, 2010, pp. 211-216, doi: 10.1109/PDGC.2010.5679895.

[7] R. A. Kemmerer, "Cybersecurity," 25th International Conference on Software Engineering, 2003. Proceedings., Portland, OR, USA, 2003, pp. 705-715, doi: 10.1109/ICSE.2003.1201257.

[8] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," in IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 998-1010, Fourth Quarter 2012, doi: 10.1109/SURV.2012.010912.00035.

[9] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016, doi: 10.1109/COMST.2015.2494502.

[10] C. Perera, R. Ranjan, L. Wang, S. U. Khan and A. Y. Zomaya, "Big Data Privacy in the Internet of Things Era," in IT Professional, vol. 17, no. 3, pp. 32-39, May-June 2015, doi: 10.1109/MITP.2015.34.

[11] M. Smith, C. Szongott, B. Henne and G. von Voigt, "Big data privacy issues in public social media," 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), Campione d'Italia, Italy, 2012, pp. 1-6, doi: 10.1109/DEST.2012.6227909.

[12] F. Ullah et al., "Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach," in IEEE Access, vol. 7, pp. 124379-124389, 2019, doi: 10.1109/ACCESS.2019.2937347.

[13] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," in IEEE Transactions on Services Computing, vol. 9, no. 1, pp. 138-151, 1 Jan.-Feb. 2016, doi: 10.1109/TSC.2015.2491281.

[14] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen and X. He, "A Review of Compressive Sensing in Information Security Field," in IEEE Access, vol. 4, pp. 2507-2519, 2016, doi: 10.1109/ACCESS.2016.2569421.

[15] E. M. Mohamed, H. S. Abdelkader and S. El-Etriby, "Enhanced data security model for cloud computing," 2012 8th International Conference on Informatics and Systems (INFOS), Giza, Egypt, 2012, pp. CC-12-CC-17.