Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 4): pp. 3926-3932
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.429

Challenges And Possible Solutions For Data Security In Cloud Environment

Sushil Chandra Dimri, Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India, dimri.sushil2@gmail.com

Adarsh Srivastava, Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India, adarsh.kr701i@gmail.com

Harendra Singh Negi, Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun, India, harendrasinghnegi@gmail.com

Dr. Suruchi Sharma, Associate Professor, School of Management, Graphic Era Hill University, Dehradun.

ABSTRACT:

With technology links to Cloud storage, cloud computing, and cloud services, the cloud computing trend is quickly expanding. Customers are managed by the providers of cloud services, including IBM, Amazon, Google, Microsoft Azure, etc. in developing requests in cloud infrastructure and approaching the ruling class from anywhere. By performing tasks provided by cloud services providers, cloud data are stored and retrieved in a separate area. As the data is sent to the separated worker across a network, ensuring independence is a key concern (internet). Prior to implementing cloud computing in a setup, freedom challenges should be addressed. This study focuses on the security-related problems that arise in a cloud environment and offers remedies for the problems.

Keywords-Cloudcomputing; Data-Security, DataAccess, Encryption.

1.0 INTRODUCTION:

Cloud computing is the type of web-based service that is used in the present and also could be used in the future on a hues scale and that gives consumers easy-to-accomplish tasks that they may personalize. By connecting the cloud requests through the WWW,cloud computing enables a technique to save and access cloud data from an unknown place. Customers arewise to save their local data in a separate document format by choosing cloud services.The data that is stored in the remote data center may be obtained or updatedusing thecloud tools offered by one cloud service provider. As a result, the files kept in a separate data centre for data processing need to be treated carefully.The security of cloud computing is the main issue that is now being discussed. Data transfers and communications are extremely risky if safety measures are not

properly maintained since cloud computing makes it convenient for a number of users to access the stored data, and there is a possibility of facing high data vulnerability. The strongest freedom measures look to be put in to effect by detailing security issues and methods to tackle these issues. See how data security and privacy are the most important and vital factors in determining faults Fig. 1. [1, 2, and 3]

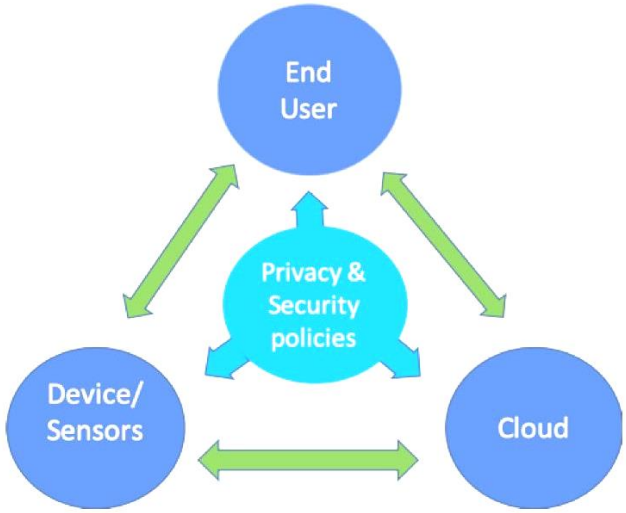

Figure-1.0- Effect of privacy security at different levels inthe cloud computing environment.

2.0 MODELSOFCLOUDCOMPUTING:

To implement cloud computing, a number of cloudcomputing-based models are utilised, including Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).With SaaS, customers and service providers employ these tools to executerequests on a cloud base. Internet browsersmay beused to access these uses. The practice of renting fittings, operating structures, repository space, and network proficiency online is known as PaaS. According to the responsibility transfermodel,the client is allowed to rent virtualized servers and the related tasks, in order to run current request sortoexperimentwithnewones. In IaaS, the services are designed to control processes, deposits, networks, and other essential assessing financial factors that are beneficial tosurvive the autocratic spreadsheet [4, 5, and 6].

3.0 Data protection -Security related Challenges:

As we move into the cloud model based in cyberspace, data security and privacy must be given top priority.Data overflow or short fall can negatively impact an institution's reputation, brand, and commerce. In Fig. 2.0. Data leak preventionis considered to be among the most essential contribution to 88 percent of Major and Very Major issues.Similarly,92 percent of protection challenges are related to data division and

security.[7, 8& 9]

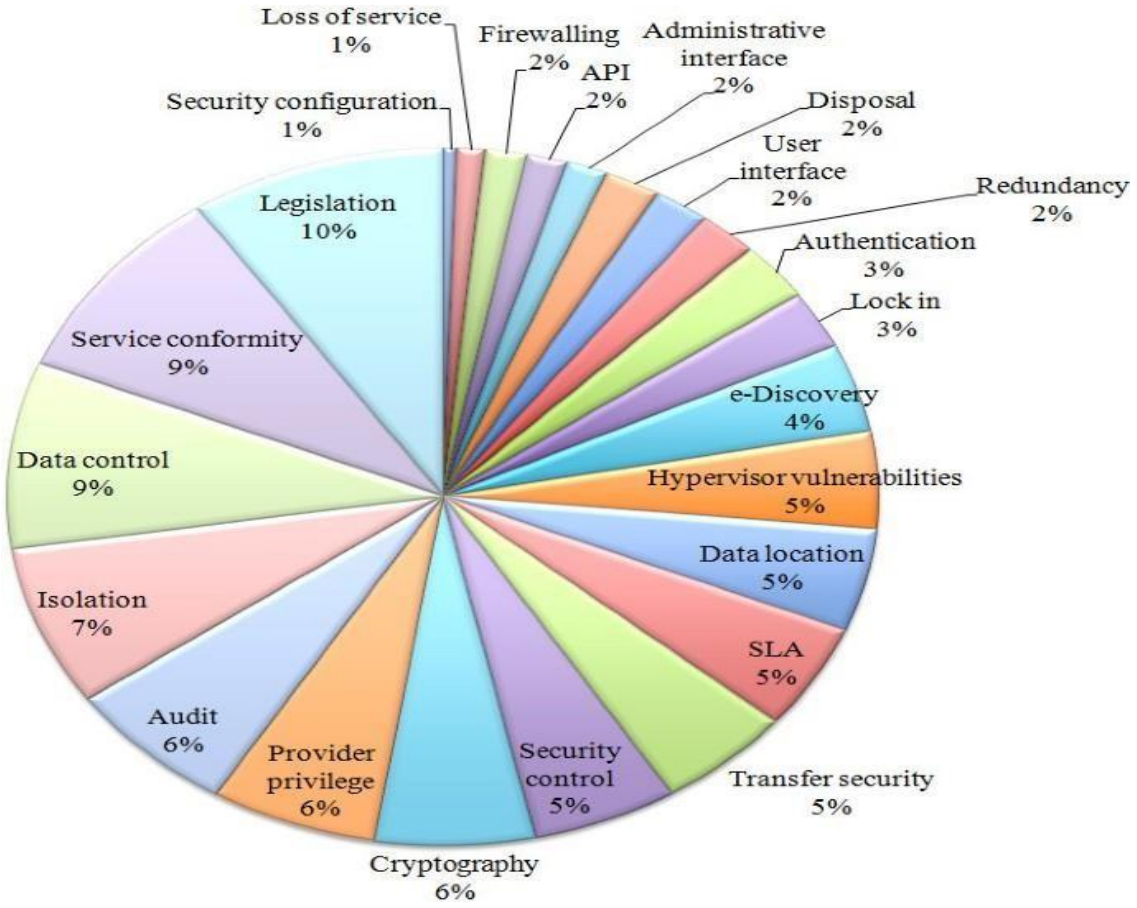

Figure: 2.0 - Pie chart for Security solutions with grouped categories

Security

There may be a chance of data manipulation when different organizations share financial informtions or resources. Therefore, in order to provide protection, it is required to protect document storage facilitiesas well as documents that includestorage, transport,or processing.The major challenges in cloud computing are related to data protection. It is crucial to enable validation, permission, and method management for cloud-stored data to improve security in cloud estimating.There are primary areas of data security:[10].

Confidentiality:- To ensure protection of data from attacks, the analysis of the top exposure should be performed. Therefore, a safety test has been planned to protect the data from malicious users using techniques like cross-platform scripting and access control, among others.

Integrity:-Thin clients are employed in places where there aren't enough things to support the client data. Users continue to not keep their passwords or other sensitive

information to a great extent out of concern about their integrity.

Availability:-Only a small number of possible owners are available to narrow clients in order to fund the customer document.Users continue not to maintain their passwords for their user data on hand for concern that security may be guaranteed.

Locality:- In cloud environment, the data is provided over several places, making it difficult to locate the data's present life.The organizations controlling the data may shift significantly when it is presented to several geographical areas.The topic of consent and data privacy regulations in cloud computing is very complex. Clients know where respective data are located, and each internet connection provider is recommended.[11].

Integrity:-The system makes security claims up front by specifying that a file can only be compressed once with in anapproved life.Data integrity must be maintained in a cloud-based setting to keep the data from becoming diverted.In order to maintain dossier integrity, all cloud enable transactions generally adhere to ACID Properties. Since most online tasks employ HTTP tasks, they frequently encounter some issues with managing projects.The HTTP protocol does not support or ensure undertaking or transmittal. Executing transaction management within the Application itself can control it.

Access: -The term "data approach" mostly refers to data security measures. According to an agreement, the employees will go to the portion of the document where their organization's security strategies are listed. Each additional employee operating under the same arrangement is restricted from accessing the same data. To ensure that data is shared only with authorized individuals, several encryption techniques and key management tools are utilized. Only the permitted bodies are given the key via various key disposal systems.The data security protocols must be strictly adhered to inorder to protect the data from illegitimate consumers. All cloud users will likely gain access through the computer network, thus it should provide authorized user access.Encryption and maintenance procedures for documents can be used by users to reduce security risks.[12]

Confidentiality: - In Cloud computing data stored on separate servers, and content like data, films,etc. may best orded with one or more different cloud providers. Data confidentiality is the most primary needs when data is stored in a separate attendant. Users must see which documents are stored in the cloud and their accessibility in order to ensure confidentiality of data understanding and categorization.

Breaches:-Data breaches are yet another significant issue with cloud security that is expected.Since there is a lot of data from different consumers stored in the cloud, there is a chance that a malicious user would disclosethe cloud and reveal that the entire cloud environment is experiencing an extreme financial attack.A breach may happen as a result of several accidental broadcast issues or an insider attack.

Segregation:-Dynamic is one of the key characteristics of cloud computing. There is a possibility of a data breach since multi-tenure enables the storage of dossiers by a wide range of users on cloud servers. The dossier can be injected by using any usageor by injecting a customerrule. So it's crucial to store client files away from surplus customer files. Dossier separation vulnerabilities may be found or recognized with tests like SQL needle AWS, Data verification,and in secure storage.

Storage:-Numerous problems exist in the virtual machines' dossier. Data conversion dependability is a person-specific issue. Virtual machines must be stored in a physical foundation that could threaten their freedom.
Operation of Data Centers:- For secure data processing and distribution across cloud users, a document structure might be designed. To identify threats in a reasonable amount of time, a network-based interruption block plan is implemented.The use of an RSA-based depository protection approach to estimate large numbers of files with various file sizes and to address detachable document freedom may be necessary.[13, 14, and 15]

4.0 Possible-Solutions:

The best policies to protect the data in the cloud environment are:

Encryption. It is preferable to encrypt the document before uploading it to the cloud.Data Owner may allow group members to view specific documents that may be easily obtained by the governing class.Tosupply dossier approach control,heterogeneous dossier-centric freedom is anticipated to be implemented. A methodology for data security that combines confirmation, data honour and encryption, dossier recovery, and customer support isprojectedtostrengthenthesecurityofdossiersstoredinthecloud.Guardianship of the data may be used to protect privacy and security. Applying encryption to documents that make them completely useless and using standard encryption can confuse availability and can stop data from being accessed by additional customers. Customers are advised to confirm either the validity of the document before uploading it to the cloud.When identity located signaling code andRSASignature are combined ,RSA located dossier integrity check may be supported. SaaS ensures that there must be different borders between two things at the physica land use levels to protect data from various customers.

In cloud computing, approach administration can be done via a distributed approach control design. Utilizing references or assigned located policies is preferable when labeling unjustifiable consumers.To inform the consumer of the potential benefit so find is criminate data collection, permission may be utilized as a tool. A fine-grained approach control mechanism enables the owner to assign the majority of computationally demanding tasks to cloud servers without disclosing the contents of the data for secure data processing and distribution across cloud users, a document structure might be designed. To identify threats in a reasonable amount of time, a network-based interruption stop plan is implemented. The use of an RSA-based depository protection

approach to estimate large numbers of files with various file sizes and to address detachable document freedom may be necessary.

A foolproof Key management mechanism system is the key to protecting the stored data and providing access to the genuine user. This can be achieved by the best key management algorithm.

A recordbook,which will keep the record of all users with a time stamp when and how long particular information is accessed by any particular user, which will help to track the malicious user and activities.

5.0 Conclusion:

Although the cloud is a new form of technology that offers users a lot of advantages,it also has certain security issues.The obstacles to dossier freedomare discussed in this study,along with ideas to help overcome the risks associated with cloud computing. Future cloud computing safety protocols may be strengthened. Modern encryption techniques may be used to bury and recover documents from the cloud in order to establish a secure document approach. Additionally,goodkey administration techniques may be utilized to categorize the key for cloud users so that only authorized clients can access the information.

6.0 References:

1. L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud definition, in: ACM SIGCOMM Computer Communication Review, 2008.p.50-55.

2. M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6

3. ShuchengYu,CongWang,KuiRen,andWenjingLou.Achievingsecure,scalable,andfine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9

4. . Kresimir Popovic and Zeljko Hocenski. Cloud computing security issues and challenges, in: MIPRO, 2010 Proceedings of the 33rd International Convention, 2010.p.344-349.

5. Akhil Bhel, Emerging Security Challenges in Cloud Computing. Information and Communication Technologies, in 2011 World Congress on, Mumbai, 2011.p.217-222.

6. .Z. Xiao and Y. Xiao. Security and Privacy in Cloud Computing, IEEE Communications

Surveys & Tutorial, Vol. 15, 2012, No 2, p.843-859.

7. . Pandey, A., Tugnayat, R. M., Tiwari, A. K. Data Security Framework for Cloud Computing Networks International Journal of Computer Engineering & Technology 2013

8. . Chen, D., Zhao, H. Data security and privacy protection issues in cloud computing 1 Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12) March 2012 Hangzhou, China 647 651

9. M. Sookhak, H. Talebian, E. Ahmed, A. Gani, M. K. Khan. A Review on remote data auditing in single cloud server: Taxonomy and open issues. Journal of Network and Computer Applications, Vol. 43, 2014, p.121-141

10. F. Sabahi. Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. International Journal of Machine Learning and Computing, Vol. 2, No. 1, 2012, p.39-45.

11.Y. Sun, J. Zhang, Y. Xiong and G. Zhu. Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, Vol. 10, Iss. 7, 2014, p.1-9.

12.A. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, Elsevier, Vol. 34, Iss. 1, 2011, p.1-11.

13. R. Bhadauria, S. Sanyal. Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. International Journal of Computer Applications, Vol. 47, 2012, No. 18, p.47-66.

.

14.. K. Jakimoski. Security Techniques for Data Protection in Cloud Computing. International Journal of Grid and Distributed Computing,Vol. 9, No. 1, 2016, p.49-56.

15 . M. Sookhak, A. Gani, M. K. Khan and R. Buyya. Dynamic Remote Data Auditing for Securing Big Data Storage in Cloud Computing.Information Sciences: An International Journal, Vol. 380, Iss. C, 2017, p.101-116.