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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111218

Security of Cloud Computing

Achal Jairam Madavi[1], Vijay M. Rakhade[2], Ashish Baban Deharkar[3]

Final Year Student, Computer Science and Engineering, Shri Sai College of Engg. & Tech. Bhadrawati, India[1]

Assistant Professor, Computer Science and Engineering, Shri Sai College of Engg. & Tech. Bhadrawati, India[2]

Assistant Professor, Computer Science and Engineering, Shri Sai College of Engg. & Tech. Bhadrawati, India[3]

Abstract: Security of cloud computing is a firm hand of cyber security devoted to securing cloud computing systems. Security of cloud computing or directly cloud security touch on to a board set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, application, services, and the associated infrastructure of security of cloud computing.

Keywords: Security, Cloud Computing

I. INTRODUCTION

The security of cloud computing is a collection of technology designed to address internal and external threats. Security of cloud computing or more clearly cloud security touch on to a board set of policie , technologies , applications ,and controls make use of to protect virtualized IP , data , application , services , and The related infrastructure of cloud computing .Cloud computing Industry is growing .According to Gartner, World Wilde cloud services revenue is on pace to surpass $56.3 billion in 2009, a 21.3% increase from 2008 revenue of 46 .4 billion, according to Gartner , Inc. The market is expected to reach $150.1 billion in 2013. Business are increasing cloud adaption. We expect a great deal of migration towards cloud computing within the federal government in addition to the already robust private sector growth. The growth of the cloud should not protect the data that goes into it.

II. ARCHITECTURE

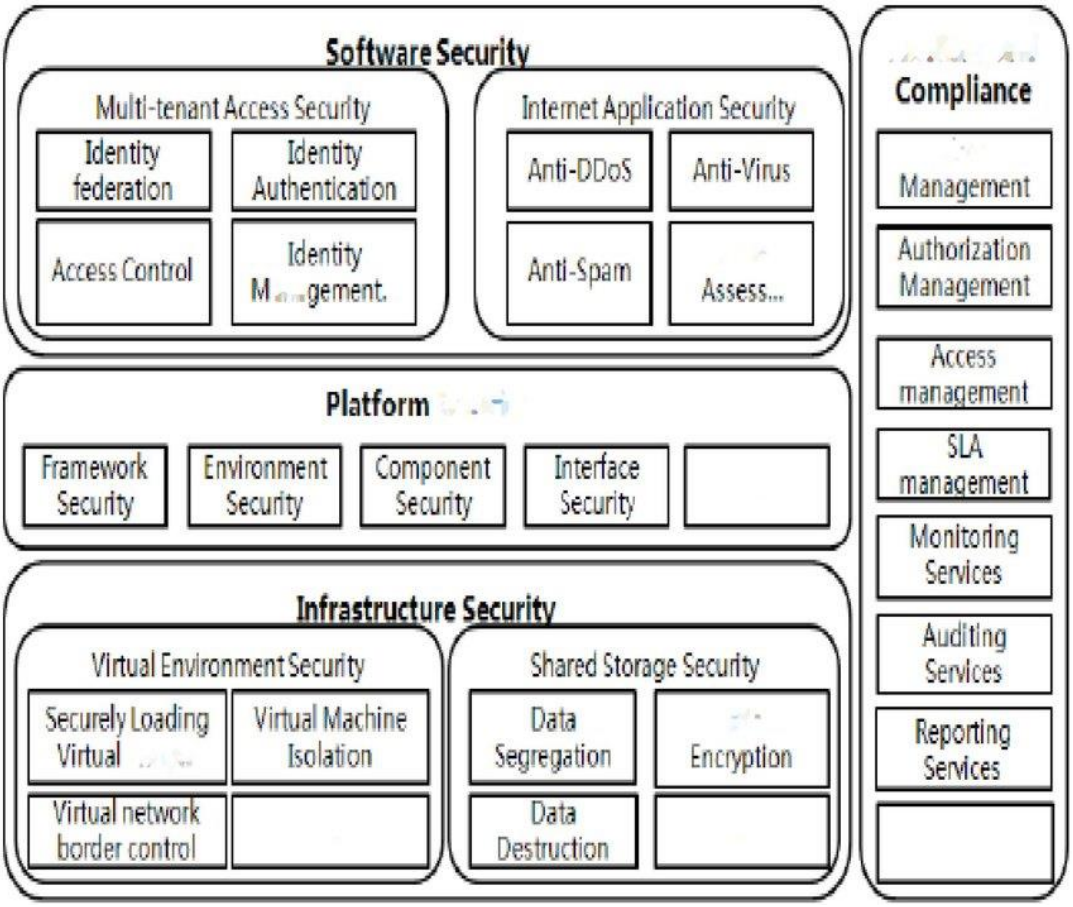
Security in cloud computing is a major concern. Proxy and brokerage servies should be employed to restrict a client from accessing the shared data directly. Data in the cloud should be stored in encrypted form.

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111218



III. SECURITY OF CLOUD COMPUTING

Security is protection from, or resilence against, potential harm caused by other,by restraing the freedom of others to act. Security of cloud computing is a collection of security measures designed to protect cloud-based infrastructure, application and data.

These security measures are configured to protect cloud data, support regulatory compliance and protect costomerrs privacy as well as setting authentication rules for indivial user and devices. From authencating access to filtering traffic , cloud security can be configured to the exact need of the business .and because these rules can be configured and managed in one place ,administration overheads area reduced and IT tearms emprovered to foucs on other area of the business.

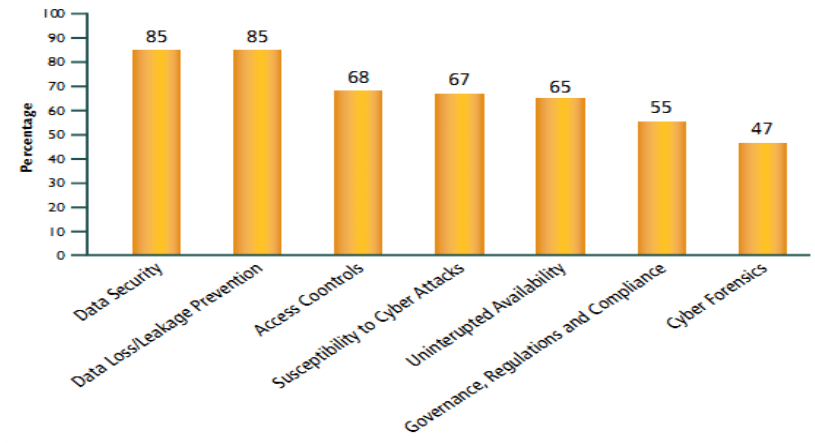


Fig1.cloud security

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111218

CLOUD COMPUTING

Cloud computing is based on five attributes: multitenancy, massive scalability, elasticity, pay as you go, and self-provisioning of resources.

Multitenancy:

Unlike previous computing models, which assumed dedicated resources (i.e., computing facilities dedicated to a single user or owner), cloud computing is based ona business model in which resources are shared (i.e., multiple users use the same resource) at the network level, host level, and application level.

Massive scalability:

Although organizations might have hundreds or thousands of systems, cloud computing provides the ability to scale to tens of thousands of systems, as well as the ability to massively scale bandwidth and storage space.

Elasticity:

Users can rapidly increase and decrease their computing resources as needed, as well as release resources for other uses when they are no longer required.

Pay as you go:

Users pay for only the resources they actually use and for only the time they require them.

Self- provisioning of resources:

User self – provision resources, such as additional system (processing capability, software, storage) and network resources.

CLOUD SECURITY DESING PRINCIPLES

The security design principle are the key pillars for implementation of cloud security to project system, application and platform security architecture.

Below are the key desing principles which needs to be considered for cloud technology adoption.

1.

1. Security at all layers: Ensure robust security is applied to all layers [physical, network, data, application,etc. of their architecture with multiple security controls. This will ensure end to end protecting of application/ data hosted by departments on cloud platform.
2. Safeguard data while at rest and in transit: Identify and Classify the dada in terms of critically / sensitivity and define their levels. This can be prevented via using the available security controls like access control, tokenization, encryption, etc.
3. Monitoring and auditing: Ensure monitoring, auditing and alerting is configured to capture the changes in the department's system in real time. Further, log integration and metric collection can automatically investigate, act and respond.
4. Access management and Controls: Ensure implementation of principle of selective privileges and impose segregation of duties with appropriate access and authorization. Centralized identity and access management can eliminate any unauthorized access and information loss/ theft
5. Readiness for security events: Department/CSP need to prepare system for any unusual security event. Regular vulnerability and security tests need to be conducts to identify the security gaps and issues. Drill can be conducted to record the response of the cloud systems at different layers.
6. Automate security best e practices: Automating software/hardware/application, based security system via AI/ML/Bots to improve the ability to secure environment which can perform regular checks and implement the controls needed to restrict the attack and enhance cloud security.
7. Cloud Vendor Lock-in: Department to ensure that there is no vendor lock-in by Cloud services provider while hosting the application/data, as there is no standard guidelines between different cloud providers for data migration and exports, so it becomes difficult to migrate data from one cloud provider to another or migration to on-premise Dara centre.

BENEFITS OF SECURITY OF CLOUD COMPUTING

High Availability – Ensuring continuity is one of the primary reasons behind businesses looking for reliable cloud security solutions. The assets, such as website and applications will always remain functional globally[3].

Cloud DDoS protection – Traditional network infrastructure work on the basic of origin and backup serves that can be easily disabled DDoS attacks that are capable of generating up to 20Gbps of traffic. These attacks can take anywhere from hours to mitigate during right cloud computing security solutions. The right cloud-computing security solution

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022
DOI: 10.17148/IJARCCE.2022.111218

should incorporate real-time support,24*7*365 live monitoring of business assets and have redundancies built-in so your website and applications remain online and functional even in the case of an attack.
With cloud service providers, such as Active Co 's cloud Services vancouver, you can rest assured that your core business which your services may be completely or partially affected and your business sustains severe financial and reputation loss. To ensure continuity of service, you need managed hosting providers and/or content delivery networks with DDoS absorption capabilities as well as real- time scanning to identify and prevent/mitigate DDoS attacks. This is done through the CDN`s capability of making use of a global network of PoPs that can manage spikes in legitimate traffic and divert synthetic spikes from a attack on the network. This enables CDN`s to both bring downtime down to zero as well as enables security controls that feel intuitive.

Flexibility- the right cloud computing solution for your business ensures irrespective of capacity. whether you`re experiencing a surge in legitimate traffic or in the case of an attack, the solution should be able to provide you enough flexibility to avoid server crashes and avoid unnecessary costs during lean hours through up or downscaling.

Data Security- Ensuring the privacy and security of your business` sensitive information and transactions is a top priority for your cloud computing security solutions. It should be able to prevent third parties for eavesdropping or tampering with your data through the right security protocols, such as, transport layer security [TLS]- the replacement to secure sockets layer [SSL] Ecommerce sites are particularly vulnerable to data breaches and should take care to implement a CDN with PCI compliance and other relevant digital rights management layers.

Regulatory compliance- Ecommerce businesses and financial institutions also face a greater degree of both industrial and governmental compliance and regulations checks. With the right CDN, you will be able to build a highly compliant infrastructure that is capable of always protecting your consumers` data.

Round The Clock Support- cloud Services Vancouver Have a host of companies offering cloud security solutions. The right cloud security solutions for your business, however, should be able to render downtimes to near zeros. It should be able to provide you with effective and time-sensitive customer support 24*7*365 any time of the day or night with live monitoring.

SECURITY OF CLOUD COMPUTING ADAVATAGES

1) Shifting public data to a external cloud reduces the exposure of the internal sensitive data
2) Cloud homogeneity makes security auditing / testing simpler
3) Clouds enable automated security management
4) Redundancy / disaster recovery

IV. CONCLUSION

The cloud computing has the potential to be a disruptive force by affecting the deployment and use of technology. The cloud be the next evolution in the history of computing, following in the footsteps of mainframes, minicomputers, PCs, servers, smart phones, and so on, and radically changing the way enterprise manage IT. Cloud computing provides advanced computing resources available on – demand, that scale as needed, with regular updates and without the need to buy and maintain an on - premise infrastructure. With cloud computing, teams to marked as they can rapidly acquire, scale services, without the considerable effort that requires managing a traditional on – premise infrastructure.
The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained.

REFERENCES

[1]. Cloud computing: concepts, technology, and architecture by Thomas Erl
[2]. Cloud computing: A hands on approach by Arshdeep Bahga & Vijay madisetti
[3]. Ashish B. Deharkar,"An Approach to reducing cloud cost and bandwidth by using the TRE System" International Journal of Research Publication and Reviews,IJRPR,Volume 3 , Issue 5, 2022.
[4]. A. Abbas, S.U. Khan, A review on the state-of-the-art privacy preserving approaches in e-health clouds, IEEE J. Biomed. Health Inform. (2014), http:// dx.doi.org/10.1109/JBHI.2014.2300846.
[5]. A. Abbas, K. Bilal, L. Zhang, S.U. Khan, A cloud based health insurance plan recommendation system: a user centered approach, Future Gener. Comput. Syst. (2014), http://dx.doi.org/10.1016/j.future.2014.08.010.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 11, Issue 12, December 2022

DOI: 10.17148/IJARCCE.2022.111218

[6]. R. Agrawal, Legal issues in cloud computing, in: IndicThreads.com, Conference on Cloud Computing, 2011. [4] K. Alhamazani, R. Ranjan, K. Mitra, F. Rabhi, S.U. Khan, A. Guabtni, V. Bhatnagar, An Overview of the Commercial Cloud Monitoring Tools: Research Dimensions, Design Issues, and State-of-the-Art, arXiv preprint arXiv:1312.6170, 2013.

[7]. M. Ali, R. Dhamotharan, E. Khan, S.U. Khan, A.V. Vasilakos, K. Li, A.Y. Zomaya, SeDaSC: secure data sharing in clouds, IEEE Syst. J. (2015), http:// dx.doi.org/10.1109/JSYST.2014.2379646.

[8]. O.D. Alowolodu, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, O.S. Ogundele, Elliptic curve cryptography for securing cloud computing applications, Int. J. Comput. Appl. 66 (2013).

[9]. M.R. Anala, J. Shetty, G. Shobha, A framework for secure live migration of virtual machines, in: IEEE International Conference on Advances in Computing, Communications and Informatics, 2013, pp. 243–248.

[10]. A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, M. Xu, Web services agreement specification (WSagreement), (accessed 26.05.14).

[11]. M. Aslam, C. Gehrmann, M. Bjorkman, Security and trust preserving VM migrations in public clouds, in: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 869–876. [10] M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, A security analysis of amazon's elastic compute cloud service, in: Proceedings of the 27th Annual ACM Symposium on Applied Computing, 2012, pp. 1427–1434.

[12]. R. Bhadauria, R. Borgohain, A. Biswas, S. Sanyal, Secure Authentication of Cloud Data Mining API, arXiv preprint arXiv:1308.0824, 2013.

[13]. K. Bilal, S.U.R. Malik, S.U. Khan, A.Y. Zomaya, Trends and challenges in cloud data centers, IEEE Cloud Comput. Mag. 1 (1) (2014) 10–20.

[14]. R. Bobba, H. Khurana, M. Prabhakaran, Attribute-sets: a practically motivated enhancement to attribute-based encryption, in: Computer Security ESORICS, Springer, Berlin, Heidelberg, 2009, pp. 587–604.

[15]. S. Carlin, K. Curran, Cloud computing security, Int. J. Ambient Comput. Intell. 3 (1) (2011) 14–19.

[16]. R. Chandramouli, M. Iorga, S. Chokhani, Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing, Springer, New York, 2014, pp. 1–30. doi: 10.1007/978-1-4614-9278-8_1.

[17]. S. Chaisiri, B. Lee, D. Niyato, Optimization of resource provisioning cost in cloud computing, IEEE Trans. Services Comput. 5 (2) (2012) 164–177.

[18]. D. Chen, H. Zhao, Data security and privacy protection issues in cloud computing, in: International Conference on Computer Science and Electronics Engineering (ICCSEE, IEEE), vol. 1, 2012, pp. 647–651.

[19]. J. Che, Y. Duan, T. Zhang, J. Fan, Study on the security models and strategies of cloud computing, Proc. Eng. 23 (2011) 586–593. [19] S.M.S. Chow, Y. He, L.C.K. Hui, S.M. Yiu, Spicesimple privacy-preserving identity-management for cloud environment, in: Applied Cryptography and Network Security, Springer, Berlin, Heidelberg, 2012, pp. 526–543.

[20]. A. Corradi, M. Fanelli, L. Foschini, VM consolidation: a real case based on openstack cloud, Future Gener. Comput. Syst. 32 (2014) 118–127