Multi-Disciplinary Journal
ISSN No- 2581-9879 (Online), 0076-2571 (Print)
www.mahratta.org,editor@mahratta.org

Threats In The World Of Cloud Computing Security

Shruti S. Gosavi
Research Scholar, Tilak Maharashtra Vidyapeeth, Pune-37

Abstract

As a replacement for of using your computer's hard drive to store or access data and programmes, you can use the cloud computing technology. Adoption rates are increased by cloud computing ability to enable customers to quickly spin up workloads without having to deal with the costs associated with maintaining physical infrastructure. As more businesses adopt the cloud in one way or another, there are a number of security risks that come with it.

Users may quickly spin up workloads thanks to cloud computing without having to deal with the hassle of maintaining physical infrastructure. This substantially boosts adoption rates when combined with the inexpensive price. What are the security dangers connected to cloud computing with this expanding adoption? In this paper we list the top online dangers.

Keywords: Cloud computing, data, cloud storage, social networks, security

Introduction

Humans use physical space extensively to retrieve and retain information that is contained on paper. The use and administration of the information technology infrastructure have been transformed by the cloud computing paradigm. The amount of administration work required by the user to use shared resources in a system where costs are paid when they are incurred rather than before or after is reduced to a minimum. On-demand self-services, pervasive network connectivity, resource pooling, elasticity, and measurable services are characteristics of cloud computing. The previously described the advantages of cloud computing make it an obvious choice for adoption by companies, organisations, and individual consumers. Increased security issues accompany the advantages of low cost, minimal management (from the users' point of view), and greater flexibility. Based on a certain user, a file is divided into fragments. criteria that ensure no useful information is contained in any individual fragments. Each cloud node—we refer to compute, storage, physical, and virtual machines collectively as "nodes"—contains a unique fragment to improve data security. On any node, though, a successful assault is always a possibility. If a single node is successfully attacked, the locations of other cloud fragments must remain a secret. We choose the nodes such that they are not contiguous and are a specific distance apart from one another to further increase security and prevent an attacker from knowing the locations of the file pieces..

The nodes are chosen based on the centrality measurements that provide a faster access time in order to speed up data retrieval time. We judiciously replicate fragments over the nodes that receive the most read/write requests in order to further reduce the retrieval time. There are two stages to the nodes' selection process. Based on the centrality metrics, the nodes are chosen for the initial placement of the pieces in the first phase. The replication nodes are chosen in the second phase. Traditional cryptographic methods for data security that increase performance

Many cloud storage platforms are available. Some of them have a specific objective, while others are prepared to gather any kind of digital data. Some cloud storage platforms are designed for small businesses, but some are so big that the mechanical components may fill an entire warehouse. At its most basic level, a cloud storage system just needs one data server connected to the internet, which is where these systems are managed. A computer user who subscribes to a cloud storage service sends copies of his files to the data server over the internet, which then stores the data on the cloud storage. The client can use a web-based interface to contact the data server when they want to restore their information.

The client can then locate and manage the files on the server itself, or the server can transmit the file back to the client. Network, computer, and data security are all included in the term "cloud security."

Loss of governance is a significant danger that must be addressed by cloud security. Both clients and providers may share responsibility for various aspects of cloud security, but the policy needs to make this clear. For both consumers and providers, the shift from local to remote computing presents numerous security concerns and difficulties. Many cloud services are offered by reliable third parties, creating additional security risks.

The cloud providers deliver their services over the internet and employ numerous web technologies, which give rise to fresh security concerns. In other words, the cloud of the future will be an even stronger and more impenetrable digital fortress. Advances in AI, machine learning, quantum computing, and other transformational technologies will lead to more intelligent, automated, and discriminating cloud security.

Cloud based product analysis-

Adobe: As reported in early October of 2013 by security blogger Brian Krebs, Adobe originally reported that hackers had stolen nearly 3 million encrypted customer credit card records, plus login data for an undetermined number of user accounts. The report says that more than 150 million username and hashed password pairs taken from Adobe. The research shows that users Id, passwords, credential information been hacked.

Canva: Canva is a Australian graphic design tool website. According to sources in may 2019 they suffered an attack that exposed email addresses, usernames, names, cities of residence, and salted and hashed with bcrypt passwords (for users not using social logins — around 61 million) of 137 million users. Canva had detected their attack and closed their data breach server.

e-Bay: It is an American multinational e-commerce corporation e-Bay reported that an attack exposed its entire account list of 145 million users in May 2014, including names, addresses, dates of birth and encrypted passwords. The online auction giant said hackers used the credentials of three corporate employees to access its network and had complete access for 229 days—more than enough time to compromise the user database. When they get to know about the threat at that time company ask customers to change their passwords for security issues.

Bigbasket: In October, a popular online grocer in India, BigBasket suffered a massive data breach that left data of 20 million users exposed. According to sources, the breach occurred on October 14 and made public on November 7 where personal information of users such as full names, email addresses, date of birth, IP addresses of user devices have been compromised and put up on sale on the dark web.

Linkedin: As the major social network for business professionals, LinkedIn has become an attractive proposition for attackers looking to conduct social engineering attacks. However, it has also fallen victim to leaking user data in the past.

In 2012 the company announced that 6.5 million unassociated passwords (unsalted SHA-1 hashes) were stolen by attackers and posted onto a Russian hacker forum. However, it wasn't until 2016 that the full extent of the incident was revealed. The same hacker selling MySpace's data was found to be offering the email addresses and passwords of around 165 million LinkedIn users for just 5 bitcoins (around $2,000(INR1,48,438.80) at the time). LinkedIn acknowledged that it had been made aware of the breach, and said it had reset the passwords of affected accounts.

SinaWeibo: With over 500 million users, Sina Weibo is China's answer to Twitter. However, in March 2020 it was reported that the real names, site usernames, gender, location, and -- for 172 million users -- phone numbers had been posted for sale on dark web markets. Passwords were not included, which may indicate why the data was available for just ¥1,799 ($250)(INR18,554.85)

Weibo: acknowledged the data for sale was from the company, but claimed the data was obtained by matching contacts against its address book API. It also said that since doesn't store passwords in plaintext, users should have nothing to worry about. This, however, doesn't tally as some of the information being offered such as location data, isn't available via the API. The social media giant said it had notified authorities about the incident and China's Cyber Security Administration of the Ministry of Industry and Information Technology said it is investigating.

Cloud computing provides users the convenience to spin up workloads without dealing with the overhead that comes with maintaining physical infrastructure, driving up adoption rates. With more and more organizations using the cloud in some form or another, it brings along with it a fair share of security threats.

Cloud computing provides users the convenience to spin up workloads without dealing with the overhead that comes with maintaining physical infrastructure. This, combined with the low cost, drives up adoption rates even further. With this growing adoption, what are the security risks associated with cloud computing?

We break down the top cyber threats below.

1. Identification and Accessibility

According to predictions, by 2023, insufficient management of identities, access, and privileges will be the cause of 75% of security failures. The most common method used in breaches today is the misuse of credentials. The identification infrastructure and company directories are being consistently attacked by the majority of attackers with amazing success. Over air-gapped networks, identity is a crucial lateral movement strategy that is responsible for the majority of breaches nowadays. Consider integrating Identity Governance and Administration (IGA), PAM (Privileged Access Management), and Cloud Infrastructure Entitlement Management (CIEM) solutions to manage identities and entitlements consistently, enforce the Principle of Least Privilege (PoLP) across all environments, and address the growing importance of identity-first security in the current distributed, largely digital landscape.

2. **Cloud Blunders**

According to data breaches revealed by companies like Verizon and Adobe Creative Cloud, incorrect settings of cloud infrastructure continue to be the leading cause of cloudcomputing s ecurity breaches globally.

The following list includes some of the most typical configuration issues in cloud infrastructure:

- Publicly accessible storage buckets
- Insecure resource access controls
- Exposed credentials in public repositories

Consistently checking for cloud misconfigurations becomes crucial because the great majority of cloud breaches are caused by configuration errors. You may do it thanks to the Cloud Security Posture Management (CSPM) software. As a result, according to Reportlinker.com, the global CSPM market is anticipated to increase from USD4M in 2020 to USD9M by 2026. It was also said that CSPM is now a required technology for enterprises using the cloud in the Gartner security conference of 2021.

3. Denial of Service

Due to the need for Internet connectivity to access them, cloud environments are particularly susceptible to DoS and Distributed Denial of Service (DDoS) assaults. Attackers may overwhelm a company's cloud network with excessive online traffic, making resources inaccessible to both customers and personnel. The size of the infrastructure component that is housed in the cloud will determine how deadly a DoS assault is to diminish the risk of DoS attacks:

- To reduce the attack surface, restrict access to network ports, protocols, and services.
- To reduce single points of failure, use load balancers and content delivery networks (CDNs).
- Establish a baseline of typical traffic so you can identify any anomalies.

- Set up a web application firewall (WAF) to stop people from taking advantage of known vulnerabilities.

4. Dangers from insiders

Up to 43% of security breaches are the result of internal organisational problems. Insider assaultscan be intentional (as in the case of irate employees) or unintentional; the best defence is appropriate training and awareness. Use the principle of least privilege when building your environment's access controls to minimise any potential harm that employees might cause and provide a suitable process for offboarding personnel. Most critically, cloud security is influenced by both technical and human factors. Taking care of your employees can reduce the possibility that rebellious employees will ruin your business.

5. Decreased visibility of infrastructure

Because of the nature of employing a third-party provider for computing, you give up some control to the cloud service provider (CSP). In this instance, your business does not own the physical infrastructure, making complete visibility of your infrastructure and resource usage more difficult, especially without the necessary technical competence. The Cloud is governed by a paradigm of shared responsibility between you and the cloud service provider (CSP). While the CSP manages the physical infrastructure, it is still your job to ensure the security of the data and application workloads in the cloud.This lack of visibility is a typical symptom in many complex cloud systems, rendering it vulnerable to data breaches and threats such as the next on this list – illegal access.

6. Cloud Workloads Used Without Authorization

Most significant CSPs use a self-service business model. Users now find it simpler to provide and de-provision workloads as needed on the fly. On the other hand, because it's so simple to use, dark IT, IT resources that users build and use without the IT team's knowledge also arises. Risks associated with dark IT include, but are not limited to:

- Increasing likelihood of data loss and data leakage
- Noncompliance issues

Make sure to follow the concept of least privilege and only permit users who require the ability to create workloads to do so on the task. Set up audit logging and alerting systems so you can keep tabs on all internal activity and quickly identify any unlawful activity.

7. APIs: That is not secure

Although your infrastructure may have watertight controls, unsecured application APIs can punch holes in your environment's protections and establish an access point. Several APIs include security flaws that, if abused, can put your cloud environment at risk. To mitigate this risk, have your IT staff check any external application that any team intends to utilise and be aware of potential hazards before implementing it. Maintain an eye out for security updates and application fixes.

8. Problems with Compliance & Regulation

Finally, depending on their geographical activities and business type, firms must keep track of and comply with a variety of regulations. Keeping up with new regulations and updating previous ones as the landscape changes can be difficult for enterprises. Constant cloud compliance emerges as the primary solution to regulatory issues. It entails regularly monitoring your cloud compliance status rather than focusing on it only during audit season. Conducting due diligence early in the process reduces the significant costs associated with non compliance.

9. Active, comprehensive defense

None of these dangers are novel, but the shifting environment and move to the cloud call for a different strategy than the on premise workloads of the past. Being proactive not only keeps bigger, more expensive problemsfrom arising, but it also helps establish the reputation of your company and frees you upto concentrate on the duties that improve your company's bottom line.

10. Data breaches

A data breach is any incident where confidential or sensitive information has been accessed without permission. Breaches are the result of a cyber-attack where criminals gain unauthorized access to a computer system or network and steal the private, sensitive, or confidential personal and financial data of the customers or users contained within. Some common cyber threats in data breaches are ransomware, data loss and denial of service.

Conclusion

In cloud computing, cloud security is crucial to maintaining the security of all data centers. Organizations must resolve this problem by enlisting the aid of specialists if some users' data is lost or accessed by an uninvited party. Even while not everyone becomes a victim of cybercrime, they are nevertheless at danger. Customers must also keep their data backups current in order to store it on numerous systems.

References

[1] Mell, Peter, and Tim Grance. ”The NIST definition of cloud computing.” National Institute of Standards and Technology 53.6 (2009): 50
[2] Lu, Yanbin, and Gene Tsudik. ”Privacy-preserving cloud database querying.” Journal of Internet Services and Information Security (JISIS) 1.4 (2011): 5-25.
[3] Pavithra, S., and Mrs E. Ramadevi. ”STUDY AND PERFORMANCE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS.” International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1.5 (2012): pp-82.
[4] Rijmen, P., and Joan Daemen. ”Advanced Encryption Standard.” Proceedings of Federal Information Processing Standards (2001)
[5] Miller, Frederic P., Agnes F. Vandome, and John McBrewster. ”Advanced Encryption Standard.” (2009).
[6] Daemen, Joan, and Vincent Rijmen. ”Rijndael, the advanced encryption standard.” Dr. Dobb’s Journal 26.3 (2001): 137-139.
[7] Rivest, Ronald L. ”The RC5 encryption algorithm.” Fast Software Encryption. Springer Berlin Heidelberg, 1995.
[8] Rivest, Ronald L., Adi Shamir, and Len Adleman. ”A method for obtaining digital signatures and public-key cryptosystems.” Communications of the ACM 21.2 (1978): 120-126
[9] Ostrovsky, Rafail, Amit Sahai, and Brent Waters. ”Attribute-based encryption with non-monotonic access structures.” Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007.
[10] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attributebased encryption. In Proc. of the 2007IEEE Symposium on Security and Privacy (S&P’07), Berkeley, California, USA, pages 321334. IEEE, May 2007.
[11] Goyal, Vipul, et al. ”Bounded ciphertext policy attribute based encryption.” Automata, Languages and Programming. Springer Berlin Heidelberg, 2008. 579-591.
[12] J. Camenisch, G. Neven, and A. Shelat. Simulatable adaptive oblivious transfer. In Proc. of the 26th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT07), Barcelona, Spain, LNCS, volume 4515, pages 573590. Springer-Verlag, May 2007.
[13] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan. Private information retrieval. Journal of the ACM (JACM), 45:965981, November 1998.
[14] V. Goyal, O. Pandey, A. Sahai, and B.Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proc. of the 13th ACM Conference on Computer and Communications Security (CCS06)Alexandria, Virginia, USA, pages 8998. ACM, October 2006.
[15] M. Green and S. Hohenberger. Blind Identity-based encryption and simulatable oblivious transfer. In Proc.of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security (ASIACRYPT07), Kuching, Malaysia, LNCS
[16] e 4833, pages 265282. Springer- Verlag, December 2007.J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Proc. of

the 27th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT08), Istanbul, Turkey, LNCS, volume 4965, pages 146162. Springer-Verlag, 2008.

[17] Shi, Elaine, and Brent Waters. ”Delegating capabilities in predicate encryption systems.” Automata, Languages and Programming. Springer Berlin Heidelberg, 2008. 560-578.

[18] Y. Lu and G. Tsudik. Enhancing data privacy in the cloud. In Proc. of the 5th IFIP WG 11.11 International Conference on Trust Management(IFIPTM11), Copenhagen, Denmark, LNCS, volume 358, pages 117132.Springer-Verlag, 2011

[19] Sahai and B. Waters. Fuzzy Identity-based encryption. In Proc. of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT05), Aarhus, Denmark, LNCS volume 3494, pages 557557. Springer-Verlag, May 2005.

[20] E. Shen, E. Shi, and B. Waters. Predicate privacy in encryption systems.In Proc. of the 6th Conference on Theory of Cryptography (TCC09), San Francisco, California, USA, LNCS, volume 5444, pages 457473. Springer-Verlag, March 2009.

[21] Horwitz, Jeremy, and Ben Lynn. ”Toward hierarchical identity-based encryption.” Advances in CryptologyEUROCRYPT 2002. Springer Berlin Heidelberg, 2002.

[22] Y.C. Chang and M. Mitzenmacher. Privacy preserving keyword searches on remote encrypted data. In Proc. of the 3rd Conference on Applied Cryptography and Network Security (ACNS04), New York, New York State, USA, LNCS, volume Smid, Miles E., and Dennis K. Branstad. ”Data encryption standard: past and future.” Proceedings of the IEEE 76.5 (1988): 550-559

[23] Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud Security and Privacy*. New York: O’Reilly.

[24] McFedries, P. (2008, August). The Cloud Is The Computer. *IEEE Spectrum*.

[25] Mikkilineni, R., & Sarathy, V. (2009). Cloud Computing and the Lessons from the Past. In *Proceedings of the 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises*, Groningen, The Netherlands.

[26] Tilak, G. (2020). Utilization of Cloud Computing in Higher Educational Institutions.