INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

COUNTER MEASURES FOR DATA BREACH IN CLOUD COMPUTING

Nandhakumar.C[1], Ranjithprabhu.K[2,] Raja.M[3]

[1]Assistant Professor, Department of CSE, PPG Institute of Technology, Coimbatore, India
[2,3]PG Scholar, Department of CSE, PPG Institute of Technology, Coimbatore, India
Author Correspondence: Dept. of CSE, PPG Institute of Technology, Coimbatore-15, Tamil Nadu, India
E-mail: [1]nandhu_army@yahoo.co.in, [2]ranjithprabhu.K@gmail.com, [3]kingrr20@gmail.com

Abstract

Cloud computing is a new era of computing that outsources massive computational power with scalable computing capabilities. It provides on-demand resources for IT provisioning based on virtualization and distributed computing technologies. Cloud computing is not without its risks. It involves in the loss of control over data as well as new security and privacy issues. To promote cloud computing in a wide range of applications, security issues need to be resolved. The fact is that these security issues are definitely manageable with some control measures taken. Data breach is one of the top threatening factors of cloud security. This paper examines the causes of data breach and describes the counter measures to prevent the cloud system from data breaches.

Keywords*:* Cloud Computing, Cloud Security, Data Breach, Data Governance, Ex-filtration

1. Introduction

Cloud Computing is a dynamically scalable distributed computing paradigm that moving towards a model, where users can avail the required services on demand at any instance. A computing technique that provides voluminous computing potential deployed via datacenter where multitudinous servers are clustered to organize the cloud environment. Cloud computing has transformed the IT into a new paradigm where users can access the services on pay per use basis. Cloud users are drastically increasing day by day. Enormous cloud services are provided by various cloud service providers. Some renowned cloud service providers are Google App Engine, Amazon EC2, and Microsoft Azure [5][6][7]. Many high profile organizations store their sensitive information in the cloud. Such data stored on the cloud servers are vulnerable to data breach (also known as data leakage or data spill).

A data breach is a security incident that violates the security goals of an individual or a network for unauthorized dissemination of information. It is an occurrence of stealing, viewing, copying and transmitting the confidential, protected and sensitive data by gaining unauthorized access to the system. An anonymous user or bot is the root cause for the data breach that occurs in the cloud arena. The uncertainty of data breach is higher than before for organizations who store their critical information assets such as proprietary corporate data, trade information, personally identifiable information, customer details and so on in the cloud server.

In 2013, Cloud Security Alliance (CSA) conducted a survey with industry experts to determine the extreme vulnerabilities in the cloud computing [10]. CSA come up with the notorious nine threats that makes cloud open to attack. As per the report of CSA, data breach is the top threatening vulnerability in cloud among the notorious nine. In the same year various public prominent sites were victimized for data breaches. Hackers

have stolen the username and passwords of almost two million accounts across various social networks in the month of November. Many sites, including Facebook, Gmail and YouTube, Twitter, LinkedIn, ADP were overwhelmed. A sophisticated security attack on October, affected over 38 million customers of Adobe [11].

2. Data Breach

A data breach is coordinated by an unauthorized hacker or attacker geared towards the electronic data stored on cloud. Data breach also leads to data loss where a security incident can thrash the entire data after replicates it to the targeted server. The four most causes of data breaches are

- Malware
- Theft or Stolen computers
- Insider attempt
- Attacks by an unauthorized user

Pwc carried out an Information Security Breach Survey (ISBS) assisted with Infosecurity Europe in the year 2014 to determine the security breaches that occurred in various levels of industries [12]. The ISBS was based on the average number of security breaches in a year and the overall cost of the security breaches. Fig 1 illustrates the types of security incident and their occurrence percentage from 2012 to 2014 based on ISBS report.

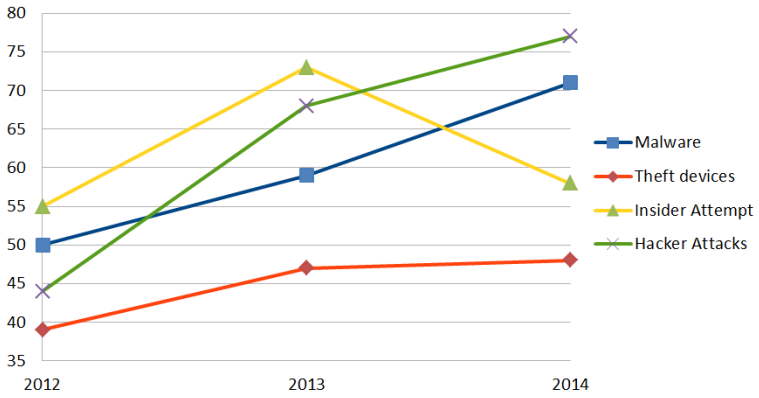

Figure 1: Data breach in IT from 2012 to 2014

2.1 Infection by Malwares

Malicious software programs familiarly known as “Malware” get installed in a cloud system in order to invade and steal passwords. Malware can be used to breach the data stored on the cloud systems. It will transmit the information to the hacker from the victim's system. Fig 1 represents that data breach through malwares and it has been increasing year by year. Malwares that affects the cloud systems are categorized into three types.

- **Virus:** a program that replicates and spread in many systems to thrash the sensitive data.
- **Spyware:** a program that retrieves the information from the victim's system in cloud and transmits it to the targeted servers.
- **Browser hijacking software:** a program that gathers the credential information such as username and passwords stored in the cache memory of the cloud system.

2.2 Stolen Computers

Risk of data breach is pertinent for corporate data stored in the lost or stolen laptops and other removable devices. Missing laptops and compact devices are a weekly occurrence in larger organizations. In such scenario, the stolen laptop might reveal sensitive information to the outsiders for unauthorized access to the cloud system. As per the report of ISBS, fig 1 shows that data breach by theft computers is literally low when compared to other causes.

2.3 Incidents caused by staff

Company employees who negligently violate data security policies continue to represent a major factor in occurrence of data breaches. From fig 2 it is clear that the data breach occurrence was significantly reduced when compared to the previous years. An engineer who weaved the network, contractors, and staffs working in the concern, former employees, even business partner who has or had authorized access to the cloud system may breach the data by violating the security and company policies.

2.4 Attacks by an unauthorized user

In cloud, data is distributed everywhere and it can be accessed from anywhere after proper authentication. But an intruder propagates various targeted attacks to breach the data kept in the cloud. More than 75 percent of data breach occurs because of hackers. From fig 1, it is clear that hacker attacks have been increasing year by year vigorously. It's a hard challenge to guard the information assets from a sophisticated hacking attack. The most common ways for an attacker to perform incursion is through targeted malware, SQL injection attacks [14] and with improper storage of login credentials.

- Targeted malware: Malware sent via emails from known senders to the victim's system to provide access to the hacker.
- SQL injection Attack: A web based attack propagated by analyzing the targeted websites to elevate the privileges and to gain access to the cloud database.
- Login credentials: Login information such us a username and password left in the browser's cache are easily obtained by the hackers and as well as the insiders.

Incursion has been just an initial level of attack in the cloud database. When it is done, then it becomes easy for the hacker to gain access to the cloud servers. Hackers usually perform four level attacks to constitute a data breach in the cloud.

1. Incursion: Hackers gain access to the cloud servers by violating the security policy.
2. Discovery: Hackers discover the data model, data structure and data map of the cloud storage system.
3. Capture: Access granted to view the data stored in the cloud and the hacker have complete unauthorized privilege to capture the data.
4. Ex-filtration: Finally, the hacker wraps up all the captured data to the targeted server in order to decrypt and breach the data stored in the cloud.

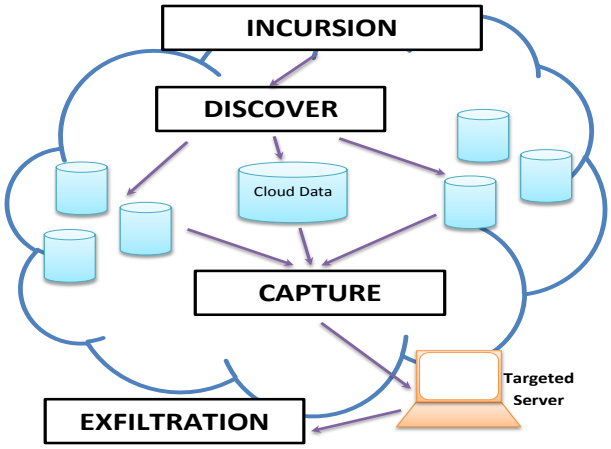

Figure 2: Data breach by Hacker in the Cloud

3. Counter Measures

In cloud computing, data breach activities can be controlled with three action measures. Control measures include data governance, maintaining information security and security architecture to minimize the potential risk of data exposure in the cloud. The hierarchy of control measures is represented in fig 3.Targeted attack by hackers to intrude in the cloud systems can be blocked by defining a strong security solution that should inspect network communications, protect core systems, detect and prevent intrusion. In addition, cloud terminals provide service to the end users should be managed centrally to make sure that strong encryption mechanism, persistent deployment of security policies and information access are used.

3.1 Data Governance

Data governance specifies to the comprehensive management of data integrity, security, availability and usability stored in the cloud database. Data governance monitors, manages, maintains and protects the information stored in the cloud.

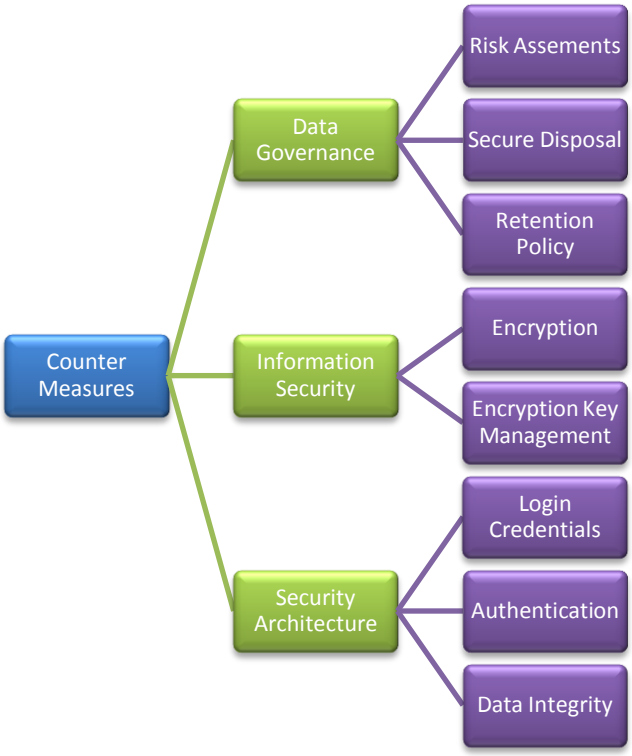

Figure 3: Counter Measures

Risk Assessments: Risks involved in storing and transmitting sensitive data across various cloud applications, servers and databases are needed to be analyzed at regular intervals and prevention mechanism need to be adapted. The possibility of unauthorized use of data stored in the cloud systems need to be determined.

Secure Disposal: Data once erased from the cloud should not be retained by any computer forensic techniques. Once after deleting the data, its replicas also need to be removed from the remaining cloud servers to ensure that data is not recoverable.

Retention Policy: A policy-based management service [15] established in an organization to retain information that offers scalable management of data retention policies attached to data objects stored in a cloud environment with high availability. Retention policy is essential to assure compliance of administrative, lawful, and permissible for business requirements with various policies and procedures.

3.2 Information Security

High security cryptographic approach is essential to manage sensitive user data stored in the cloud. Data should be accessed only by the authorized users by producing the indispensable decryption keys. Encryption and encryption key management has a vital role in the cloud to protect the data.

Encryption: Encryption should assure security and consent of consumer's confidential data. Encryption system should endorse fine grained access control [16] such as like standard based encryption and attribute based encryption [17] in order to enact secure storage and transmission of data in the cloud.

Encryption Key Management: Effective key management is essential to annihilate data breach from the cloud environment. The encryption key control need to be managed by a well trusted cloud servers, such as

like RSA data protection manager servers [18] for effective implementation of key management and to provide the decryption keys to the authorized cloud tenants.

3.3 Security Architecture

Defining security architecture is a tough challenge in cloud computing. We cannot define hardware based remedy since the cloud is scalable. Therefore, multi-layered data protection architecture similar to three-tier security model [20] is essential to authenticate and authorize various levels of cloud users in concerned with privacy. Login credentials, authentication and data integrity are the parameters needs to be considered to design trusted security architecture.

Login Credentials: Enforce the cloud users to create login credentials with strong passwords with alphanumeric letters. A minimum standard should be made mandatory for the cloud users to create their login to access the data. The password should be changed at regular intervals and it should not be the same one as previously used password. Apart from this cloud administrator needs to monitor and maintain the user activity logs and needs to terminate the access rights of the former employees.

Authentication: Data can be accessed from anywhere in the cloud. Consequently, Multi-factor authentication [21] is required for all remote users who access the data stored in the cloud. A user can be authenticated in multiple ways, such as like one time password (OTP) [22] can be generated and sent to user's registered mobile or e-mail and the user needs to enter the password to gain access to the cloud systems.

Data Integrity: Data is replicated and stored in multiple sites to avoid data loss and single point of failure [24]. In such scenario data needs to be integrated to ensure consistency and accuracy of data after being altered in any one of the sites.

Apart from these, recently created threat may vulnerable and it may not be detected by the security system used in the cloud. Consequently, real time regular update of newly discovered threats coordinated by the global security intelligence [19] is essential in order to increase the efficiency of the cloud security.

4. Conclusion

Advancement of cloud in a wide range of applications is threatened by various security issues. Many high profile organizations use cloud computing to store their sensitive and confidential data. Data breach is one of the most threatening vulnerability in cloud computing which will hand over valuable data of an organization to another. Cloud users should be cautious about the risk of data breach in cloud environment. In this paper, we have examined the foremost causes of data breach and described the counter measures to prevent the cloud system from data breaches.

REFERENCES

[1] Kandukuri, Balachandra Reddy, V. Ramakrishna Paturi, and AtanuRakshit, "Cloud security issues," *IEEE International Conference onServices Computing*, pp. 517-520, 2009.
[2] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding Cloud-Computing Vulnerabilities," *IEEE Security and Privacy*, Vol. 9, No. 2, pp. 50–57, 2011.
[3] Feng, Deng-Guo, Min Zhang, Yan Zhang, and Zhen Xu, "Study on cloud computing security," *Journal of Software*, Vol. 22, No. 1, pp. 71-83, 2011.
[4] Popovic and Z. Hocenski, "Cloud Computing Security Issues and Challenges," Proc. 33rd Int'l Convention on Information and Comm. Technology, Electronics and Microelectronics, IEEE Press, pp. 344–349, 2010.
[5] https://appengine.google.com
[6] https://aws.amazon.com/ec2
[7] https://azure.microsoft.com
[8] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications*, Vol. 34, No. 1, pp. 1 - 11, 2011.
[9] Takabi, Hassan, James BD Joshi, and Gail-JoonAhn. "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security & Privacy*, Vol. 8, No. 6, pp. 24 - 31, 2010.
[10] "The Notorious Nine: Cloud Computing Top Threats in 2013" retrieved from https://cloudsecurityalliance.org/research/top-threats/ on 09, July, 2014.
[11] http://www.techradar.com/news/software/security-software/the-top-10-data-breaches-of-the-past-12-months-1248890 accessed on 09/07/2014.
[12] "2014 Information Security Breaches Survey" retrieved from https://www.gov.uk/government/publications/information-security-breaches-survey-2014 on 11, July, 2014.
[13] Squicciarini, Anna, SmithaSundareswaran, and Dan Lin, "Preventing information leakage from indexing in the cloud," *IEEE 3rd International Conference in Cloud Computing (CLOUD)*, pp. 188-195, 2010.

[14] Halfond, William GJ, and Alessandro Orso. "AMNESIA: analysis and monitoring for Neutralizing SQL-injection attacks," In *Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering*, pp. 174-183, 2005.
[15] Li, Jun, SharadSinghal, Ram Swaminathan, and Alan H. Karp, "Managing data retention policies at scale," *IEEE Transactions on Network and Service Management*, Vol. 9, No. 4, pp. 393-406, 2012.
[16] Yu, Shucheng, Cong Wang, KuiRen, and Wenjing Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing." *IEEE Proceedings of INFOCOM*, pp. 1-9, 2010.
[17] Goyal, Vipul, OmkantPandey, AmitSahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data," *13th ACM conference on Computer and communications security*, pp. 89-98, 2006.
[18] Mowbray, Miranda, and Siani Pearson. "A client-based privacy manager for cloud computing." *4thinternational ICST conference on Communication system software and middleware*, pp. 5, 2009.
[19] http://www.globalsecurity.org/intell/
[20] Joshi, BD James, Walid G. Aref, ArifGhafoor, and Eugene H. Spafford. "Security models for web-based applications." *Communications of the ACM* 44, No. 2, pp. 38-44, 2001.
[21] Chang, Hyokyung, and Euiin Choi, "User Authentication in Cloud Computing." In *Ubiquitous Computing and Multimedia Applications*, pp. 338-342, Springer Berlin Heidelberg, 2011.
[22] Cheng, Fred, "Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm," *Mobile Networks and Applications*, Vol. 16, No. 3, 2011.
[23] K. Ranjithprabhu, and D. Sasirega, "Eliminating Single Point of failure and Data loss in cloud computing," IJSR, Vol. 3, No. 4, pp. 335-337, 2013.
[24] Wang, Cong, Qian Wang, KuiRen, and Wenjing Lou, "Privacy-preserving public auditing for data storage security in cloud computing," *IEEE Proceedings of INFOCOM*, pp. 1-9, 2010.
[25] Shaw M., 2003, Writing good software engineering research papers, *In Proceedings of 25th International Conference on Software Engineering*, pp.726-736

Author Profile

Nandhakumar.C – He is presently working as an Assistant Professor in the department of Computer Science in PPG Institute of technology under Anna University. He completed his Master's degree in computer science in the year 2006 under Bharathiar University. He received his post-graduation in software engineering from Anna University of Technology, Coimbatore in the year 2010. His research interests include Software Engineering and Cloud Computing.

Ranjithprabhu.K – He received his Master's degree in software systems under Bharathiar University in the year 2013. He is presently pursuing his post-graduation in computer science & engineering under Anna University in full time and Master of Philosophy in computer science in part time under Bharathiar University. His research interests include Network Security and Cloud Computing.

Raja.M – He is presently pursuing post-graduation in computer science & engineering under Anna University in PPG Institute of technology. He completed his bachelor degree in computer science under Anna University in the year 2007. His research interests include network security and Cloud Computing.