A Study on the Alternative Strategies and Approaches to Condense the Security Challenges and Threats Faced in the area of Cloud Computing

Habiba Sohail[a] and Dhanalakshmi Venugopal[a]

The focal point of this research maneuvers over the challenges and threats that are continuously being faced in cloud computing. Cloud computing is considered as one of the most versatile technology in the recent years. It is an innovative approach towards Information Systems and it has become an integral part of the IT industry. The paper aims to highlight the seriousness of the threats and challenges encountered in cloud computing. In this paper, we give an overview on what makes this technology the future of computing. Immense literature study was conducted to gather adequate data on the recent techniques and terminologies related to the research field. An in-depth research analysis presents a competent mechanism that identifies the challenges and threats in cloud computing. The paper also refers to different security breaches that occurred over the years and what measures were taken to overcome the catastrophic loss. Along with that, it also caters the alternative strategies and approaches available to overcome the possible security threats and challenges. Different alternative methods such as Cryptography and Access Control Mechanisms are identified which are feasible and can be utilized for enhancing the security in cloud computing. Cloud computing is no doubt growing in popularity but even the immensity of this technology cannot disguise the security issues that linger with it. After thoroughly investigating and inspecting all the literary resources, gathered data and information, it is discovered that although cloud computing is tremendously gaining its popularity in the IT field, concerns about its security impact have also been raised considerably. The conclusion of this paper provides different strategies to be adopted to condense the effect of security challenges in the chosen area of the research.

Keywords: Access Control, Cloud Application, Cloud Computing, Challenges, Cryptography, Data Portability, Information System, Interoperability, PaaS, SaaS, Security, Threats, Virtualization;

Introduction

Cloud computing is the future of computing. This research article discusses the challenges and threats faced in the area of cloud computing. Moreover, it highlights the alternative strategies and approaches to condense the security challenges being faced in cloud computing. It is an innovative approach towards Information Systems. Cloud computing reduces the complexity of storing and managing the data. All the big organizations such as Amazon, Google, IBM, and Microsoft are utilizing the flexibility of cloud computing.

In 2010, Hassan Takabi, James B.D.Joshi and Gail-Joon Ahn defined cloud computing as a model that enables convenient, on-demand network access to a shared pool of configurable computing resources. This cloud model promotes availability of data (Takabi, H., 2010).

According to Armbrust, et al., 2010, Cloud computing includes both, the services over the Internet as well as the hardware's and software's which are stored in the data centers that offers these services. These services are commonly referred to as "Software as a Service" which is abbreviated as (SaaS).

Some people also use the terms; IaaS (Infrastructure as a Service) or PaaS (Platform as a Service) to describe these services (Armbrust, M., 2010).

Cloud computing is considered as one of the most versatile technology in the recent years. In the year 2009, Christian Cachin, Idit Keidar, and Alexander Shraer stated that most of the organizations are turning towards Cloud computing because it not only provides remote data monitoring around the clock but also remote backup tools (Cachin, C., 2009).

Although cloud computing is tremendously gaining popularity in the IT field, concerns about the security issues have also been raised. This research article sheds light on two case studies from different organizations that mentions the security concerns that faced in cloud computing.

Framework

The framework conducted for this research paper is shown in Fig 1.

a. Department of Computer Science, Middle East College, Muscat, Oman
Correspondence: dhanalakshmi@mec.edu.om

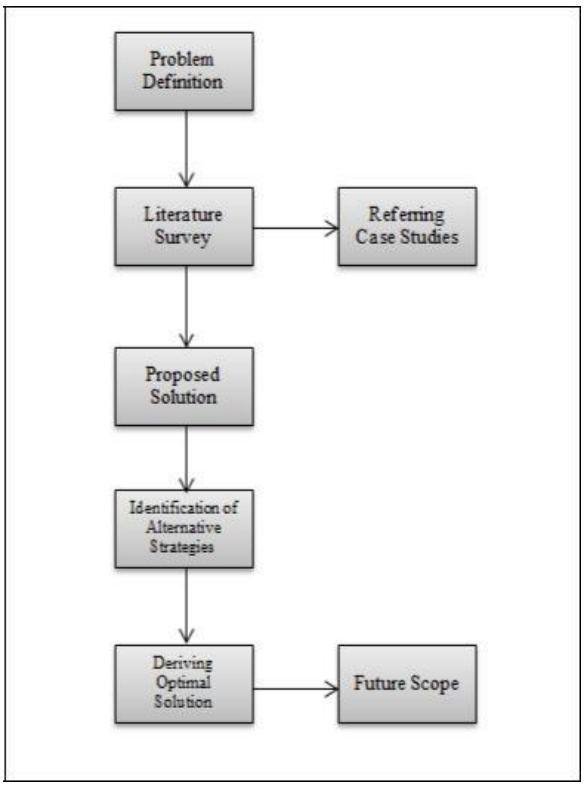

Fig 1: The framework

Literature study related to the research area

In this section, case studies related to the research area are presented. Many researchers have already performed a lot of detailed work in the same area of direction.

In the year 2013, Chimere Barron, Huiming Yu and Justin Zhan gave a detailed insight about the security challenges being faced by cloud computing. The presented work explained the concepts of cloud computing and how it is rapidly gaining popularity. It demonstrates different security case studies and describes the different types of security attacks on cloud such as Social Engineering Attacks, Account Hijacking etc. the work also provides solutions to how to keep the cloud secure and protected from different attacks (Barron, C., 2013).

The presented work is a comprehensive article that includes detailed research about the security challenges in cloud computing. It includes precise description of different cloud related security breaches that happened over time. It includes a lot of real life examples of organization that suffered from security breaches related to cloud computing. Moreover, it also elaborates the actions taken by the organizations to solve the security challenges. It also provides the reasons why the security breaches were occurred in the first place (Barron, C., 2013).

In the following year 2014, Harshit Srivastava defined the concepts of cloud computing in more detail.

The presented work described the different types of clouds which are available. Moreover, it gave an overview of the security breaches that occurred over the years. It also describes the security challenges and risks of cloud computing. The work explains the methods to make the cloud more secure and provides solutions for the security challenges.

The work includes real life examples of cloud security incidents that happened over the years. But it doesn't include the detailed scenario of how and why the security breaches were occurred in the first place. It should also give more insight about the solutions for these security concerns (Srivastava, H., 2014).

Case studies related to the research area

The following section sheds lights on the different case studies that highlight the security breaches related to cloud computing that occurred over the years.

A. Case Study 1: Security Breach at Drop Box

Drop Box which is Amazon's cloud based cloud storage service encountered a security breach in July 2012. The users suffered from a spam attack by the hackers. The hackers stole user names and passwords from third party websites. They used the stolen user names and passwords to gain access to the accounts of the Drop Box users. The hackers launched a spam attack by sending large amounts of spam emails to the email address used by those Drop Box accounts.

After further investigation, later it was revealed that a stolen password was used by the hackers to gain access to an employee's Drop Box account. The employee's account contained a file that included the user email addresses (Barron, C., 2013).

Drop Box immediately contacted the users which were affected by the spam attack and helped them to protect their accounts. In order to prevent any future similar attacks, Drop Box introduced additional controls to their system. They implemented two-factor authentication in the company's security controls. Two-factor authentication is a more secure and stronger authentication technique.

By using Two-factor authentication, the users have to enter at least two of the following three properties to prove his or her identity,

- Something that only the user knows such as a password or PIN
- Something that the user has like an ATM card
- Something unique that the user is identified by for example a biometric characteristic, such as a fingerprint

In addition to this, Drop Box also launched new and improved automated mechanisms to promptly identify any suspicious activities (Barron, C., 2013).

Although cloud computing is an evolving technology, but still the security risks are quite high. Drop Box should have already paid more attention to their security mechanism to prevent such blunders. But Drop Box learned from their mistake and followed a steady strategy to avoid any future attacks.

B. Case Study 2: Security Breach at Google

Google has the world's largest Cloud computing infrastructure. In March 2009, a data breach took place in Google Docs. The information privacy and security was compromised. Similarly, in March 2011, Google faced another major security breach. A highly unexpected bug was triggered at Google because of a faulty storage software update.

As a result of this breach at Google, around 150,000 Gmail accounts were affected. The email contents, calendar information, contacts and other contents stored in the Gmail accounts were all deleted. The entire 150,000 accounts were wiped cleaned. All of this happened because of the flawed security bug (Srivastava, H., 2014).

Google immediately took control of the situation. All the Cloud Service Providers ensures in the Service Level Agreement that at least three backup copies of the data is made and is stored in three distinct Data Centers. The locations of these Data Centers are highly classified and only few high level employees have access to it to ensure that the data remains protected from external interference.

Google itself uses several backup methods for ensuring the recovery of data. Google uses tape cartridges for data backup that can be transported to different external locations for long term safe keeping. By using this backup, Google was able to recover the contents of the Gmail accounts affected by the security breach. It took 4 days for Google to fully recover all of the lost data for the impacted 150,000 users (Srivastava, H., 2014).

Cloud computing is a great option because it makes the data easily accessible and available. But Security challenges are a big concern in cloud storage. Google had a very substantial security breach strategy because of which they handled the situation and recovered a massive amount of the lost data in a matter of days. But the faulty security bug should have been monitored before it caused any damage. Hopefully, Google takes this into consideration and avoids any future mishaps.

Alternative strategies and methods for enhancing security in cloud computing

In this section, we present security methods that are available for ensuring the privacy of data in cloud computing for organizations.

Alternative strategies and methods for enhancing security in cloud computing

In this section, we present security methods that are available for ensuring the privacy of data in cloud computing for organizations.

A. Cryptography (Encryption)

Cryptography is a good approach for data privacy in cloud computing. It provides secrecy of the data and information so that anyone who is not having access to that information cannot illegally use it.

As stated by Dorothy E. R. Denning 1982, Cipher is the secret technique of writing where the plain text is converted into cipher text. This process of converting simple text into cipher text is known as encryption. And the process of converting cipher text into simple readable text is known as decryption (Robling 1982).

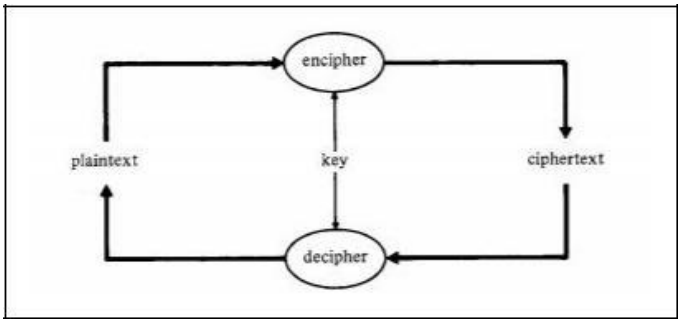

Fig. 2. Process of Cryptography

Only the people having access to the key can cipher or decipher the data. In the way the organization has full control over who has the right to access the stored data and information.

When anyone wants to access the stored data, the system will check the privacy policies and reveal the data only when the privacy policies are met and satisfied. Otherwise if the policies are not satisfied, the access will not be granted. And hence and the data remains secure from any external interference (Takabi, H., 2010).

Although encryption is a suitable approach for data security but a disadvantage is that sometimes it may happen that encryption can lead to problems related to indexing and query.

However, Deyan Chen, and Zhao Hong 2012, informs that in June 2009; IBM developed a homomorphic encryption scheme. This encryption scheme processes the data without decrypting it (Chen, D., 2012).

B. Access Control Mechanism

Access controls are used to ensure that the direct access to data stored in the cloud is authorized. It provides user identification so that no one can acquire the access rights of someone else.

According to Te-Shun Chou 2013, access control mechanism is carried out using authentication and authorization procedures. All the information in the cloud storage should specify the access rights of users so that the stored data is protected from unauthorized users (Chou, T.-S., 2013).

The system's access control mechanism enforces the security policies of the system. When the organizations apply access control mechanisms, it provides assurance that only the authorized users will have access to their data (Robling, 1982).

Two of the most common tools that are used to restrict the authorized access are; Firewalls and Intrusion Detection Systems. They are used to monitor any malicious activities and restrict the access from any untrusted resources.

Moreover, different standards of authentication such as eXtensible Access Control Markup Language (XACML) and Security Assertion Markup Language (SAML) are also used.

These tools are used for controlling the access to different cloud based applications and data.

SAML focuses on the authorization and authentication between the cooperating entities where as XACML focuses on determining the authorization decisions (Chou, T.-S., 2013).

Although access control is a great method to ensure data privacy but sometimes it can be costly and time consuming.

C. Some other approaches

a. Real-Time Alerting and Blocking:

It is important to monitor all the access activities to detect any data leakage, unauthorized transactions, or system attacks. Any attempt of accessing the unauthorized data terminates the session of the user immediately. Predefined and custom security policies should be used to detect any excessive privileges abuse. Activity based user profiles helps to detect any authorized access to confidential data and monitor the activity of the highly privileged users.

b. Blocking Malicious Web Requests:

Web applications are always open to input injection attacks therefore it is essential to use a web Application Firewall that will detect and block any malicious attacks. It is also important to monitor the activities of the users.

c. Scanning & Mitigating Vulnerabilities:

Recognizing the vulnerabilities that might expose your data to malicious attacks is necessary. Malwares exploit data vulnerabilities which makes them an easy target. Vulnerability assessment tools must be used to identify the security vulnerabilities and misconfigurations in the cloud. The risk scores should be calculated as it helps to prioritize risk, and manage vulnerabilities.

Perceived findings

After thoroughly analyzing the security breaches and strategies for enhancing the security in cloud computing, it is discovered that by combing multiple approaches and strategies such as Access control mechanisms along with cryptography, the overall security challenges currently being faced in cloud computing can be minimized drastically.

The security breaches that occurred at Google and Drop Box were a result of inadequate security planning. These threats could have been prevented easily if necessary precautionary measures would have been taken.

By combining these strategies together, the defense mechanisms can be improved against the threats and challenges of cloud computing. There are a number of other alternative strategies and approaches as well that can be combined with these to provide a more secure clod computing environment.

Conclusion and future scope

Cloud computing is rapidly enhancing and transforming the way Information Technology is being utilized. We are all well aware of the fact that nothing is perfect; there is always some room for improvement in every technology.

Although Cloud computing is an evolving technology but still it is lacking some features. With the passage of time, the increase in the amounts of data is massive and so are the security requirements.

Security is a critical challenge in cloud computing. Identity management mechanisms as well as authentication of users and services can be applied to cloud computing for overcoming the future security concerns.

The sensitive data should be separated and classified as highly confidential. State of the art firewalls and other privacy protection mechanisms should be set up to stop any unauthorized access to the organization's cloud storage resources.

The organizations who are using cloud computing can also apply a privacy-aware framework to make the employees aware of the privacy policies. All the security breaches should monitored effectively and immediate actions should be taken to ensure that the crucial data remains protected. In future, more detailed work can be improvised in this direction.

Acknowledgments

The author would like to thank her supervisor Dhanalakshmi Venugopal, for always motivating her to push the limits and achieve her goals.

References

Takabi, H., Joshi, J. B. & Ahn, G.-J., (2010). Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy, Issue 6, pp. 24-31.

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M., (2010). A view of cloud computing. Communications of the ACM, 53(4), pp.50-58.

Cachin, C., Keidar, I. & Shraer, A., (2009). Trusting the cloud. Acm Sigact News, Issue 2, pp. 81-86.

Barron, C., Yu, H. & Zhan, J., (2013). Cloud computing security case studies and research. Proceedings of the World Congress on Engineering, Volume II, pp. 1-5..

Srivastava, H., (2014). Research Opportunities and Challenges in Cloud Security. Communication, Cloud and Big Data: Proceedings of CCB.

Robling Denning, D.E., (1982). Cryptography and data security. Addison-Wesley Longman Publishing Co., Inc..

Chen, D. & Zhao, H., (2012). Data security and privacy protection issues in cloud computing. Computer Science and Electronics Engineering (ICCSEE), Volume 1, pp. 647-651.

Chou, T.-S., (2013). Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology (IJCSIT), Volume 5, pp. 79-88.