Security Challenges in the Sustainable Cloud Computing along with Big Data Analytics

B Kiruthika[1], Dr. B. Srinivasan[2], Dr. P. Prabhusundhar[3]
[1]Research Scholar in Computer Science
[2]Associate Professor in Computer Science,
[3]Assistant Professor in Computer Science,
Gobi Arts & Science College (Autonomous), Gobichettipalayam.
[1]kiruthikabalu@gmail.com
[2]srinivasanb@gascgobi.ac.in
[3]drprabhusundhar@gascgobi.ac.in

ABSTRACT

Big Data and cloud computing are two important advancement of technologies in the recent years, which enables computing resources to be provided as Information Technology services with high efficiency. Predominantly cloud computing is a powerful technology to perform massive-scale and complex computing. Also it provides a reliable, fault-tolerant, available and scalable environment to adapt with big data distributed management systems. Substantial growth in the varied volumes of big data generated through cloud computing has been observed. Cloud computing plays a vital role in protecting data, applications and its infrastructure with the help of technologies, controls, and big data tools**.** Within the context of this paper, the fundamental focus is on security issues that arise between big data and cloud computing such as PC security, system security, data and information security.

KEYWORDS

Cloud Computing, Big Data, Security, Big Data tools, Big Data Analytics, API (Application Programming Interfaces), CSP (Cloud Service Provider)

1 INTRODUCTION

The ever increasing demand to store and process more and more data either in structured or unstructured format rise from the domains such as social media, Internet of Things (IoT), multimedia, finance, science, and government. Systems that support big data, and host them using cloud computing, have been developed and in use currently. Big Data brings many opportunities along with some challenges from data collection to visualization. There exists large number of Big Data techniques and technologies to overcome all these obstacles, whereas cloud computing has become a pioneer and facilitator for the emergence of Big Data. Cloud computing is one of the major shifts in IT and service for enterprise applications and has become a powerful architecture to perform large-scale and complex computing. Therefore, hybrid of big data with cloud computing can become a solution for data storage needs that growing time to time and also to manage and secure the data from attack or loss. In this paper, we come up with some security issues and system of approaches in providing security which can also process large and massive amount of data.

2 BIG DATA AND ITS ADVANTAGES

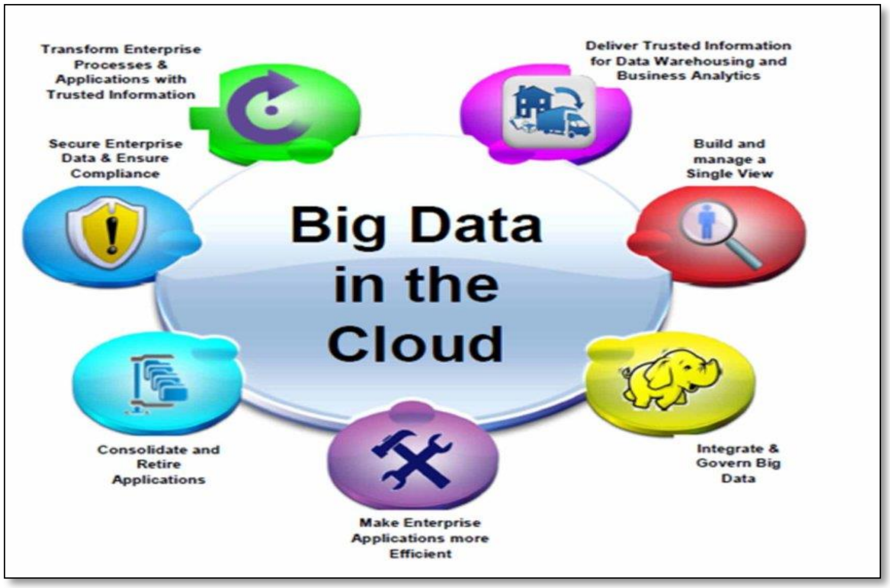
Big Data analytics has revolutionized the field of IT, enhancing and adding added advantage to organizations. Big data is generally collected through search engines, social media platforms, mobile phones, service networks, public records, and connected devices. This huge datasets may be placed in a structured (relational data), unstructured (media logs), or semi-structured (XML data) database for further processing and analysis. Big data are often characterized by 3Vs: (a) data are numerous (volume), (b) data cannot be categorized into regular relational databases (variety), and (c) data are generated, captured, and processed rapidly (velocity). Moreover, big data is transforming healthcare, science, engineering, finance, business, and eventually, the society. Like any other technology Big Data also comes with its own benefits like better decision making, cost reduction of business processes, fraud detection using machine learning and AI techniques, increased productivity, improved customer service and increased agility.

3 NEED OF CLOUD COMPUTING

Cloud computing is computing based on the internet. Cloud computing is a type of technology that provides remote services on the internet to manage, access, and store data rather than storing it on Servers or local drives. Here the data can be anything like Image, Audio, video, documents, files, etc. This technology is also known as Serverless technology. The advantages of cloud computing include virtualized resources, parallel processing, security, and data service integration with scalable data storage.

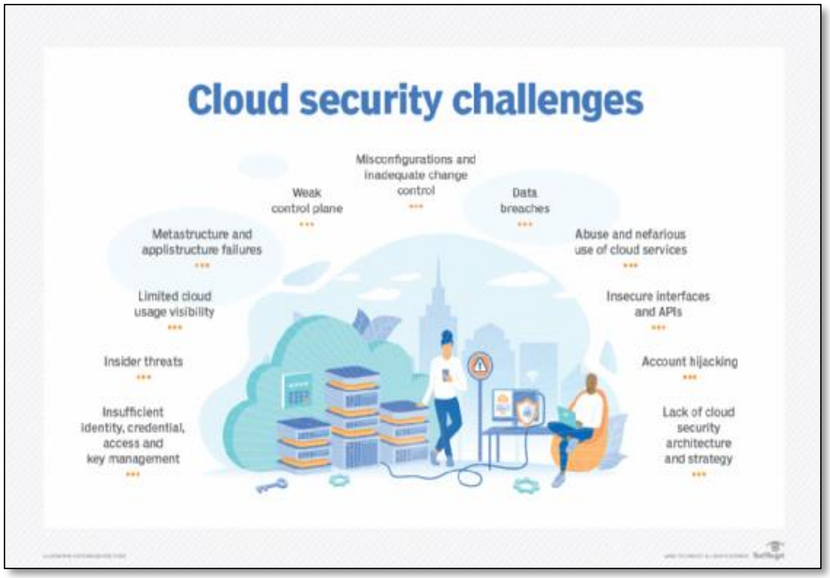
3.1 Big Data in Cloud Computing

Big data and cloud computing are two distinctly different ideas, but the two concepts had become so interwoven that they are almost inseparable. The implementation of big data needs a big server which requires a high cost and high maintenance. Cloud server can become a solution to tackle this issue by providing a reliable, fault-tolerant, available and scalable environment.


Big Data in the Cloud
Transform Enterprise Processes & Applications with Trusted Information
Deliver Trusted Information for Data Warehousing and Business Analytics
Secure Enterprise Data & Ensure Compliance
Build and manage a Single View
Consolidate and Retire Applications
Integrate & Govern Big Data
Make Enterprise Applications more Efficient

4 SECURITY THREATS IN CLOUD BASED SERVICES

There is no doubt that Cloud Computing provides various advantages like improved IT efficiency, flexibility and scalability but there are also some security issues in cloud computing. According to Cloud Security Alliance (CSA), over 70 percent of the world's businesses now operate at least in part on the cloud. Since cloud server using third-party service, data security is one major challenge and it needed to get full pay attention.


Cloud security challenges
Misconfigurations and inadequate change control
Weak control plane
Data breaches
Metastructure and applistructure failures
Abuse and nefarious use of cloud services
Limited cloud usage visibility
Insecure interfaces and APIs
Insider threats
Account hijacking
Insufficient identity, credential, access and key management
Lack of cloud security architecture and strategy

Here we discuss the top cloud security threats and concerns in the market today.

4.1 Data Loss

Data Loss is also known as Data Leakage. Data on cloud services can be lost through a malicious attack, natural disaster, or the service provider makes the data inaccessible (data wipe). If the security of cloud service is broken then the chances for hackers to get full control over the database is high which results in stealing the sensitive data or personal files stored in it. Moreover, losing vital and critical information will be devastating to businesses that don’t have a recovery plan in place.

4.2 Interference of Hackers and Insecure API’s

Cloud services are all about Internet and the easiest way to communicate and customize with cloud by suing the exposed components API (Application Programming Interfaces) and CSP UI’s. The role of API is not only to fit the business needs with cloud services, but they also authenticate, provide access, and effect encryption. So it is necessary to protect the Interfaces and API’s used by an external user in the cloud environment. The vulnerability of an API lies in the communication that takes place between applications. Even though this can help programmers and businesses, they also leave exploitable security risks. Few services that are available in the public domain are also vulnerable part of Cloud Computing because it may be possible that these services can be accessed by some third parties. It helps the hackers to easily hack or harm the data.

4.3 Hijacking of User Accounts

Cloud account hijacking is the most serious security issue, which means the disclosure or accidental leakage of cloud account that is critical to the operation, administration or maintenance of a cloud environment. Other methods of hijacking include scripting bugs and password reuse, which allow hackers to steal the credentials easily. If somehow, these highly privileged and sensitive accounts of user or an organization are breached/hijacked, can cause massive consequences and also lead to service disruptions. The attackers now have full authority to perform unauthorized activities like remote access of sensitive data stored on the cloud; additionally, attackers can falsify and manipulate information through hijacked credentials. Phishing, keylogging, and buffer overflow all present similar threats. However, the most notable new threat – known as the *Man In Cloud Attack* – stealing user tokens which are used to verify individual devices without requiring logins during each update and sync in cloud computing.

4.4 Changing Service Provider and Lack of Skill

Vendor Lock-In is also an important security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, an organization wants to shift from AWS Cloud to Google Cloud Services then they are various problems like data transfer risk, application transfer risk, infrastructure transfer risk and human resource knowledge risk. Also, it may be possible that the charges of AWS are different from Google Cloud, etc. While working, shifting to another service provider, needs an extra feature, how to use a feature, etc. are the main problems caused in IT company who doesn’t have skilled employee. So it requires a skilled person to work in cloud environment

4.5 Denial of Service (DoS) Attacks

This DoS attack occurs when the system receives too much traffic. Mostly this attack occurs in large organizations such as the banking sector, government sector, etc. Unlike other kind of cyber attacks, DoS assaults do not attempt to breach your security perimeter. Rather, they attempt to make your website and servers unavailable to legal users. In some cases, DoS is also used as a smokescreen for other malicious activities, and to take down security appliances such as web application firewalls. It requires a great amount of money as well as time to handle the data recovery.

4.6 Data Breaches

Data breaches remained the top cloud security threat all year around. A number of data breaches have been attributed to the cloud in recent years**.** A data breach can bring a company to its knees, causing permanent damage to its reputation, financial woes due to regulatory implications, legal liabilities, incident response costs and decreased market value.

4.7 Insider Threats

An attack from inside your organization may seem unlikely, but the insider threat does exist. The risks associated with employees (current/former) and others (contractors/partners) working within an organization's network are not limited to the cloud. Moreover, these insiders don't even need to have malicious intentions. Employees will misuse or access information such as customer accounts, financial forms, and other sensitive information using their authorized access in organization's cloud-based services. This can cause data loss, system downtime, reduced customer confidence and data breaches.

4.8 Malware Injection

The cloud computing infrastructure is susceptible to malware injection attacks. Malware injections are malicious scripts or code created by cyber attacker is injected into SaaS Software as a Service (SaaS), Platform as a Service (PaaS) and the Infrastructure as a Service (IaaS). This infected implementation act as "valid instances" and run as SaaS to cloud servers. Once an injection is executed and the cloud begins operating in tandem with it, attackers can now spy on the content, compromise the integrity of sensitive information by manipulation, and steal data.

4.9 Abuse of Cloud Services

The expansion of cloud-based services has made it possible for both small and enterprise-level organizations to host vast amounts of data easily. However, the cloud's unprecedented storage capacity has also allowed both hackers and authorized users to easily host and spread malware, illegal software, and other digital properties. These risks include the sharing of pirated software, videos, music, or books, and can result in immense consequences for the business. In certain cases this practice affects both the cloud service provider and its client. You can reduce your exposure to risk by monitoring usage and setting guidelines for what your employees host in the cloud. Cloud service providers have to be really diligent in detecting and mitigating such attacks with an incident response framework.

4.10 Misconfigurations

Setting up computing assets incorrectly ultimately results in misconfigurations, making them vulnerable to attacks. Unsecured data containers, unchanged credentials, disabled security controls, excess permissions, and disabled monitoring are among some examples of misconfigurations. Though some cloud aspects can be extremely complex, there are resources that can ease management and control. Automation as well as technologies should be embraced which can help scan for misconfigurations.

4.11 Lack of Cloud Security Strategy

As migrations become more and more mainstream, too many organizations jump into the cloud without the proper architecture and strategy in place. A company's security architecture is essential for operating within the cloud framework. Prior to making the leap to the cloud, customers must understand the threats they are exposed to, how to migrate to the cloud securely. Remember, it's not a lift-and-shift process whereas the security plans and models should always be kept up to date. Otherwise the cyber attacks can result in financial losses, reputational damage, and legal and compliance issues

4.12 Insufficient Authentication Management

Another major cloud security threats stems from an inappropriate credential protection, lack of automated cryptographic key, password and certificate rotation, absence of multifactor authentication and weak passwords. Businesses should practice strict identity and access controls for those who utilize the cloud services.

4.13 Limited Cloud Usage Visibility

It is an organization ability to have a visual of the cloud service and analyze whether the usage in the company is safe or not. Limited cloud visibility results in two key challenges, 1.*Unsanctioned app use* - employees use applications not permitted by IT, 2. *Sanctioned app misuse* - apps approved by IT are not used as intended. This includes users authorized to use the app, as well as unauthorized individuals accessing it with stolen credentials. This limited visibility, leads to lack of governance, awareness and security -- all of which can result in cyber attacks, data loss and breaches.

5 DATA SECURITY APPROACHES

Following security measures should be taken to ensure the security in a cloud environment:

Data Loss - Carefully reviewing the provider's back up procedures as they relate to physical storage locations, physical access, and physical disasters.

Interference of Hackers and Insecure API's - Avoiding API key reuse and using standard and open API frameworks.

Hijacking of User Accounts - Using defense-in-depth and IAM controls.

Data Breaches - Protecting data via encryption and having a strong, well-tested incident response plan. Also perform data input and output integrity routines

Insider Threats - Conducting security awareness training, fixing misconfigured cloud servers and restricting access to critical systems.

Abuse of Cloud Services - Monitoring employee cloud use and using cloud data loss prevention technologies.

Lack of cloud security architecture and strategy - Ensuring the security architecture aligns with business goals and objectives, developing and implementing a security architecture framework and implementing continuous security monitoring procedures.

Insufficient Authentication Management - Using two-factor authentication and rotating keys, removing unused credentials and access privileges, and employing central, programmatic key management

Limited cloud usage visibility - Developing a cloud visibility effort from the top down and mandating and enforcing companywide training on acceptable cloud usage policies.

6 CONCLUSION

The cloud is a complex environment that has opened up a whole new frontier with multitude of benefits for storage, access, flexibility, and productivity. It's also opened up a new world of security concerns. It is important, however, to be proactive when dealing with the threat and risks that come with cloud infrastructure. Becoming aware is step one in protecting your livelihood. By being aware of these top listed security concerns, we can build a cloud security strategy to protect the business. By applying the proposed approaches, cloud environments can be secured for complex business operations along with the speed and reliability aspects.

REFERENCES

[1]. Pedro Caldeira Neves, Bradley Schmerl, Jorge Bernardino and Javier Cámara, "Big Data in Cloud Computing: features and issues",International Conference on Internet of Things and Big Data, January 2016.

[2]. Ibrahim Abaker Targio Hashem,Ibrar Yaqoob, Nor Badrul Anuar, Salimah Mokhtar, Abdullah Gani and SameeUllah Khan, "The rise of "big data" on cloud computing: Review and open research issues", August 2014.

[3]. Finka Ria Damayant, Kemal Anshari Elmizan, Yoel Frans Alfredo, Zidni Nurrobi Agam and Antoni Wibowo, "Big Data Security Approach in Cloud: Review", 2018 International Conference on Information Management and Technology (ICIMTech).

[4]. Elmustafa Sayed Ali Ahmed and Rashid Saeed, "A Survey of Big Data Cloud Computing Security", December 2014 International Journal of Computer Science and Software Engineering.

[5]. P. Madana Mohan and B. Murali Manohar, "Challenges in Big Data Analytics and Cloud Computing", Volume 9, Issue 2, e-ISSN: 2347-4696.

[6]. Anitya Kumar Gupta and Srishti Gupta, "Security Issues in Big Data with Cloud Computing", Vol.5, Issue.6, pp.27-32, December (2017), E-ISSN: 2320-7639.

[7]. K.Shanmugapriya, M.Murugeswari and K.Suriya, "Security Issues Associated With Big Data in Cloud Computing" Vol. 6 (6) , 2015, 4952-4956, ISSN:0975-9646.

[8]. Venkata Narasimha Inukollu, Sailaja Arsi and Srinivasa Rao Ravuri, "Security Issues Associated With Big Data in Cloud Computing", Vol.6, No.3, May 2014.

[9]. Security Issues in Cloud Computing - https://www.geeksforgeeks.org/security-issues-in-cloud-computing/

[10]. Security Concerns for Cloud-Based Services - https://www.imperva.com/blog/top-10-cloud-security-concerns/

[11]. Cloud security challenges and how to combat them - https://www.techtarget.com/searchsecurity/tip/Top-11-cloud-security-challenges-and-how-to-combat-them

[12]. K. Chitharanjan and Kala Karun A, "A review on hadoop — HDFS infrastructure extensions.". JeJu Island: 2013, pp. 132-137, 11-12 Apr. 2013.

[13]. Zhao, Yaxiong , and Jie Wu. "Dache: A data aware caching for bigdata applications using the MapReduce framework." INFOCOM, 2013 Proceedings IEEE, Turin, Apr 14-19, 2013, pp. 35 - 39.

[14]. Ren, Yulong, and Wen Tang. "A SERVICE INTEGRITY ASSURANCE FRAMEWORK FOR CLOUD COMPUTING BASED ON MAPREDUCE."Proceedings of IEEE CCIS2012. Hangzhou: 2012, pp 240 –244, Oct. 30 2012-Nov. 1 2012.

[15]. A. Katal, Wazid M, and Goudar R.H. "Big data: Issues, challenges, tools and Good practices.". Noida:2013, pp. 404 – 409, 8-10 Aug. 2013.

[16]. A. Haripriya, A.P. Siva Kumar, "An Effective Patient Treatment Plan Recommendation with Predicted Treatment Time Using Hadoop", International Journal of Computer Sciences and Engineering, Vol.5, Issue.8, pp.155-158, 2017.

[17]. Ujjwal Agarwal, "Cloud Computing: BDaaS and HDaaS (Big Data as a Service and Hadoop as a Service)", International Journal of Computer Sciences and Engineering, Vol.5, Issue.11, pp.131-134, 2017.

[18]. Khan N, Alsaqer M, Shah H, Badsha G and Abbasi A, etal. (2018) The 10 Vs, issues and challenges of big data. ACM International Conference Proceeding Series.

[19]. Trovati, Marcello, Richard Hill, S. Y. Zhu and L. Liu (2015) Big-data analytics and cloud computing. Springer Berlin Heidelberg.

[20]. Mehta N, & Pandit A (2018) Concurrence of big data analytics and healthcare: A systematic review. International journal of medical informatics, 114: 57-65.

[21]. Buyya, Rajkumar, Kotagiri Ramamohanarao, Chris Leckie, Rodrigo N. Calheiros, Amir Vahid Dastjerdi, et al. (2015) Big data analytics-enhanced cloud computing: Challenges, architectural elements, and future directions. 2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS), pp. 75-84.

[22]. Yibin Li, Keke Gai,Longfei Qiu, Meikang Qiu and Zhao Hui "Intelligent cryptography approach for secure distributed big data storage in cloud computing," Information Sciences, vol. 387, pp.103-115, 2017.

[23]. K. Gai, M. Qiu and H. Zhao, "Security-aware efficient mass distributed storage approach for cloud systems in big data," in Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), 2016.

[24]. G. Manogaran, C. Thota and M. V. Kumar, "MetaCloudDataStorage architecture for big data security in cloud computing," Procedia Computer Science, vol. 87, pp. 128-133, 2016.

[25]. Popovic K and Hocenski Z, "Cloud computing security issues and challenges", (January 2015), pp.344–349.