Security and laws of Cyber / cloud Computing

[1]Saumya Kumar, [2]Warshit Poonia, [3]Harshita Jain, [4]Dr. Ritu Shrivastava

Dept. of computer science & Engineering
Sagar Institute of Research & Technology
Bhopal, Madhya Pradesh, India

Abstract: **Iot devices have spread everywhere, and their services have become widespread everyone can see their types and that is why the attackers attacks these iot devices and services and these types of cases are increasing rapidly so we need to step up and take cyber-defense seriously these articles point out the importance of the growth of cyber-threads and securities cyber threats today pose serious challenge due to rapidly changing advancements in technology. This paper focus on cloud computing, cyber security situation and details about the methods to protect the data and its approaches which are being used worldwide to get the maximum protection of data by reducing various risks and threats. Data which are available on cloud is very critically important for many applications but it also at the same time poses many risks by the data exposed to applications already having different loophole in its security.**

***Keywords*: Cyber Threats, Cloud Security, IOT Devices**

1)INTRODUCTION

Cyber threat is act that is consider as malicious. attackers look for steal, damage, or harm your data and social/digital life. Cyber threats incorporate malwares and viruses, social engineering, data breaches, DoS (Denial of Service) attacks, and other attacks. Lewis and Andrew (2002)

Delivering computing services via the internet that contain data needs to be protected from hackers, so this is done via cloud computing. When using cloud services, the privacy and security of data are of utmost importance. The confidentiality, integrity, and privacy of the data are of utmost importance for cloud computing. Numerous cloud service providers are applying various mechanisms and policies for that exact same location. Alharthi and others (2015).

We need to be aware because attackers are constantly coming up with new ways to access networks, programs, and data without authorization. They aim to compromise the confidentiality, integrity, and availability of information by choosing targets ranging from single people to small and medium-sized businesses to even global corporations. Komarov and others (????)

2)ADVANTAGES AND DISADVANTAGES

In present era as technology and the Internet have spread rapidly, cybercrime is also growing exponentially. Due to the widespread adoption of the internet and digital technologies, information technology security solutions are essential for all types of enterprises and organizations.

Have a look at some cybersecurity solutions which helps us to protect our personal and enterprise information. How it protects and enhances productivity, prevents crashing of websites, and support your IT professionals.

but there are some drawbacks too like The High -Cost of Cyber Security, the complicated nature of Cyber security, The need for constant monitoring, The Lifelong process as a nature of the field, Cyber security can be of massive risk. Hideshima and Koike (2006)

3)CIA TRIADS

A popular information security model called the CIA triad can direct an organization's actions and policies focused at protecting its data. The initials of the model stand for the three information security tenets rather than the American Central Intelligence Agency. - Whitman and Mattord

Confidentiality: Only authorized individuals and processes have the authority to edit or access the data.

Integrity: - Nobody should be able to alter the data, which must be kept in a correct state, whether unintentionally or maliciously.

Availability:- - Only authorized users should have access to data when they need it.

4)CLOUD ATTACK

First and foremost, lets understand what form a cloud cyber-attack.

Cyber-attack that targets storage-related service platforms a cyberattacker Attacks against services like SaaS, IaaS, and PaaS. which cloud attacks have been the biggest?

CAM4-2020 - In March 2020, a cloud cyber-attack targets CAM4, an adult live-streaming platform. 10.8 billion sensitive entries, or 7 TB of data, were exposed.

MICROSOFT-2019- Microsoft suffered a database breach in December 2019 that exposed 250 million records, including emails, IP addresses, and other information.

CAUSE: The server containing the vital data had been improperly configured. 149

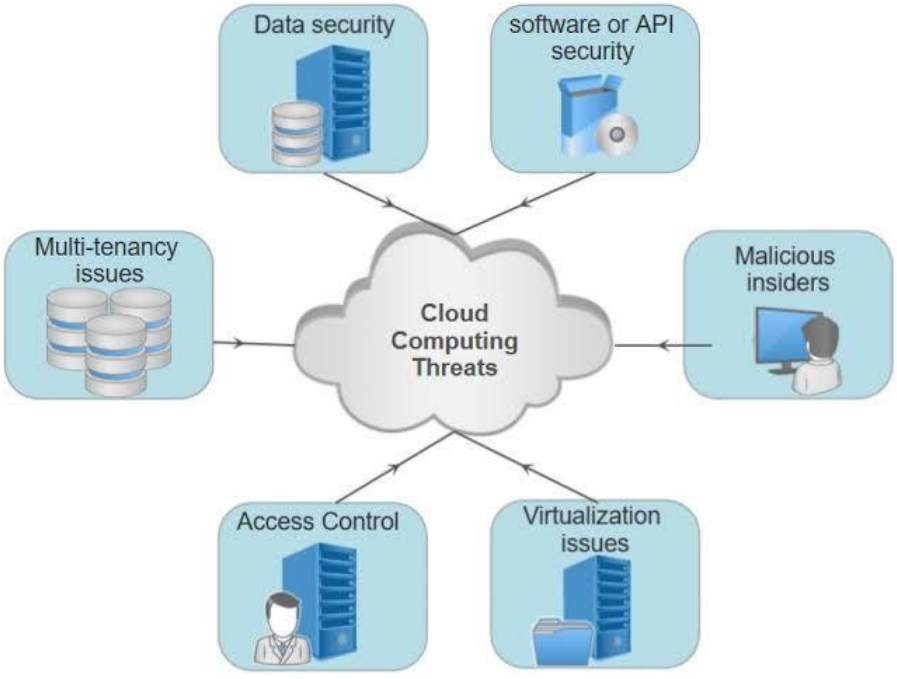
Cyberattacks against cloud computing are caused by:

According to McAfee, cloud data are more exposed than those on local servers. Mistakes among end users and cloud service providers (CSPs) further amplify these vulnerabilities.
1)SECURITY PROBLEMS
Failure of isolation: - when IT resources are shared through cloud computing they possess some risk of confidentiality of data. for reducing the problem of separating storage, we use multi-tenancy to help minimizing of requirement of separate storage. Saumya (2022)

5)PHISHING ATTACKS IN CLOUD
Users participate in phishing attacks by working on a bogus website that appears to be a legitimate one. In order to obtain the user's credentials, phishing websites are made. The other phishing scam uses email, with users receiving messages from the attackers. Email that was received appears to be genuine correspondence from a well-known source. These emails offer very little or no information and a link that can be clicked to learn more.
When the supplied bogus link is clicked, malware is downloaded and installed on the user's computer. According to Li et al. (2011), some of the cloud-based phishing attacks include:
LONGLINE PHISHING: - It is a brand-new kind of cloud attack in which the adversary exploits email to look for users' personal information. Grance and Mell (2011a)

6)DDoS ATTACK IN CLOUD COMPUTING
The well-publicized cyberattack known as DDoS (Distributed denial of services) targets cloud computing. In this cyberattack, many computers are deployed to attack a single target. Compromised computers are referred to as "zombies" here. When all the resources are used by unauthorized users owing to DDoS, legitimate users are prevented from accessing them.
DDoS uses the volumetric technique or the amplification technique. The volumetric strategy sends a massive amount of traffic into the network in an effort to consume bandwidth or cause resource exhausts.
In the amplification approach, the attacker uses the victim to boost traffic. Here, the attacked resource is used by the attackers. The bandwidth increased by a factor of more than 60 when the attacked botnet sent a DNS query of roughly 60 bytes to an open recursive DNS resolver, which returned a response message of up to 400 bytes.
Major DDoS attacks: - **ATTACK ON SPAMHOUS**
DDOS ATTACK TOOK PLACE ON BITBUCHET

7. CYBER THREATS LAWS
The IT Act regulates cybersecurity laws. Sections 43(a) through (h) of the Cyber Offenses and Cyber Contraventions Act impose penalties for (Sections 63–74).
According to a survey, rookie and overconfident attackers commit crimes most frequently, with many offences falling under sections 66A and above. Cybersecurity refers to the methods and technology used to prevent unauthorized access, crimes, and attacks on computers, networks, and data. Criminal acts like theft, defamation, fraud, forgery, identity theft, and other felonies can be committed online.



8)RESULT:
Every year, more people try to take advantage of weak corporate systems, which has led to an increase in cybercrime. Any cyberattack that uses cloud infrastructure to target platforms that provide storage, computing, or hosting services is referred to as a cloud cyberattack. Dowling and Mcguire (2013)

The use of cloud computing is growing daily. Nowadays, practically everyone who owns a smartphone uses the cloud in some capacity. significant use of cloud services for data storage. Most people keep some data in the cloud so they can access it from anywhere in the world. Because there is so much data saved in the cloud. What puts the security of cloud-stored data at risk? My paper's main focus is on security risks and threats to cloud-stored data, and I present a brief summary of several security concerns. We also attempt to address some of the threats to cloud computing. This article also provides a brief review of the hash function, block cypher, and stream cypher. These are some of the methods used in the cloud to authenticate users and encrypt data while it is in motion or at rest.
However, denial of service attacks, hostile insiders, malware, viruses, worms, and trojans, stolen devices, phishing and social engineering attacks, and web-based attacks are the most frequent types of attacks. And depending on the goal of the attack, the outcomes might easily be divided into four categories: cybercrime, cyber espionage, cyber war, and hacktivism.

9). DRAWBACKS

1)This technology is more expensive in ever field.
2) There is legally limited access for the users, but some users break those limitations for their own profits by illegal process.
3) These technologies take control of your life day by days.
4)Due to constant updates in technologies, a user needs to be continuously up to date about these technologies.
5) These technologies require patience in every way (learning, implementation).

10)CONCLUSION

We wish to address the main issue of cybercrime and believe there is a more effective approach to understand and be informed about online risks and attacks, as well as how to defend against them. a more beneficial, less intrusive method that allows us to be safe rather than victims.
We are fervently focused on making it happen because we are so passionate about it.

REFERENCES:

1. URL https://www.triskelelabs.com/blog/cloud-cyber-attacks- the-latest-cloud-computing-security-issues\#:\textasciitilde:text=Any\
2. %20cyber\%20attack\%20that\%20targets
3. URL http://www.information-age.com/technology/security/ 123457411/-dropbox-hit-by-zeus-phishing-attack(2011a)
4. (2011b) URL fromhttp://www.nist.gov/itl/cloud/ Alharthi A, Yahya F, Walters RJ, Wills GB (2015)
5. Ali, Mazhar SU, Khan AV, Vasilakos (2015) Security in cloud computing: Opportunities and challenges. Information sciences 305:357–383
6. Chickowski E (2013) URL http://www.darkreading.com/attacks-breaches/ sony-still-digging-its-way-out-of-breach/229402823
7. Hideshima Y, Koike H (2006) STARMINE: A visualization system for cyber- attacks. Proceedings of the 2006 Asia-Pacific Symposium on Information Visualisation 60:131–138
8. Komarov M, Davydiuk A, Onyskova A, Tkachenko V, Honchar S Requirements for a taxonomy of cyber threats of critical infrastructure facilities and an analysis of existing approaches. In: Systems, Decision and Control in Energy II, Springer, pp 2021–2021
9. Lewis J, Andrew (2002) Assessing the risks of cyber terrorism, cyber war and other cyber threats. Center for Strategic & International Studies, Washington, DC
10. Li T, Han F, Ding S, Chen Z (2011) Larx: Large-scale anti-phishing by retrospective data-exploring based on a cloud computing platform. 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN) pp 1–5
11. Mcguire M, Dowling S (2013) Summary of key findings and implications. Home Office Research report 75:2021–2021
12. Mell P, Grance T (2011a) The NIST definition of cloud computing. Special Publication pp 800–145
13. Mell P, Grance T (2011b) The NIST definition of cloud computing. Special Publication pp 800–145
14. Singh J (2014) Cyber-attacks in cloud computing: A case study. gov/ publi- cations/ PubsSPs 1:800–145
15. Saumya Kumar. "Privacy and security in cloud computing: A survey." *IJIRT* 8.11 (2022).
16. Tep K, Suntana B, Martini R, Hunt KKR, Choo (2015) A taxonomy of cloud attack consequences and mitigation strategies: The role of access control and privileged access management. 2015 IEEE Trustcom/BigDataSE/ISPA 1:1073–1080
17. Westervelt R URL http://searchsecurity.techtarget.com/news/ 2240172466/Phishing-attack-stolen-credentials-sparked-SouthCarolina- breach?asrc=EM_NLN_19698566\&track=NL-102\&ad=88
18. Whitman ME, Mattord HJ Yeboah-Boateng E, Osei (2013