IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Securing The Cloud: Diverse Perspectives On AI-Driven Solutions

Suman, Anjaly Chauhan

Department of Computer Science

IITM Janakpuri,New Delhi

Abstract

Cloud is a place where data resides in server at a distant location. All of the data is connected to the internet and we as a user are using cloud at a daily basis. As the internet is expanding every second, so is the cloud. Clients are dependent on the cloud service provider to ensure that their data which is handled in the cloud is secure. As the cyber security breaches is at rise the probability of a user's data to be breached and show up in black market is high. There are several methods that ensure the safety of data inside cloud. In this paper we concentrate on security that AI provides to keep cloud secure from security risks. As AI name suggests it learns from artificial intelligence that has been provided to it therefore it can learn new techniques and act according to it, this factor is important because security breaches are getting more and more sophisticated.AI can perform many tasks like vulnerability scan, various types of analysis which is important in a system which is very vast such as cloud.AI is important because the increasing volume, data, applications and the users on cloud makes a complex eco-system which has to be managed and analyzed, all of these tasks is hard to be done by human security analyst. Various security flaws can be sought out and unknown flaws can be reported using AI algorithms.

Keywords: Artificial Intelligence (AI), Security, Security threat, Cloud computing (CC), IoT(Internet Of Things)

I. INTRODUCTION

Cloud is a platform where users can store their data without having to have a physical form of storage to carry everywhere. Users can access this data from anywhere around the world with ease. With access to data from anywhere and information that is stored far away from a user point of view, there's an unease about how protected data really is? Security is an important aspect where data is encrypted and protected using several methods so that data breach or unauthorized access to data is not compromised. Companies are gambling more and more money into costly corporate firewalls, security analyzing which turn out to be useless against modern and more sophisticated cyber security risks. An aspect which arises in this situation is AI. IT industry is collectively working to fight back and prevent such sophisticated and severe attacks from happening, by improving many of the system designed to confront attacks and analyze the data affected. Increasing volume of

data and networking intersects with complex attacks, and AI can be used to keep things safe. Increasing volume of data and more complex networking makes it demanding for security personals to manage and analyze data and attacks. Data has to be managed and necessary steps have to be taken. AI or Artificial Intelligence can solve problems and it thinks by itself as a human does. The insights become more valuable and reliable as the more data patterns are analyzed by AI .AI gets more self-adjusted based on these patterns and using this information companies can automate tasks to secure their infrastructure. Using Algorithms to learn from data security can be greatly improved this method which is a subset of AI is known as Machine Learning. The more data which is analyzed my tracing user activities and log produced by system AI and Machine Learning can be improved to take security measures that can deal with situations where a human analyst is helpless.

II. CLOUD COMPUTING

Cloud computing refers to utilizing the internet to avail a range of services, encompassing data storage, hardware resources such as servers, databases, networking, and various applications[10-13]. With cloud computing, files can now be stored centrally in an archive instead of on individual hard drives or storage devices [10]. Whenever an internet user connects online, they gain access to applications and information. The adoption of cloud storage is widespread among individuals and businesses due to its ability to provide financial benefits enhance productivity, offer speed, reliability, and customizable options [9].

Security Threat in Cloud

Cloud security is essential for the users who have their data stored in cloud. User data is stored in multiple servers with cloud providers managing the data and security experts to look over the security of the data. On-premise data is more susceptible to data breach as the user data can be compromised using social-engineering and malware, user being less experienced in detecting security threats cannot handle the sophisticated forms of attacks. Cloud security is vital aspect for cloud providers. Storing of sensitive data such as credit card info. has to be followed certain regulatory requirements which has to be maintained by the cloud storage providers. Some of the threats include Distributed denial of service (DDOS), Account compromising, data breach, and service traffic hijacking. DDOS attacks enable hackers to overwhelm the servers with data request due to which server goes down due to too much load. Which lets the attackers to make users to unable to access their accounts and services? Users using cloud must also protect themselves as the login credentials stored in phones and devices can be compromised.

Cloud computing (CC) is poised for substantial and extensive growth, but it also faces significant challenges in terms of security and protection. The analysis is centered around the CIA (Confidentiality, Integrity, Authenticity) feature and the risks associated with cloud computing. Confidentiality, integrity, authenticity, and availability have been highlighted as the primary vulnerabilities by CC. Here, we briefly examine these concerns.

Fig 1. Cloud Computing Security Threats

Confidentiality is threatened by software vulnerabilities, external risks, and internal threats to client information. A significant security concern is the unlawful or unauthorized access to personal data by intruders targeting cloud service providers. Additionally, cloud systems in exposed locations face a heightened risk of external attacks due to their centralized hardware and software infrastructure. Moreover, data loss is an inevitable vulnerability in cloud agreements, stemming from human error, inadequate tools, and occasional access issues.

Integrity: Integrity threats encompass concerns regarding data fragmentation, inadequate client access controls, and vulnerabilities at the data level. Initially, there's a risk of customers misconfiguring virtual servers and poorly managing VM setups, potentially leading to exclusion from crucial security measures [10, 11]. This complex cloud challenge also involves customer connections that may impact data reliability due to asset adjustments. The second concern involves inadequate client access management, presenting various risks and allowing attackers to compromise data assets through improper influence and identity sharing.

Authentication: The authentication process ensures the originality and reliability of the equipment and its associated components. For example, various medical and healthcare facilities receive patient data, which, if accessed by unauthorized individuals, could complicate the patient's treatment [12].

Availability: is threatened by risks to transparency, the consequences of panel expansion, organizational inaccessibility, external equipment disruption, and insufficient recovery methods. Initially, attention is drawn to the panel, which incorporates basic adjustments' outcomes and the implications of various users accessing test environments. Infrastructure and cloud conditions negatively impact the usability of cloud services. The second concern revolves around system inaccessibility, encompassing DNS applications, properties, and device data transmission, presenting a ubiquitous external threat across all cloud iterations. Thirdly, physical disruptions to institutions specializing in wide-area networks (WAN), cloud users, and IT service providers pose a threat. Fourth, inadequate recovery mechanisms, such as ineffective failure recovery, affect the time and efficacy of recovery processes in the event of a disruption [13].

Establishing security attributes

Before connecting to the intelligent home system, a new IoT device must undergo a specific procedure. The IoT platform offers a range of cryptographic algorithms tailored to meet the confidentiality, integrity, and encryption requirements of the device's applications and systems. The trustworthiness of potential users is vital for ensuring the effectiveness and widespread acceptance of reliable IoT infrastructures and the numerous applications they support. Such trust is crucial due to the potential harm that stolen or misused private information can inflict on people's social, financial, and physical well-being. Ensuring proper security implementation is essential to address potential safety hazards. This measure is critical in safeguarding the

smart home against various security threats. An incident involving forged or tainted data can disrupt the surveillance system's operations, as decisions made based on false information may not achieve the system's intended objectives, such as reducing energy consumption. The underlying reasons for such an attack include:

Intentionally configuring an IoT system in a dubious manner leads to the generation of inaccurate data. For example, there might be a false increase in the overall power consumption. IoT devices may process data deceitfully, manipulating variables like electricity usage. Another risk is the manipulation of data through Multi-Hop Interaction via a compromised IoT Gateway. Additionally, without encrypting the data source through a robust protocol like IPsec, IoT devices connecting to the same network are vulnerable to identity theft and IP spoofing attacks.

Relationship between Cloud, AI and IoT

The IoT environment facilitates the creation of more inventive applications and these applications can leverage server less computing to enhance their design.IoT also enhances upcoming systems such as electric vehicles and micro-grids. Perspectives on the contribution of the triumvirate to the progression of cloud computing in Artificial Intelligence: It has the potential to decrease resource consumption and carbon emissions. It can also predict and mitigate anxiety associated with errors.AI can identify and rectify errors during software encoding.

AI has also impacted safety by aiding experts in detecting network anomalies through the analysis of user behavior and habits. Safety professionals can now utilize AI-generated network data to identify vulnerabilities and prevent malicious attacks [15]. AI will enhance traditional security solutions in the following ways:

- Advanced AI-powered security tools will be employed to monitor and respond to security events.
- Modern firewalls integrate machine learning technologies to swiftly identify and eliminate potentially malicious network traffic patterns [14, 15].
- Security experts can leverage AI's natural language processing capabilities to forecast the origins of cyber threats and assist in vulnerability analysis.
- AI facilitates the screening and statistical analysis of internet traffic to identify malignant risks.
- Enhanced security measures and authorization protocols ensure preferential access.

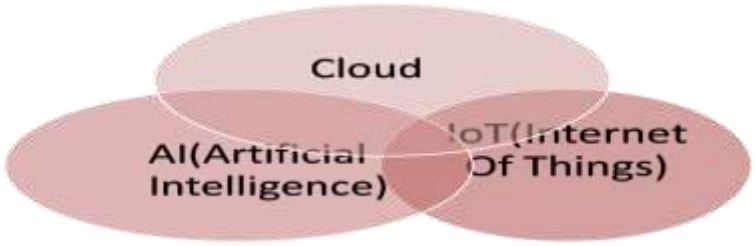

Fig 2.Understanding the evolution of cloud computing.

II. LITERATURE REVIEW

The security and privacy concerns with cloud computing are covered in this section. Because cloud computing transmits and hosts its capabilities over the Internet, it is a fairly vast field in and of itself. It charges appropriately and offers services to suit the needs of the customers. People are beginning to rely on the Cloud, and businesses can now readily hire Cloud services, which make the Cloud essential. Literature Review Cloud Security analysis Organization uses various cloud services as IaaS, PaaS, SaaS and the models like public, private, hybrid. These models and services have various cloud security issues. Each service model is associated with some issues.[1]. This is the one of the major concerning issue in an organization because it releases the confidential information of an organization in open. Clouds are not like a private network; they have more interfaces than private network. So, hackers and attackers have advantage of exploiting the API, weakness and may do a connection breaking [2]

E. K. Subramanian et al. [16] studies that used supervised and unsupervised machine learning approaches for cloud security and intrusion detection, such as decision trees, neural networks, support vector machines, and other techniques. Although they haven't been expressly investigated for cloud security, deep learning techniques like convolutional neural networks (CNNs) have been investigated for related cyber security applications. In summary, the research underscores the promise of machine learning, particularly sophisticated deep learning models, to improve cloud security solutions. However, it also points out a limitation in using CNN models directly for this purpose.

Another paper that is about artificial intelligence in cloud computing security is by Avinash Ganne at al.[17], the application of conventional machine learning models for cloud security is examined. Convolutional neural networks (CNNs) are shown to have the ability to detect threats and anomalies more accurately than classic ML techniques.

Nita, S. L., & Mihailescu, M. I. et al.[18] examines the effectiveness of Artificial Neural Networks (ANNs) in reducing security risks, including intrusion detection, malware detection, DDoS assaults, and authentication, providing a comprehensive understanding of ANNs' potential in cloud security.

S Kavitha et al.[19] exploring the nexus of IoT, cloud computing, and AI, the authors offer creative solutions to security issues that arise with cloud-based IoT systems. In order to strengthen the integrity and confidentiality of data saved and transferred via IoT devices in cloud infrastructures, the article proposes proactive strategies for threat identification and mitigation by utilizing AI techniques like machine learning and anomaly detection.

Wu, Han, Wang, and Shengli's et al.[20] study explores the use of Artificial Intelligence (AI) in improving security in the Internet of Things (IoT). They analyze various AI methodologies, including machine learning, deep learning, and natural language processing, and discuss their strengths, limitations, and future directions.

Hassan Rehan et al.[21] paper explores the need for robust security measures in cloud environments, utilizing AI algorithms for real-time threat detection and anomaly identification. It highlights the transformative potential of AI in mitigating security challenges and discusses ethical and regulatory considerations for its implementation in IoT security.

III. ARTIFICIAL INTELLIGENCE

The cloud is increasing itself as the data increases and sheer increase in the volume of devices, user's, servers which makes it hard and complex for the human security analyst to keep track of all the records in case of data breach. Cyber attacks are getting more and more sophisticated and severe over the years. IT industry is working to improve its capability to fight back in case of such attacks to happen. One avenue where experts are exploring to improve the capability of cyber security is by the use of Artificial Intelligence and Machine Learning. AI and Machine Learning can play a major role in elevating the capability of security in Cloud. AI is a program that can think itself using logic and solve problems just like a human. Machine Learning being a derivative of AI uses algorithms to learn from data units provided to it. It analyzes data and learns the more the data more the pattern it learns. AI and Machine Learning can provide faster response to threats which means before any serious harm done the threat can be neutralized and will be analyzed. Automated AI cloud security uses behavioral analysis on the user to analyze the pattern for threat to happen and take counter measures

against it. Adaptive capabilities of AI and Machine learning in hand will be efficient cloud security against cybercriminals. Data injected will impact the number of patterns processed by Machine Learning.

IV. ADVANTAGES OF USING AI IN CLOUD SECURITY

Blocking and Detection of threats Artificial Intelligence can detect vulnerability based on known problem rules known by it and can determine response. Whenever AI detects inconsistencies in framework it warns user or closes out the particular user out. New rules can be facilitated to the system so that automated process can handle threats more efficiently. Event Prediction With appropriate data, machine learning can be used to predict future events. Event prediction is critical in business as the upcoming change in the market can have a major impact in how the business has to strategize their marketing. In cyber security event prediction can assist in about potential threats and how it will impact the organization. This is calculated by observing the data in and out of the protected endpoints. Event prediction will reveal about how and from where the threats are about to happen. Knowing about the threats beforehand will let the organization to prepare for similar events and helps to reduce the time between detection of threat and remediation. With enough data this approach can detect threats based on known behavioral patterns.

Big Data Processing and Self-handling Security Due to increase in data which increases in every second it is impossible for a human security team to deal with the massive data. But using machine learning the massive amount of data can be churned to detect potential threats. The more data processed, the more it understands pattern for better detection. Automated detection and Action Along with predictive models, automated tasks can be done through AI -it is capable of analyzing and reacting to certain events.AI can respond to threats instantly rather than waiting for data to get through security team and make a decision. By utilizing such a system companies can detect and deal with the threats more effectively and efficiently.AI can do things like lock out users or prevent users, block out traffic through certain ports. Monitoring and alerts AI can learn through algorithms to detect events and monitor behavioral activities of users in case of any suspicious behavior AI alerts the security crew. Companies combine monitoring with automation to deal with threats and react to the problem in more efficient way.

Vulnerability Detection even if the cloud technologies are secure on the backend and in server side, it doesn't mean that it is safe from potential threats. With attacks being more and more sophisticated security can be a problem and multitudes of other vulnerabilities can pose a problem. Zero-day vulnerabilities can pose an issue if the system is not patched as soon as possible. Therefore, AI and Machine learning can be used to detect possible vulnerability that can be exploited.

V.CONCLUSION

The increasing in cyber security threats modern advancements have to be made in the field of security in cloud and increasing data is complex and hard for a human to look over therefore advancements in security for cloud using AI and Machine Learning will benefit organizations in long run.AI and Machine Learning will prove to be an important asset to the security of the data held in cloud. As a result, the cyber threats can be detected and analyzed before causing much harm. Cyber-attacks are getting sophisticated day by day so attacks will continue but AI and ML will be able to automate tasks using which the gravity of attacks can be reduced and future attacks can be avoided

References

[1]. Garima Gupta, P.R. Laxmi and Shubhanjali Sharma (Cloud Security Issues and Techniques)

[2]. Akhil Behl (2011), Emerging Security Challenges in Cloud Computing (An insight to Cloud security challenges and their mitigation).

[3]. Stefan, H.; Liakat, M. Cloud Computing Security Threats and Solutions. J. Cloud Comput. 2015, 4, 1.

[4]. Fauzi, C.; Azila, A.; Noraziah, A.; Tutut, H.; Noriyani, Z. On Cloud Computing Security Issues. Intell. Inf.Database Syst. Lect. Notes Comput. Sci. 2012, 7197, 560–569.

[5]. Venkatraman, S.; Mamoun, A. Use of data visualization for zero-day malware detection. Secur. Commun. Netw 2018, 1–13.

[6]. Shamshirband, S.; Chronopoulos, A.T. A new malware detection system using a high performance-ELM method.

[7]. Abdurachman, E.; Gaol, F.L.; Soewito, B. Survey on Threats and Risks in the Cloud Computing Environment.

[8]. Wani, A.; Rana, Q.; Saxena, U.; Pandey, N. Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques

[9] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial intelligence for securing IoT services in edge computing: a survey," Security and communication networks, vol. 2020, 2020.

[10] R. S. Chunduri and N. Mazher, "Sas Viya 4.0 Deployment in Cloud."

[11] R. S. Chunduri and N. Mazher, "SEIBEL IP. 22X DEPLOYMENT IN CLOUD SYSTEMS

[12] A. Grusho, M. Zabezhailo, A. Zatsarinnyi, and V. Piskovskii, "On some artificial intelligence methods and technologies for cloud-computing protection," Automatic Documentation and Mathematical Linguistics, vol. 51, no. 2, pp. 62-74, 2017.

[13] U. F. Mustapha, A. W. Alhassan, D. N. Jiang, and G. L. Li, "Sustainable aquaculture development: a review on the roles of cloud computing, internet of things and artificial intelligence (CIA)," Reviews in Aquaculture, vol. 13, no. 4, pp. 2076-2091, 2021.

[14]Praveen, S.P., Rao, K.T., Janakiramaiah, B. “Effective Allocation of Resources and Task Scheduling in Cloud Environment using Social Group Optimization” ,Arabian Journal forScience and Engineering, 10.1007/s13369-017-2926-z 6.

[15]Pravin Kshirsagar, Dr. Sudhir Akojwar, “Classification and Prediction of Epilepsy using FFBPNN with PSO”, IEEE International Conference on Communication Networks, 2015.

16. Subramanian, E. K., & Tamilselvan, L. (2019). A focus on future cloud: machine learning-based cloud security. Service Oriented Computing and Applications, 13(3), 237-249.

17. Asharaf, Z., Ganne, A., & Mazher, N. (2023). Artificial Intelligence in Cloud Computing Security. Research Gate.

18 Nita, S. L., & Mihailescu, M. I. (2018, June). On artificial neural network used in cloud computing security-a survey. In 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-6). IEEE.

19. Kavitha, S., Bora, A., Naved, M., Raj, K. B., & Singh, B. R. N. (2021). An internet of things for data security in cloud using artificial intelligence. International Journal of Grid and Distributed Computing, 14(1), 1257-1275.

20 Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: A survey. Ieee Access, 8, 153826-153848.

21 Rehan, H. (2024). AI-Driven Cloud Security: The Future of Safeguarding Sensitive Data in the Digital Age. Journal of Artificial Intelligence General Science (JAIGS) ISSN, 3006-4023.