European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 06, 2020

Leveraging AI for Secure Public Cloud

DIVYA SREE REDDY CHINTA[1], Dr. Saikat Gochhait[2]

Symbiosis Institute of Digital and Telecom Management, constituent of Symbiosis International (Deemed University)

Abstract: The enormous volume of applications on and the requirement of massive infrastructure to provide services has requisite Enterprises to move towards Cloud Computing. Hosting applications on Public cloud have various advantages such as reduced cost and scalability; however, the security concerns pertain. A data breach can create mistrust among customers and impact the company's brand and lead to financial losses. Subsequently , the need to secure the applications on cloud is increasing and enterprises need to employ best practices and work with their security teams and identify ways to incorporate advanced technologies such as Artificial Intelligence to utilize its capabilities to Identify threat, mitigate risks and predict upcoming issues and counter them on time.

The volume of applications on Public cloud are rapidly increasing and the cloud ecosystem is complex and need to be safeguarded by security teams. Also, security is a major concern for cloud migration and early detection of threats and vulnerabilities is important, Application of Artificial Intelligence is of dire need to identify the threats faced in cloud computing and safeguard the security of enterprise applications. This paper proposed a framework for leveraging AI for public cloud computing to identify threats and vulnerabilities in cloud applications. This paper further discusses the applications of AI for cloud security practices.

Problem:

Cloud Adoption has accelerated over the past few years; however, security risks of cloud computing have become a top priority for Enterprises. With Sophisticated criminal attacks, the cloud computing is at stake and with the void for lack of resources and expertise the security issues remain unresolved and resulting in insecure interfaces and data security concerns. In this paper, we will discuss the security challenges faced in public cloud and application of AI to face the security concerns.

Introduction:

Technologies have been constantly enhancing from the past decade and, businesses are attempting to find ways to limit expenditure and increase revenues by leveraging technologies such as AI and Cloud computing. Cloud vendors provide 3 major categories of cloud computing services: Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS).

Cloud Deployments are provided through public cloud, private cloud, Hybrid cloud depending on enterprise objectives and requirements. With an increase in the amount of data and imperative needs for remote access to data, Enterprises have started to move towards Cloud connectivity and storage.

Although cloud computing in its different structures has been around for a couple of years, the uses of the cloud are changing according to the organization's needs. Associations have started the utilization of the cloud computing worldview inside to improve IT administration conveyance and cultivate advancement. Some Telecom vendors are conferring a few services, for example, network data backup and in a couple of occurrences are partnering with driving cloud organizations to both exchange their contributions or offer foundation and site hosting services. The adoption of cloud has helped organizations reduced cost, increases scalability, provide business continuity, and flexibility of work practices. As the data is moving away from the organization’s network perimeter, the security concerns are increasing and hence companies have started to prioritize cloud security.

Cloud security uses applications, controls and various policies to protect the cloud Infrastructure to provide a secure environment . Cloud computing has grown to be a need for corporations searching for ways to advance enterprise innovation. To support the growth and secure systems, the need to use predictive technologies such as Artificial Intelligence is imperative to combat the increasing cloud cyber-attacks.

Literature Review:

- Jaydip K., (2019) Cloud Computing Security Issues and Its Challenges: A Comprehensive Research. International Journal of Recent Technology and Engineering
- Ahmed A., (2016) Privacy and security are concerns for cloud Adoption. Cloud Integrity, protection and privacy should be given priority to ensure secure services by cloud vendors
- Rajesh Y., Anand S. A Critical Review of Data Security in Cloud Computing Infrastructure. International Journal of Advanced Studies of Scientific Research
- Olasupo A., and Sanjay M. (2018) Cloud Computing Security: Issues and Developments. .Proceedings of the World Congress on Engineering
- Takahiko K., Murray J., Theophilus A, (2017) To cloud or not to cloud: how risks and threats are affecting cloud adoption decisions. Information and Computer Security

- Yudong L., Shuai X., Han W., Xu An W. (2019) New provable data transfer from provable data possession and deletion for secure cloud storage

- David S. (2017) Artificial intelligence is best leveraged for specific types of applications such as fraud detection, predictive marketing, machine monitoring , and inventory management.
- Jun Feng T., Hao- Ning W. (2020) An efficient and secure data auditing scheme based on fog-to-cloud computing for Internet of things scenarios

Why move to Public cloud:

As per Gartner research, services of public cloud market is estimated to reach $302 billion. Although few companies are hesitant to move towards public cloud, many organizations have adopted public cloud. The major highlight of public cloud is the improved security. Large public cloud vendors have expert cyber security teams that provide security to client applicants with market leading tools. Additionally, cloud0native have advanced security services and security innovations are increasing for cloud-based solutions. Furthermore, with cloud computing, flexibility and scalability increases with various options (ex: partly on-premise and partly on the cloud, multi-cloud vendors, all-in-one cloud). According to NetEnrich 2019, 68% of IT departments are using public cloud services to store data. With all the added advantages, public cloud is less expensive than private cloud, however, the costs can be variable dependent on workload. Companies eyeing a move to the public cloud can take advantage of the solutions and applications that are booming in market to smooth the transition and support their operations.

Public Cloud Security Challenges:

- Public cloud services work on a shared model where the customer is held responsible for access control and to ensure security counter measures depending on the type of cloud service adopted. These security measures need to be constantly shifted with the changing threat landscape. Statistics from McAfee reveal that 24% of organizations miss high severity patches in their public cloud infrastructure.
- Shared security model between Cloud service provider and customer becomes yet another digital asset for enterprise's Security operations (SecOps) team to monitor which includes intrusion detection to patching vulnerabilities
- Misconfigurations in public cloud services has been a major reason for cloud data breaches in the past as per CSA report. These security gaps can turn in to a threat to organizations.
- Increasing applications on cloud and high number of vulnerabilities is becoming a concern to organizations in deciding the vulnerabilities to be patched

AI and Cloud Adoption trends:

The worldwide AI market is one of the quickest developing markets today. Gartner predicts that the business value of Artificial Intelligence will reach $3.9T in 2020. Cloud computing has demonstrated to be a critical factor in growing business. For newly established companies, cloud infrastructure adoption has enabled them to leap in advance of their competitor, huge numbers of whom have battled to incorporate cloud into their complex heritage frameworks.

Cloud computing initially emerged in the United States. The U.S. has been the leader in cloud adoption since 2015, However not all countries are on par with the U.S. It is expected that by 2022, cloud adoption for all other countries will lag behind the U.S. by 1 to 7 or more years according to Gartner and the expected that in 2022 14% of total IT spending will be on cloud services in USA.

As per Gartner research, Public cloud industry is estimated to grow 17 percent in 2020 to $266.4 billion. In 2019, public cloud industry was $227.8 billion. Without cloud computing, the present AI abilities would not have been present as AI depend on tremendous stores of premium data. Enterprises are in different states of their cloud adoption and have different cloud aspirations for future. McKinsey report has recently shown that more fewer than 15% of organizations have more than half of their applications on cloud and have benefited by the sophisticated security services provided by cloud vendors. Additionally, nearly 80% of organizations plan to have their workloads moved to cloud.

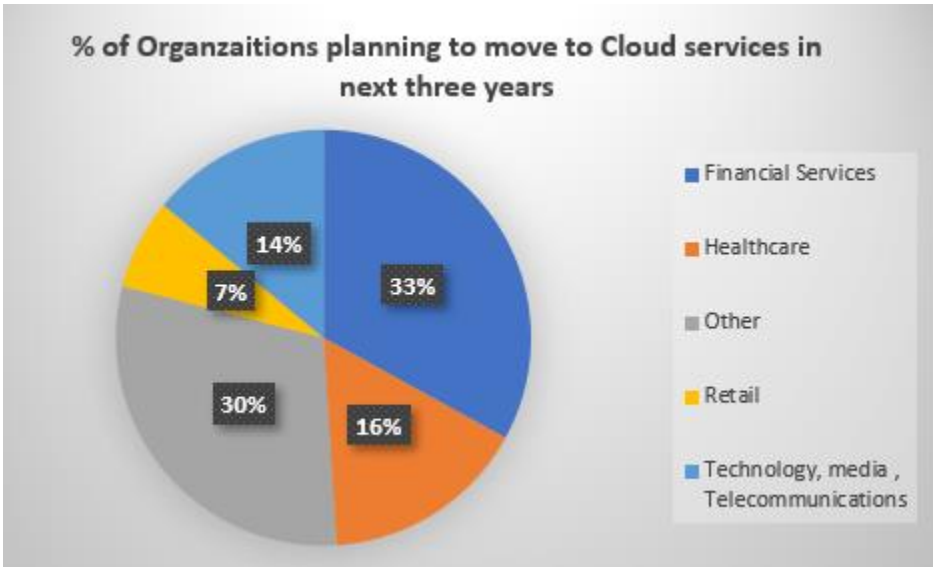

Figure 1: Enterprises Planning for cloud Adoption

[Link: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Making%20a%20secure%20transition/Making-a-secure-transition-to-the-public-cloud-full-report.ashx]

Even though in 2017 only 10% of companies had their workload on cloud, the future looked different. In three years (2020) 80% of companies have planned to move towards public cloud platforms as per the report. As per the report, China remains lagging and expected to become a tracking country beyond 2023. Japan's spending in expected to grow by 4.4% by 2022 on cloud adoption.

AI centric cloud Security Framework:

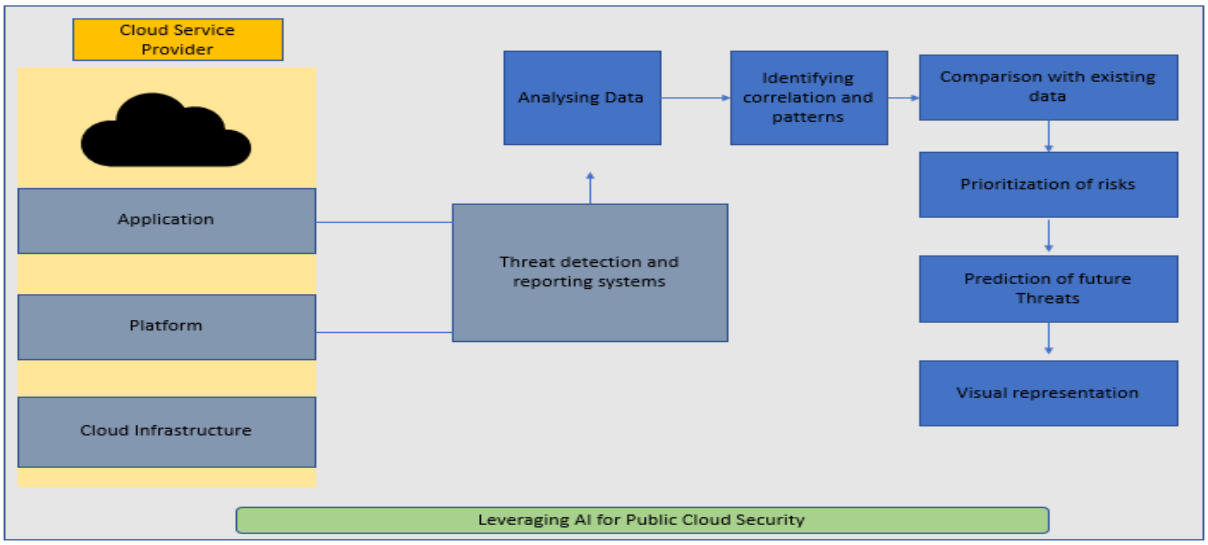

Figure 2: Framework for leveraging AI in Public Cloud Infrastructure

AI and Cloud Security:

While Leveraging AI tools in public cloud Infrastructure, security experts can identify threats and AI tools can provide recommendations. The threats identified in cloud environment can be modeled to draw conclusions on which type of threats are highly surfacing in the environment. Further, with the help of prediction algorithms, we can predict the threats which are likely to affect the systems. With the sheer volume of applications and devices, AI can bolster security teams with AI capabilities to mitigate risk faced. While Threat detectors collect large amount of data, this information can be used to analyses the patterns of vulnerabilities in systems and patch accordingly. We can further understand the type of devices, vulnerabilities that are targeted. With AI's massive computing efficiency and its capability to analyze huge sets of data at a faster pace than human employee, artificial intelligence can quickly learn, adapt, and introduce security measures. Security Alarms on potential threats or any anomalies in user access behavior can be tracked and there is a huge potential with automated technologies to eliminate basic security checks. When security teams have AI technologies handling routine tasks, security teams are free to focus on more critical or complex threats.

Application of AI for Public cloud security:

Prediction of Vulnerabilities

- Vulnerability management tools can leverage AI strategies to develop context of each asset.
- With the asset categories, the vulnerabilities can be prioritized based on risk and for both internal and external threats. Establishing priorities can help resolve or remediate the vulnerabilities that pose highest risk to the organization
- AI can also be used to identify false positives. By considering services running on an asset and various detection mechanisms an identified vulnerability can be scrutinized to check if it is a legitimate vulnerability.
- Application AI to vulnerability remediation data across various organizations can yield insights based on the aggregate judgment of huge number of IT and security teams. Using techniques such a regression, client practices and inclinations can be mixed with their history of remediation to foresee what is significant. Utilizing this ever-growing database of cloud computing data and their remediation activity, the commitment to the vulnerability score turns into a unique component that mirrors the continually changing nature of the danger.

Access Management

- AI can be used to provide recommendations on roles and access maintained by various users on public cloud. These recommendations of user role maintenance can reduce time and cost involved in defining user roles.
- Further, AI can be leveraged to recommend the level of access required to a user based on peer groups or access requests made earlier. Hence AI can be used as an engine to provide access level recommendations
- AI can be applied to identity anomalies in user actions and data sources and applications accessed. This can be performed by comparing the data accessed with previous data sources. Any threats or risk identified can be reported.
- Further we can incorporate usage data to generate efficient insights through analytics engine

Enterprise growth and expenditure:

In various research, organizations have mentioned about the benefits they leap from cloud computing. Also, AI is expected to spur economic growth. McKinsey has mentioned in its global institute model that 70% will adopt a AI in some form by 2030 and AI can contribute 1.2% of GDP for the next decade at least. The below graph is obtained from report by oracle and KPMG the amount of business-critical applications that enterprises are planning to move to cloud in the next 24 months.

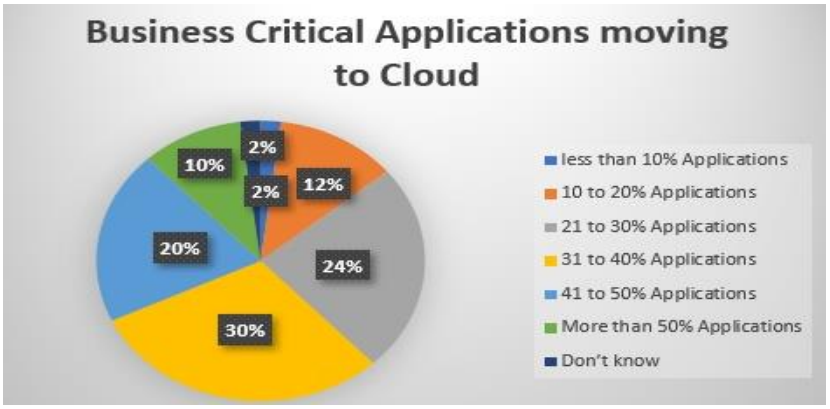

Figure 3: **Business Critical Applications moving to Cloud**

[Link: https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf]

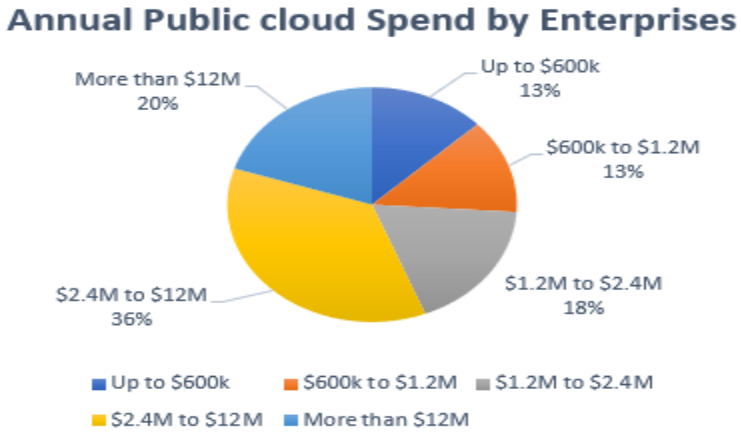

Figure 4: Annual Public cloud expenditure by enterprises

Link : [https://www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/#:~:text=Enterprise%20cloud%20spend%20is%20growing,exceeds%20%241.2%20million%20per%20year.]

Zero Day Threats and AI

Zero day refers to the day a vulnerability is identified in a software. The software vendors create a patch to fix the vulnerability to avoid any data breach or cyber-attacks. The time gap between the identification of a vulnerability and creation of patch may be weaponized by cyber criminals to attack the systems and in our case the public cloud. The patches are applied to avoid zero-day exploit and zero-day attacks. While traditional security systems employ antivirus software and patch management systems, these are insufficient to prevent or detect zero-day exploits.

The reason being, these threats are new to the system and have not occurred before. By Leveraging AI, zero-day exploits can be identified by automating the aberrant behavior recognition and then altering the administrations.

In this manner, to viably manage zero-day threats, organizations need to be progressively proactive and prescient with their security methodologies This requires perceivability into traffic from each endpoint by disassembling every approaching record to scan for any malignant components whether they be known or obscure, The time when traditional security measures were effective has come and gone. Using Behavior based techniques to identify any zero-day attacks can predict malicious actions if any.

Future scope

Currently, Organizations are viewing opportunities to advance on the technology front to compete with competitors. Implementing advanced technologies such as Artificial Intelligence and cloud computing not only will reduce the expenditure but also aid enterprises in to achieve business objectives. Cloud computing is incredibly financially savvy, and organizations leverage public cloud for technology advancements. To fully leverage the advantage of cloud computing, organizations should be acquainted with the most recent advancement in Cloud innovation. Considering this, cloud computing is on the ascent in the technology ecosystem. According to the report by Right scale, 81 percent of organizations with 1,000 representatives or more have a multi-platform system and the value by 2024 is expected to increase to 90 percent. Between 2018 to 2021, overall investments on open cloud administrations is to develop to 73 percent, from $160B to $277B. It is evident that organizations are increasing their investments on Cloud storage.

As on today, every critical advancement, for example, blockchain, artificial intelligence, AR/VR, robotics, and IoT depend on cloud computing innovation. India is relied upon to see in excess of a million cloud computing work jobs by 2022 as enterprises move their activities to the cloud foundation, according to a report by Great Learning. As the Indian cloud computing market, presently at $2.2 billion, is relied upon to develop to $4 billion by 2020 with a yearly development pace of over 30%; Additionally ,IDC has estimated more than 1 million job openings to be made available in India in the future. The implementation of AI and cloud are hence expected to have a rapid increase in the coming years.

Conclusion:

This paper discusses the security concerns of public cloud adoption and application of AI to manage the security challenges in public cloud. The paper also discusses about the future adoption of cloud, AI technologies and their advantages to the economy. Leveraging Artificial Intelligence in cloud computing will reduce the dependency of human intervention and with the help of prediction models, the threats can be predicted and prioritized as per the risk posed to organizations.

With the various applications of AI in public cloud computing discussed in the paper. With the future scope of AI adoption, it is evident that Predictive models and automated threat prediction systems are of dire importance to overcome the public cloud security challenges.

References

1. Darren E., Jonathan L., & Christopher W. (2018, April). Bringing AI to BI: Enabiling Visual analytics of unstructured data in a modern business Intelligence platform. *Extended Abstracts pf the 2018 CHI Conference on human factor in computing systems*. doi:10.1145/3170427
2. Dr. Krishna Murthy N., & Dr. Selvam R. (2015, December). Security Issues and Challenges in Cloud computing. *International Advanced Research Journal in Science, Engineering and Technology*(ISSN: 2393-8021).
3. Faheem G., Aaqib A., & Suhail A. (2017, July). Enhancement of Cloud Computing security with secure data storage using AES. *International Journal of Computer Science and Mobile Computing, ISSN 2320–088X*.
4. Flexera. (2020, May). *Cloud computing trends* . Retrieved from https://www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/#:~:text=Enterprise%20cloud%20spend%20is%20growing,exceeds%20%241.2%20million%20per%20year.
5. Luke M., Tsvetelina H., & Liam M. (2017, June). Clouded data: Privacy and the promise of encryption. *Big Data & Society*. doi:10.1177/2053951719848781
6. Mckinsey & Company. (2019). *Making a secure Transition to public Cloud.* Retrieved from https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Making%20a%20secure%20transition/Making-a-secure-transition-to-the-public-cloud-full-report.ashx
7. McKinsey & Company. (2019, March). *Perspectives on transforming cybersecuity.* Retreved from https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx.
8. Oracle & KPMG. (2020). *Cloud Threat Report.* Retrieved on July 1st 2020 from https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf

9. Panjun S. (2020, January). Cloud computing service based on trust access control. *International journal of engineering business management*. doi:10.1177/1847979019897444

10. Qianmu L., Xiaochun Y., Shunmei M., Yaozong L., & Zijian Y. (2020, May). A security event description of intelligent applications in edge-cloud environment. *The Journal of Cloud Computing: Advances, Systems and Applications*. doi:10.1186/s13677-020-00171-0

11. Shalin P., Dharmin ., Reema P., & Nishant D. (2019, November). Security and Privacy Issues in Cloud, Fog and Edge Computing. *Science Direct*

12. Vikas K., & Vidhyalakshmi P. (2012, December). Cloud Computing for Business Sustainability. *Asia Pacific Journal of Management Research and Innovation*. doi:10.1177/2319510X13481905

13. Vishal R., & Dr. Bhadresh P. (2016, February). Enhancement of Cloud Computing Security with Secure Data Storage using AES. *International Journal for Innovative Research in Science & Technology, ISSN (online): 2349-6010*.

14. Yashar A., & Meena C. (2018, December). The Challenges of Institutional Distance: Data Privacy Issues in Cloud Computing. *Science, Technology & Society*. doi:10.1177/0971721818806088

15. Zhenguo C., Liqin T., & Chuang L. (2018, May). Trust evaluation model of cloud user based on behavior data. *International Journal of Distributed Sensor Networks*. doi:10.1177/1550147718776924