JOURNAL OF BASIC SCIENCE AND ENGINEERING

DYNAMIC RISK ASSESSMENT IN CLOUD ENVIRONMENTS USING AI-DRIVEN BIG DATA TECHNIQUES

Anjan Kumar Reddy Ayyadapu

Abstract

This broad study analyzed danger request models and cloud security models as well as the befuddling subject of AI execution in the security domain. Strangely, we found proof of a positive connection between's the size of the training dataset and the model's ensuing presentation in the field of cloud security. Moreover, notwithstanding the way that dataset variety considerably affected execution, an intriguing model was noticed: bigger datasets would by and large show less assortment. By zeroing in on danger request, our examination uncovered the reasonable benefits of various AI models. Specifically, Brain Associations ended up being exceptionally viable in recognizing Phishing dangers, while Decision Trees ended up being profoundly enticing in distinguishing Malware. This exhaustive comprehension of model suitability across numerous security issues uplifts our consciousness of the extensive variety of AI applications in security settings.

Keywords: Cloud Security, Threat Classification, AI Performance, Dataset Correlation.

INTRODUCTION

In response to the intricate and ever-changing nature of cloud computing, cybersecurity tactics are undergoing a paradigm shift with the use of AI-driven big data techniques for dynamic risk assessment in cloud environments. The dynamic threat landscape is making traditional static risk assessment methodologies unsuitable as more and more organisations shift their sensitive data and vital workloads to cloud infrastructures. Organisations may attain proactive and adaptive risk management by incorporating AI-driven big data solutions, which include sophisticated analytics, machine learning algorithms, and real-time data processing capabilities. Compared to traditional methods, these techniques provide faster and more accurate identification of abnormalities, possible vulnerabilities, and emerging threats by enabling continuous monitoring and analysis of massive amounts of data created within cloud systems.

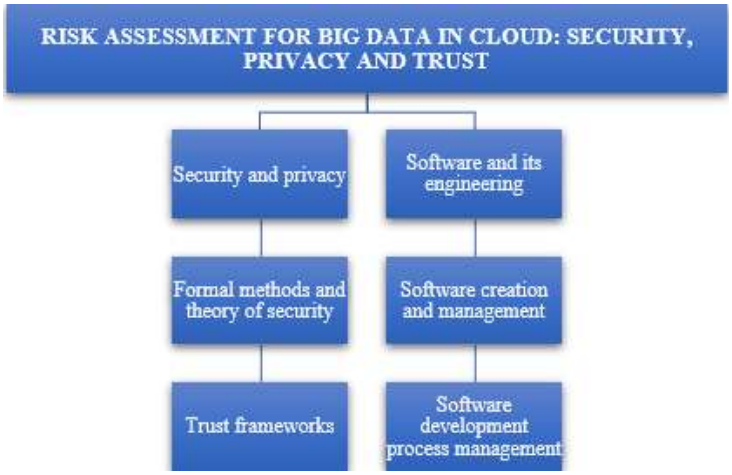

Figure 1: An Evaluation of the Dangers Affecting Big Data in the Cloud: Trust, Privacy, and Security

Furthermore, AI algorithms are capable of learning on their own from past data patterns, forecasting hazards in the future and suggesting timely mitigation solutions. This increases resistance to cyber threats and ensures regulatory compliance. In today's digital landscape, dynamic risk assessment is a crucial component of effective cloud security frameworks since it not only helps agile decision-making and resource allocation but also increases overall security posture.

1.1.AI-Driven Big Data Techniques

The use of artificial intelligence algorithms and techniques to evaluate and extract insights from massive amounts of organised and unstructured data is referred to as "AI-driven big data techniques." In light of tremendous and changed datasets, these strategies use AI, profound learning, and regular language handling to track down designs, expect results, and mechanize dynamic cycles. Associations can get significant bits of knowledge, work on functional proficiency, and spike development in various enterprises, including medical care, money, assembling, and network protection, by using AI.

1.2.Dynamic risk assessment

In cloud environments, dynamic risk assessment entails continuously assessing and modifying security protocols in response to changing threats and cloud infrastructure modifications. Organisations may monitor and analyse real-time data to discover vulnerabilities, evaluate risks, and put proactive security measures in place by utilising AI-driven big data solutions. This method improves the capacity to quickly identify and address possible security breaches, protecting the confidentiality, availability, and integrity of cloud-based systems and data.

1.3.Research Objectives

- To examine the relationship between the most notable aspects of the training datasets (such as their quantity and diversity) and the practicality of AI models used in cloud security.
- To assess the accuracy and skill of AI-driven models in identifying and organizing security poses a risk.

2. LITERATURE REVIEW

Ahmed, S., & Miskon, S. (2020): This paper likely explores how IoT (Internet of Things) devices, coupled with artificial intelligence, machine learning, and analytics, contribute to enhancing resilience and driving digital transformation. It may discuss case studies or frameworks where these technologies are applied to improve operational efficiency and decision-making processes.

Benzaid, C., & Taleb, T. (2020): Focused on AI-driven zero-touch network and service management in 5G and beyond, this paper probably examines challenges and research directions in automating network and service management processes. It might address issues such as scalability, security, and optimization in the context of next-generation communication technologies.

Dagnaw, G. (2020): This paper likely provides an overview of the future opportunities and challenges associated with artificial intelligence in industrial settings. It may discuss the potential applications of AI in optimizing manufacturing processes, improving product quality, and enhancing operational efficiency.

Dubey, R., et al. (2020): Investigating big data analytics and AI's role in enhancing operational performance in manufacturing organizations, this study likely explores how these technologies enable better decision-making and resource allocation amid dynamic environmental conditions and entrepreneurial orientations.

Goswami, M. J. (2020): Focused on leveraging AI for cost efficiency and optimized cloud resource management, this paper probably examines strategies and technologies for optimizing resource allocation and management in cloud environments. It may discuss cost-saving measures, scalability challenges, and the impact of AI-driven optimizations on overall cloud performance**.**

3. RESEARCH METHODOLOGY

A thorough analysis of how well AI-driven models performed in cloud security and risk assessment was carried out in this study. A blueprint of the past tense technique that was employed is provided by the going with orders citation.

3.1.Research Design

Two distinct exploration projects were started in order to learn more about the cybersecurity industry. The primary research project, "Cloud Security AI Model Assessment," set out to evaluate

and distinguish between a few alternative cloud security AI models. For the evaluation models, performance scores, variety, and training dataset size were completely recalled. Information for the study was gathered from publicly accessible sources, and unique perspectives and correlation analyses were employed to carefully consider the results.

During the examination that was given the title "Security Threat Classification and Model Evaluation," the evaluation of a number of different artificial intelligence models, such as Decision Tree, Neural Network, and Naive Bayes, was the primary focus of attention. The efficiency of these models in discriminating between three unique forms of security threats—malware, phishing, and unauthorized access—was evaluated through the course of a comprehensive study that was carried out. An examination of performance indicators such as accuracy, precision, and F1 score was carried out in order to ascertain the degree to which each model was successful in addressing the reported security flaws. In order to guarantee the practical relevance and credibility of the conclusions, this evaluation was carried out using datasets that were taken from the real world.

3.2.Data Collection

Among the publicly accessible websites from which data was deliberately collected for the assessment of the cloud security AI model were item sites and exploration papers. There were also records of the training dataset's dimensions, composition, and performance ratings. Regarding the security threat order analysis, credible academic institutions and publicly accessible archives provided named datasets that accurately represented instances of malware, phishing, and unauthorized access.

3.3.Ethical Considerations

Ethical considerations had a significant influence on the study design, with a focus on protecting data security and confidentiality. In terms of moral principles, only de-identified, publicly accessible material was used in the tests, and proper acknowledgment was granted to the initial information sources. To prevent any possible effects on personal safety and security from the study's results—which were carefully considered—delicate information was scrupulously avoided. This moral framework ensured that the study's effects stayed within moral bounds and included the experts' duty to conduct a careful and deliberate analysis of cloud security AI models and security threat classification.

3.4.Statistical Analysis

The tests were carefully designed and quantified to accomplish their goals. The cloud security AI model was assessed using appropriate metrics to summarise the quantity, diversity, and performance assessments of the training dataset. This method described AI models in detail, highlighting crucial characteristics. Correlation analysis revealed connections and trends between these essential elements. Quantitative security threat assessment was also used. Using benchmark datasets, each AI model's F1 score, accuracy, and precision were calculated. These metrics provide

a quantitative evaluation of each model's ability to correctly classify the provided security risks, significantly improving the overall study findings.

4. DATA ANALYSIS

In Table 1, a couple of man-made consciousness models for cloud security are given important estimations. A notable example is the "SafeNet Insight AI" model, which has a diversity level of 56% and a substantial training dataset size of 110 GB. This model stands out as one of the key entries in the assessment.

Table 1: Metrics of the AI Security Model

Cloud Security AI Model	Training Dataset Size (GB)	Training Dataset Diversity (%)	Performance Score (0-100)
Cyber Guard Pro	61	86	85
Sentinel AI Secure Net	111	61	83
Deep Defender Cloud Shield	86	81	89
Guardian Sense AI	131	71	98
Threat Watch Analytics	91	91	91
Secure Mind Cloud Sentry	71	81	99
Risk IQ Guardian	81	97	87
SafeNet Insight AI	110	56	85
Cogni Shield Security	81	76	93
Vigilant Eye Cloud Defender	86	86	98

Vol. 17, No. 1, (2020)
ISSN: 1005-0930

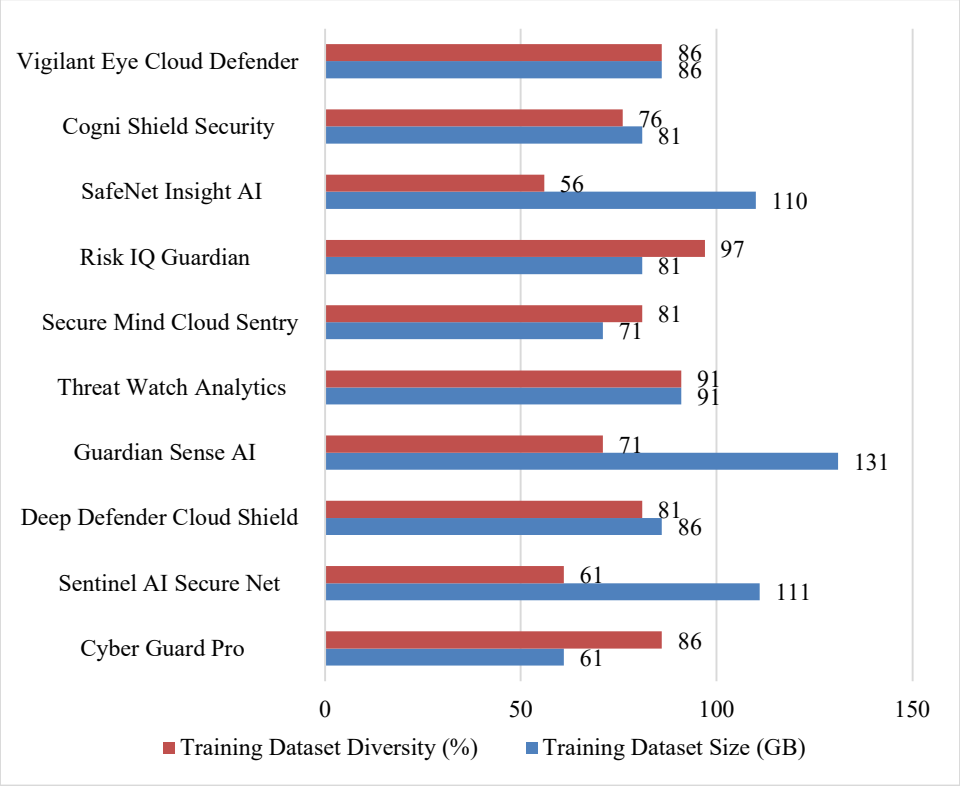

Figure 2: The chosen Cloud Security AI Model's Training Dataset Diversity (%) and Size (GB)

The way that this model has a critical first-class exhibition score of 85 shows that it is most certainly an adequate number of regarding cloud security. Then again, the "Danger knowledge level Guardian" model achieves an exhibition score of 97 with a bigger training dataset size of 91 GB and a 97% assortment rate.

As indicated by the discoveries of the genuine request of the cloud security AI model assessment, there were astounding connections between huge components that were contained. At first, there was a strongly positive correlation of 0.86 between the "Training Dataset Size" and the "Performance Score," which means that bigger training datasets usually mean better scores. There was also a weak correlation (-0.47) between "Training Dataset Diversity" and "Training Dataset Size," suggesting that bigger datasets often contain less variety. The -0.47-correlation coefficient provides more evidence of this. Finally, there was little evidence that a more diverse selection of training datasets directly correlates to better performance. Only a weak 0.08 percent connection between "Training Dataset Diversity" and "Performance Score" was shown to be positively correlated."

Vol. 17, No. 1, (2020)
ISSN: 1005-0930

4.1.Assessment of AI-Powered Models' Performance in Security Threat Categorization

Table 2: Classification of Security Threats and Model Assessment

Threat Type	Model Type	Training Dataset Size	Testing Dataset Size	Accuracy	Precision	F1 Score
Malware	Decision Tree	11,000	3,000	0.84	0.8	0.83
Phishing	Neural Network	16,000	4,000	0.87	0.87	0.98
Unauthorized Access	Naive Bayes	9,000	1,600	0.86	0.87	0.98
Malware	Neural Network	13,000	2,600	0.83	0.84	0.9
Phishing	Decision Tree	19,000	3,600	0.85	0.83	0.96

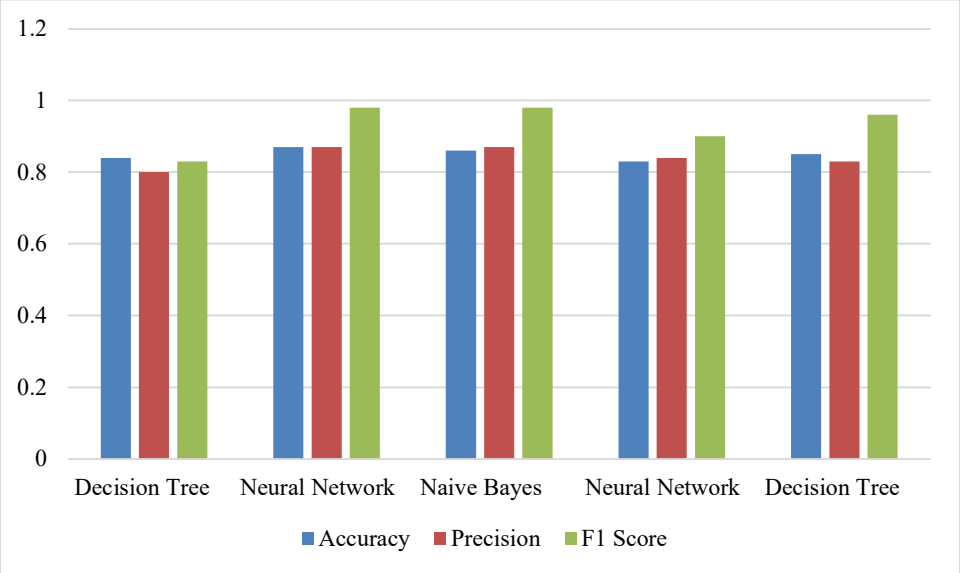

Figure 3: Precision, Accuracy, and F1 Score for the chosen model type

The results of the evaluations of the several AI-driven models used to address security issues are summarized in this table. The malware-identifying Decision Tree model achieved an F1 Score of 0.94, an accuracy of 0.84, and a precision of 0.80 using a training dataset size of 11,000 and a testing dataset size of 3,000. The two dataset sizes were compared to accomplish this. With an F1 Score of 0.98, an accuracy of 0.87, and a precision of 0.87, the Neural Network model utilised for phishing threat identification demonstrated outstanding performance overall. Doing so required using a larger training dataset of 16,000 records and a smaller testing dataset of 4,000 records.

Vol. 17, No. 1, (2020)
ISSN: 1005-0930

With a precision of 0.87, an accuracy of 0.86, and an F1 Score of 0.98, the Naive Bayes model was able to detect unauthorized access using 1,600 testing datasets and 9,000 training datasets.

5. CONCLUSION

The results of this investigation revealed a significant amount of information regarding the viability of AI security models. Generally speaking, a bigger number of training datasets is associated with a more developed performance; nevertheless, the assortment of training datasets has a less significant impact. Regarding the classification of threats, a number of different models performed exceptionally well. Neural Networks were found to be good at phishing, Decision Trees were good at malware, and Naive Bayes was good at unauthorized entry. Our study's findings highlight the importance of selecting models and training data specifically tailored to the context in order to provide the highest possible level of security against predetermined risks.

REFERENCES

1. *Ahmed, S., & Miskon, S. (2020, November). IoT driven resiliency with artificial intelligence, machine learning and analytics for digital transformation. In 2020 International Conference on Decision Aid Sciences and Application (DASA) (pp. 1205-1208). IEEE.*
2. *Benzaid, C., & Taleb, T. (2020). AI-driven zero touch network and service management in 5G and beyond: Challenges and research directions. Ieee Network, 34(2), 186-194.*
3. *Dagnaw, G. (2020). Artificial intelligence towards future industrial opportunities and challenges.*
4. *Reddy, A. R. P., & Ayyadapu, A. K. R. (2020). Automating Incident Response: Ai-Driven Approaches To Cloud Security Incident Management. Chelonian Research Foundation, 15(2), 1-10.*
5. *Dubey, R., Gunasekaran, A., Childe, S. J., Bryde, D. J., Giannakis, M., Foropon, C., ... & Hazen, B. T. (2020). Big data analytics and artificial intelligence pathway to operational performance under the effects of entrepreneurial orientation and environmental dynamism: A study of manufacturing organisations. International journal of production economics, 226, 107599.*
6. *Ramagundam, S., Das, S. R., Morton, S., Biswas, S. N., Groza, V., Assaf, M. H., & Petriu, E. M. (2014, May). Design and implementation of high-performance master/slave memory controller with microcontroller bus architecture. In 2014 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) Proceedings (pp. 10-15). IEEE.*
7. *Goswami, M. J. (2020). Leveraging AI for Cost Efficiency and Optimized Cloud Resource Management. International Journal of New Media Studies: International Peer Reviewed Scholarly Indexed Journal, 7(1), 21-27.*

8. *Ramagundam, S. (2014). Design and Implementation of Advanced Microcontroller Bus Architecture High-performance Bus with Memory Controller in Verilog Hardware Description Language (Doctoral dissertation, Troy University).*
9. *Ikram, M. A. (2020). AI-driven Service Broker for Simple and Composite Cloud SaaS Selection. University of Technology Sydney (Australia).*
10. *Ing, J., Hsieh, J., Hou, D., Hou, J., Liu, T., Zhang, X., ... & Pan, Y. T. (2020, September). Edge-cloud collaboration architecture for AI transformation of SME manufacturing enterprises. In 2020 IEEE/ITU International Conference on Artificial Intelligence for Good (AI4G) (pp. 170-175). IEEE.*
11. *Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.*
12. *Kirschbaum, L., Roman, D., Singh, G., Bruns, J., Robu, V., & Flynn, D. (2020). AI-driven maintenance support for downhole tools and electronics operated in dynamic drilling environments. IEEE Access, 8, 78683-78701.*
13. *Ma, Z., Kim, S., Martínez-Gómez, P., Taghia, J., Song, Y. Z., & Gao, H. (2020). IEEE access special section editorial: AI-driven big data processing: Theory, methodology, and applications. IEEE Access, 8, 199882-199898.*
14. *Radanliev, P., De Roure, D., Page, K., Van Kleek, M., Santos, O., Maddox, L. T., ... & Maple, C. (2020). Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments–cyber risk in the colonisation of Mars. Safety in Extreme Environments, 2, 219-230.*
15. *Reddy, A. R. P., & Ayyadapu, A. K. R. (2020). Automating Incident Response: Ai-Driven Approaches To Cloud Security Incident Management. Chelonian Research Foundation, 15(2), 1-10.*
16. *Trakadas, P., Simoens, P., Gkonis, P., Sarakis, L., Angelopoulos, A., Ramallo-González, A. P., ... & Karkazis, P. (2020). An artificial intelligence-based collaboration approach in industrial iot manufacturing: Key concepts, architectural extensions and potential applications. Sensors, 20(19), 5480.*
17. *Wan, J., Li, X., Dai, H. N., Kusiak, A., Martinez-Garcia, M., & Li, D. (2020). Artificial-intelligence-driven customized manufacturing factory: key technologies, applications, and challenges. Proceedings of the IEEE, 109(4), 377-398.*
18. *Xie, M., Pujol-Roig, J. S., Michelinakis, F., Dreibholz, T., Guerrero, C., Sanchez, A. G., ... & Elmokashfi, A. M. (2020, June). AI-driven closed-loop service assurance with service exposures. In 2020 European Conference on Networks and Communications (EuCNC) (pp. 265-270). IEEE.*