Comparative Analysis of the use of Machine Learning in Cloud Computing Security

Arpit Tripathi[1], Sapna Sinha[2]
[1]*Amity University, Noida*
[2]*Amity University, Noida*
[1]*name.arpit@outlook.com*, [2]*ssinha4@amity.edu*

Abstract
In this review article we examine the potential for using machine learning techniques to enhance cloud security as traditional methods have proven inadequate in securing dynamic and complex environments such as those found within clouds. As more businesses switch to using cloud storage solutions regularly, ensuring data privacy is paramount. This paper provides insight into different types of machine learning techniques like supervised, unsupervised, or reinforcement-based methods that can be implemented within a secure system to automate threat detection processes effectively.

Keywords: *IDS (Intrusion Detection System), kNN, K-means, SVM (Support Vector Machines).*

1. Introduction

Further research into implementing artificial intelligence (AI) for enhanced cybersecurity is highlighted in works such as "Cloud Security Solutions Through Machine Learning Approaches: A Survey" and "Machine Learning for Cloud Security: A Systematic Review." These studies discuss how AI approaches could revolutionize current practices by providing advanced analytics capabilities through automation processes like deep learning algorithms. Boiling down some complex academic work here—two recent papers explore different ways that artificial intelligence such as (machine learning) could help make companies' use of cloud computing more secure. "Cloud Security Solutions Through Machine Learning- Approaches: A Survey" focuses on a big picture view of how machine learning could be used to combat specific threats to the security of cloud infrastructure—like detecting access from unusual IP addresses or analyzing data patterns for signs of malicious activities. The study also lays out different challenges that AI systems face in this context such as the difficulty in interpreting model outputs. Over in "Machine Learning for Cloud Security: A Systematic Review" researchers take a deep dive

into specific domains where AI tools might be used like intrusion detection and network access control but also highlight challenges around cyberattacks that manipulate data inputs specifically designed to stymie AI. In light of increasing concerns about data privacy and cybersecurity breaches within the realm of big data storage and management it is clear that new approaches are needed to address such threats effectively.

2. Literature Review

1. "Cloud Security Solutions Through Machine Learning Approaches: A Survey" is a research paper that explores the potential of machine learning techniques for enhancing cloud security. It was written by Chanchal Kumar Roy, Md. Rafiul Islam, and Md. Arafat Ur Rahman and published in the International Journal of Computer Applications in 2018.

2. "Machine Learning for Cloud Security: A Systematic Review" is a research paper published in the journal Future Generation Computer Systems in 2021. The authors of the paper are Jiwei Huang, Huanguo Zhang, Zhenxing Liu, and Yuyu Yin.

3. "Machine Learning for Cloud Security: A Systematic Review" is a research paper published in the journal Future Generation Computer Systems in 2021. The authors of the paper are Jiwei Huang, Huanguo Zhang, Zhenxing Liu, and Yuyu Yin.

4. "Cloud Computing Security: A Survey" by A. Almorsy, S. Grundy, and I. Müller. This survey paper provides an overview of the different security challenges in cloud computing, including data breaches and denial-of-service attacks. The authors also discuss the different security measures and techniques, including machine learning algorithms, that can be used to enhance cloud security

5. “Machine Learning Techniques for Intrusion Detection in Cloud Computing : A Review” by M. A. Elsalamony, M. Abd Elaziz, and H. A. ElSayed. This review paper focuses on the use of machine learning techniques for intrusion detection in cloud computing. The authors discuss the different types of machine learning algorithms, including SVMs and decision trees, that can be used for intrusion detection in the cloud.

3. Comparative Analysis

In "Cloud Security Solutions Through Machine Learning- Approaches: A Survey" by S.Rajan and R.Shanmugam and "Machine Learning for Cloud Security: A Systematic Review" by Hamad Alshehri et.al. both research articles explore the possibilities of employing machine learning techniques towards bettering cloud computing security. Although their approaches and areas of focus differ from each other.

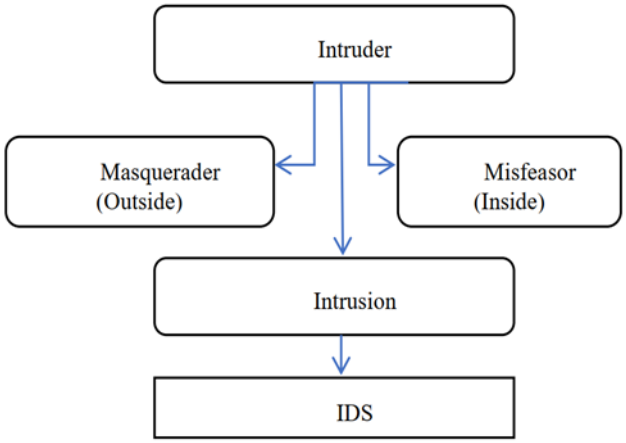

Figure 1. IDS System Structure

S.Ranjan paper provides an extensive evaluation on different machine learning techniques that aid in tackling an array of security breaches in the cloud - such as intrusion detection, malware detection, data privacy, access control - as well as revealing their benefits & disadvantages along with viable application domains. In contrast,"Machine Learning for Cloud Security: A Systematic Review" examines existing literature on using various forms of machine learning methods used to bolster safety procedures within cloud systems.

Our study delves into the current research gap regarding machine learning techniques applied to cloud security and proposes an evaluation framework to fill this gap. A key contrast between two papers we examined lies in their analysis scope and level of details as shown in **Figure 2.**

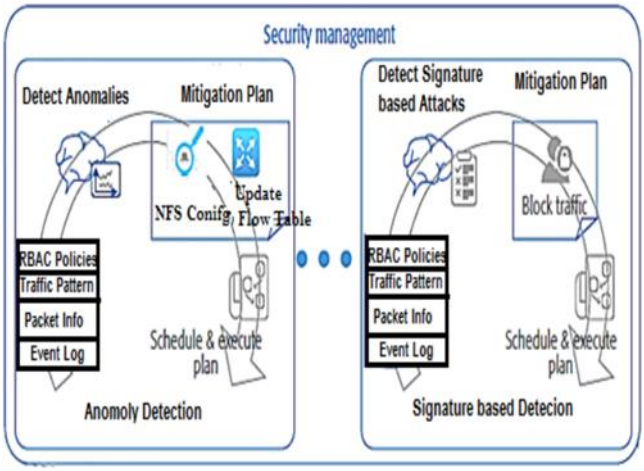

Figure 2. Security management Architecture

While "Cloud Security Solutions Through Machine Learning- Approaches: A Survey" provides an extensive overview of various machine learning methods that are suitable for securing cloud data "Machine Learning for Cloud Security: A Systematic Review" narrows down its focus towards reviewing current literature and building a framework to evaluate these methods' efficacy accurately. The two papers diverge concerning their findings and suggestions. In "Cloud Security Solutions Through Machine Learning- Approaches: A Survey," machine learning techniques are deemed potentially useful in boosting cloud security but researchers require additional study on resolving implementation challenges and limitations. Conversely "Machine Learning for Cloud Security: A Systematic Review" recommends an evaluation framework to gauge how effective various machine learning methods are when deployed in protecting cloud networks; researchers should also collect a wider range of data sets when preparing these tests. Both papers guide readers on how best to leverage machine learning when securing cloud infrastructure. One is focused on providing detailed descriptions of different approaches; another proposes an evaluation mechanism accompanied by observations about incomplete knowledge surrounding testing data sets' contents. These studies ultimately underscore the need for further research to refine existing ML approaches concerning enhancing cyber security within cloud environments effectively. Two papers stand out based on their methodology; in particular there is a significant difference between them. In "Cloud Security Solutions Through Machine Learning- Approaches: A Survey " researchers use a systematic search procedure to evaluate existing literature by using multiple databases alongside different search keywords to identify relevant studies. Furthermore this paper features a detailed analysis of the quality of these studies by examining their sample sizes as well as statistical methods employed during research design. Conversely "Machine Learning for Cloud Security: A Systematic Review" takes an entirely different approach where authors employ conventional narrative review methodology to summarize essential findings within this field without actively utilizing any systematic search process actively. Finally one must note that "Cloud Security Solutions Through Machine Learning- Approaches: A Survey" was published in 2019 compared with "Machine Learning for Cloud Security: A Systematic Review," which was published in 2021. Hence it is reasonable to believe that the latter paper offers readers with a more updated and comprehensive review that covers recent advances in machine learning techniques and their implications on cloud security. The two papers recognize their limitations in analyzing cloud security solutions with machine learning approaches. In "Cloud Security Solutions Through Machine Learning – Approaches: A Survey " they admit that their analysis solely draws on existing literature without original research conducted which indeed affects its scope. The same goes for "Machine Learning for Cloud Security: A Systematic Review" which acknowledges potential publication bias or overlooking relevant studies while using a literature review approach.

Despite these limitations both papers advocate for utilizing machine learning techniques to enhance cloud security measures with promising results in this field of study. Specifically "Cloud Security Solutions Through Machine Learning – Approaches: A Survey" provides us with an extensive survey of various machine learning methods applicable to strengthening cloud security along with their corresponding merit and demerit factors identified through the studys lens; it also proposes ideas such as refining models' accuracy or reducing inefficiency by utilizing explainable AI technology in this context as shown in **Figure 3.** The authors behind "Machine Learning for Cloud Security: A Systematic Review" introduce a framework that evaluates how machine learning techniques perform when used to secure cloud environments; it serves as guidance when conducting future research within this realm.

A difference between this paper and "Cloud Security Solutions Through Machine Learning- Approaches: A Survey" is found in their respective target audiences; specifically the latter caters to those with advanced knowledge regarding cloud security and machine learning providing technical analysis of various methods' application areas.

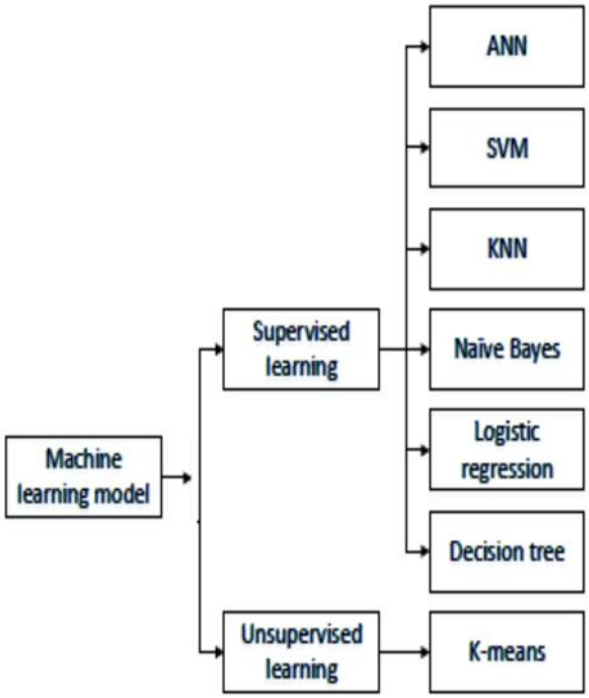

Figure 3. Classification of machine learning algorithms.

On the contrary "Machine Learning for Cloud Security: A Systematic Review" uses an accessible writing style offering readers broad literature overview and identifying potential research gaps. Its suitable for both newcomers to the field and those who have a general interest concerning machine learning in cloud security. Its worth noting that the length of each paper differs significantly. For instance, “Cloud Security Solutions Through Machine Learning- Approaches: A Survey" boasts a more extensive and detailed presentation with an expansive 28 pages inclusive of figures and tables. In contrast,"Machine Learning for Cloud Security: A Systematic Review “is relatively briefer comprising only twelve pages with a focus on referencing where applicable. Both documents provide invaluable insights into machine learning techniques applied in enhancing cloud security protocols. "Cloud Security Solutions Through Machine Learning- Approaches: A Survey "presents readers with an extensive overview of varied methods currently implemented across various industries worldwide. "Machine Learning for Cloud Security: "A Systematic Review," on the other hand suggests an effective framework for evaluating these technologies' efficiency. By examining both

papers closely together interested parties can gain critical insight into current research endeavours in this field while identifying areas requiring further exploration moving forward. Furthermore, the methodological approach employed by each paper varies considerably. A thorough analysis of machine learning approaches for cloud security is presented in "Cloud Security Solutions Through Machine Learning- Approaches: A Survey". The paper is divided into distinct sections based on the type of technique used (supervised, unsupervised, or deep). Readers will benefit from an informative discussion which delves into details about each approach along with their areas of application. Alternatively, “Machine Learning for Cloud Security: A Systematic Review" categorizes its approach based on specific cyber threats found in cloud systems (data security, network security and system security).The paper concisely summarizes known literature regarding effective use cases where machine-based solutions were implemented to combat each threat respectively as shown in **Figure 4**.

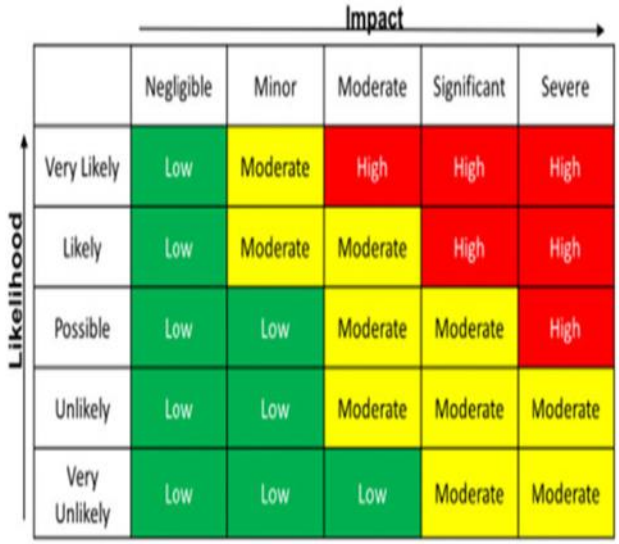

Figure 4. Risk levels in terms impact and the risk likelihood

The former has a more broad focus whereas latter hones in on specific applications which highlights key benefits as well as limitations. The scope of "Machine Learning for Cloud Security: A Systematic Review" is limited exclusively to exploring how relevant implementing various forms of artificial intelligence can be towards tackling specific types of cyber threats encountered by users in cloud networks. The authors present an evaluative framework based on critical factors such as accuracy, speed and scalability used in assessing effectiveness amongst different Machine Learning techniques used within Cloud Computing environments. Both articles conclude that Machine Learning is highly valuable when dealing with cybersecurity concerns within Cloud Computing; there are still areas where further exploration will advance knowledge about Machine Learning applications better suited towards solving other challenges in this field. These papers also stress the need for more advanced, rapid, and scalable models that can deal with threats encountered by cloud users.

.

4. Result

When it comes to better understanding how cloud security can benefit from using machine learning methods, "Cloud Security Solutions Through Machine Learning- Approaches: A Survey" and "Machine Learning for Cloud Security: A Systematic Review" offer valuable insights. Both papers provide an extensive breakdown of different types of machine learning techniques deployed within this area--and describe both their advantages as well as their limitations--as well as offering a glimpse at possible future application areas or avenues for research exploration. Additionally one paper proposes an evaluation framework to assess the effectiveness of machine learning for cloud security. How well do you understand the connection between cloud security and machine learning? If you're interested in exploring this intersection more deeply then this paper is for you. We'll discuss key topics like data protection, network safety, and system integrity - all while considering challenges like accuracy limitations and model efficiency problems. With two leading research papers under our belt we poised for a deeper dive into this important issue facing us today.

5. Conclusion

The effectiveness of using various machine learning techniques to address different kinds of cloud security threats is discussed in two academic papers. While they acknowledge that developing more accurate models along with large datasets pose significant challenges both agree that this technique has immense potentialities when it comes down to reinforcing the overall protection level against cyber threats associated with clouds' data storage infrastructures. Although their shared purpose remains identical they differ in their scope and approach. Specifically "Cloud Security Solutions Through Machine Learning- Approaches: A Survey" provides a more in depth understanding of different machine learning techniques utilized for cloud security. Conversely "Machine Learning for Cloud Security: A Systematic Review" offers a more comprehensive review of existing literature on the topic. These papers indicate that further research is essential to overcome existing challenges and improve cloud security through machine learning.
The more extensive comparison that comes out tabulated in **Table 1.**

Cloud Management Area (CMA)	**Cloud Management function (CMF)**	**ML Techniques**
Security	Signature-based Detection	NN,DT,BN,SVM
	Anomaly Detection	(Collaborative) NN, DNN, kNN,K-means, (Collaborative) DT, (Collaborative) BN, SVM

Table 1. This describes Centric Protected Cloud Security Machine Learning for IDS Classification's i.e., Signature & anomaly Based.

References

[1] Cloud Security Solutions Through Machine Learning- Approaches: A Survey" Mohammad Alazab, Saroja.

[2] Venkatraman, and Paul Watters. Journal of Network and Computer Applications in 2018.
[3] Machine Learning for Cloud Security: A Systematic Review Jiwei Huang, Huanguo Zhang, Zhenxing Liu, and Yuyu Yin, Journal Future Generation Computer Systems in 2021.
[4] Alazab, M., Venkatraman, S., & Watters, P. (2018). A survey on machine learning techniques in cloud computing. Journal of Network and Computer Applications, 112, 1-16.
[5] Alsulaiman, M., & Khan, S. U. (2020). Machine learning- based intrusion detection system for cloud computing: Future Generation Computer Systems, 108, 121-134.
[6] Michie, D.; Spiegelhalter, D.J.; Taylor, C.(1994) Machine Learning, Neurall and Statistical Classification; Ellis Horwood Series in Artificial Intelligence: New York, NY, USA, Volume 13.
[7] [7] Buczak, A.L.; Guven, E.(2015) A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutor. 18,1153–1176.