IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 20-22
www.iosrjournals.org

A Periodical of Machine Learning Algorithms for Cloud Security

S.Hassan Abdul Cader, Research Scholar,
Department of Computer Science,
Quaid-E-Milleth Govt college for women,
Chennai.

Dr. K. Nirmala, Associate professor,
Department of Computer Science,
Quaid-E-Milleth Govt college for women
Chennai.

Abstract
Cloud computing (CC) is the on-demand accessibility of network resources, especially datastorage and processing power, without special and direct management by the users. CC recentlyhas emerged as a set of public and private data centers that offers the client a single platform acrossthe Internet. Edge computing is an evolving computing paradigm that brings computation andinformation storage nearer to the end-users to improve response times and spare transmissioncapacity. Mobile CC (MCC) uses distributed computing to convey applications to cell phones.However, CC and edge computing have security challenges, including vulnerability for clients and
association acknowledgment, that delay the rapid adoption of computing models. Machine learning(ML) is the investigation of computer algorithms that improve naturally through experience. In thisreview paper, we present an analysis of CC security threats, issues, and solutions that utilizedone or several ML algorithms. We review different ML algorithms that are used to overcomethe cloud security issues including supervised, unsupervised, semi-supervised, and reinforcementlearning. Then, we compare the performance of each technique based on their features, advantages,and disadvantages. Moreover, we enlist future research directions to secure CC models.

Keywords
loud computing; cloud security; security threats; cybersecurity; machine learning

I. Introduction

Cloud Computing (CC) has recently emerged as a new framework for facilitation and delivery. Services over the Internet [1]. Usual financial limits and increasing computational complexity include: Storing, Analyzing, and Presenting the Data That Drives Today's Critical Change Cloud model [2,3]. CC is on-demand access to end-user resources, especially information. storage and computing power. No direct special organization by the customer is required. distributed computing is a common expression that means different things to different people. distributed computing products It provides public and private data to customers on a single platform over the Internet [4]. However, CC Several security challenges slowing the rapid adoption of the computer model. B. Vulnerability For client and association [5,6]. Edge computing, a version of CC used to process time-sensitive data, offers application developers Service providers distributed computing power at the edge of the system [7]. Edge processing now extends this methodology with virtualization innovations to simplify delivery and operations Broader application potential on edge servers. The distributed concept of this paradigm is Changes in security plans used in distributed computing. Additional cryptographic information specific Since information can be transmitted between different distributed systems, encryption systems should be employed. A hub that connects to the web before it finally reaches the cloud. Edge Hub can also do this An asset-based device that constrains security strategy decisions. through care It is conceivable that responsibility for information is shifted from peripheral information and services Provider for end users. The core concept is to allow computers to modify and change themselves without human intervention or help activity as a requirement. CC has service models such as Infrastructure as a Service (IaaS) and Platform. a Service (PaaS) and Software as a Service (SaaS), public, private, Communities and hybrid clouds are also discussed. The main security concerns in CC are categorized as follows: Under threat of integrity, availability and confidentiality. Cloud services from information storage For managing software services with unlimited availability requirements. CC is usually developed As an impenetrable environment that can provide architecture, products and computing power, Thickness on request [8]. Cloud model favours' and supports large-scale deployment of hardware assets (to provide supported services) and infrastructure [9]. CC as a new model of data processing Despite its benefits, challenges. Not all cloud deployment styles are suitable for all services. Customers of each provider or all parties involved [10]. This document addresses security issues and Challenges of CC and related solutions using machine learning (ML) algorithms. ML algorithms are used to solve security problems and manage data more efficiently [11]. ML is Use of artificial consciousness that allows frames to be successfully absorbed and actually improved Not explicitly adapted [12]. ML focuses on advances in computer programs. I can find the

right pace to study on my own [13]. the learning approach Direct understanding or directing to channels of perception or data, structure, such as models Based on the model given, you will be informed and later make better decisions on this topic.

II. Related Work:

Explore related articles on cloud security using ML algorithm. We then discuss the comparison of relevant papers with ours. Khan et al. [15] discussed algorithms that solve security problems and improve performance. cloud system. Lack of interest in information still exists due to the volatility of information. Outsiders who store, manage and shape information. The authors used artificial neural networks. (ANN) Encrypted Information. Killer etc. [16] Investigate trust-based security issues; Challenges of the cloud model. They defined CC as the appropriate processing terms to host. Dedicated registration of resources anytime, anywhere. This creates information flexibility Inevitability and diversity of information. The author proposed a trust-based access control model An efficient method for security in distributed computer systems. The main motivation behind it Their model is to grant access to authorized clients in the cloud and select assets for computation. Both client assets and cloud he assets are evaluated based on trust ratings. The authors of [17] discussed cloud security issues and models. The authors examined identifiability Security aspects of organizational dynamics models arising from distributed computing. But the conclusion is Evolution of the cloud without others offers significant security potential. Mobility model methodology should not struggle with required features and capacity Installed in the current model. Another model focused on enhancing presentation characteristics A model must not compromise or weaken other important features of the current model. Bamare et al. [18] Improves data security as described in the ML model. the concept of Distributed computing has been discussed for scaling critical traction and virtualized server farms. As a practical framework and answer to huge business applications [19]. Researchers used assistance models to solve security threats and protection challenges Distributed computing [20]. They examined fundamental threats and protection challenges in distributed environments We analysed computing, various existing deployments, and their strengths and limitations. The authors of [21] described a CC threat classification model based on ML feasibility. Algorithms for detecting and solving security problems. They also suggested CC risk grouping. A model based on the feasibility of ML algorithms to distinguish them. ML algorithms and defenses Techniques have been used to solve security threats and problems in CC [22,23]. Furthermore, they 5 Notable Trends Introduced When Searching for ML Security Threats and Mitigation Strategies proficiency test.

III. Conclusion

The study analyzed security threats and attacks as the top CC challenge. Various types of ML algorithms. B. ANN, K-NN, Naive Bayes, SVM, K-Means, and SVD are It is being researched as a solution to address security issues in CC. We have considered several proposed techniques Used ML algorithms for cloud security. presented an analytical review and analysis of. We have proposed techniques and highlighted their strengths and weaknesses. We also introduced some The direction of research that requires further investigation in the future.

References

[1]. Lim, S.Y.; Kiah, M.M.; Ang, T.F. Security Issues and Future Challenges of Cloud Service Authentication.Polytech. Hung. 2017, 14, 69–89.

[2]. Borylo, P.; Tornatore, M.; Jaglarz, P.; Shahriar, N.; Cholda, P.; Boutaba, R. Latency and energy-aware provisioning of network slices in cloud networks. Comput. Commun. 2020, 157, 1–19. [CrossRef]

[3]. Carmo, M.; Dantas Silva, F.S.; Neto, A.V.; Corujo, D.; Aguiar, R. Network-Cloud Slicing Definitions for Wi-Fi

[4]. Sharing Systems to Enhance 5G Ultra-Dense Network Capabilities. Wirel. Commun. Mob. Comput. 2019, 2019, 1–17. [CrossRef]

[5]. Dang, L.M.; Piran, M.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for healthcare. Electronics 2019, 8, 768. [CrossRef]

[6]. Srinivasamurthy, S.; Liu, D. Survey on Cloud Computing Security. 2020. Available online: https://www. semanticscholar.org/ (accessed on 19 July 2020).

[7]. Mathkunti, N. Cloud Computing: Security Issues. Int. J. Comput. Commun. Eng. 2014, 3, 259–263

[8]. Stefan, H.; Liakat, M. Cloud Computing Security Threats And Solutions. J. Cloud Comput. 2015, 4, 1.[CrossRef] Electronics 2020, 9, 1379 22 of 25

[9]. Fauzi, C.; Azila, A.; Noraziah, A.; Tutut, H.; Noriyani, Z. On Cloud Computing Security Issues. Intell. Inf.

[10]. Database Syst. Lect. Notes Comput. Sci. 2012, 7197, 560–569.

[11]. Palumbo, F.; Aceto, G.; Botta, A.; Ciuonzo, D.; Persico, V.; Pescapé, A. Characterizing Cloud-to-user Latency as perceived by AWS and Azure Users spread over the Globe. In Proceedings of the 2019 IEEE Global

[12]. Communications Conference (GLOBECOM), Taipei, Taiwan, 7–11 December 2019; pp. 1–6.

[13]. Hussein, N.H.; Khalid, A. A survey of Cloud Computing Security challenges and solutions. Int. J. Comput.Sci. Inf. Secur. 2017, 1, 52–56.

[14]. Le Duc, T.; Leiva, R.G.; Casari, P.; Östberg, P.O. Machine Learning Methods for Reliable Resource Provisioning in Edge-Cloud Computing: A Survey. ACM Comput. Surv. 2019, 52, 1–39. [CrossRef]

[15]. Li, K.; Gibson, C.; Ho, D.; Zhou, Q.; Kim, J.; Buhisi, O.; Gerber, M. Assessment of machine learning algorithms in cloud computing frameworks. In Proceedings of the IEEE Systems and Information Engineering Design Symposium, Charlottesville, VA, USA, 26 April 2013; pp. 98–103.
[16]. Callara, M.; Wira, P. User Behavior Analysis with Machine Learning Techniques in Cloud Computing Architectures. In Proceedings of the 2018 International Conference on Applied Smart Systems, Médéa, Algeria, 24–25 November 2018; pp. 1–6.
[17]. Singh, S.; Jeong, Y.-S.; Park, J. A Survey on Cloud Computing Security: Issues, Threats, and Solutions. J. Netw. Comput. Appl. 2016, 75, 200–222.
[18]. Khan, A.N.; Fan, M.Y.; Malik, A.; Memon, R.A. Learning from Privacy Preserved Encrypted Data on Cloud Through Supervised and Unsupervised Machine Learning. In Proceedings of the International Conference on Computing, Mathematics and Engineering Technologies, Sindh, Pakistan, 29–30 January 2019; pp. 1–5.
[19]. Khilar, P.; Vijay, C.; Rakesh, S. Trust-Based Access Control in Cloud Computing Using Machine Learning. In Cloud Computing for Geospatial Big Data Analytics; Das, H., Barik, R., Dubey, H., Roy, D., Eds.; Springer: Cham, Switzerland, 2019; Volume 49, pp. 55–79.
[20]. Subashini, S.; Kavitha, V. A Survey on Security Issues in Service Delivery Models of Cloud Computing. J. Netw. Comput. Appl. 2011, 35, 1–11. [CrossRef]
[21]. Bhamare, D.; Salman, T.; Samaka, M.; Erbad, A.; Jain, R. Feasibility of Supervised Machine Learning for Cloud Security. In Proceedings of the International Conference on Information Science and Security, Jaipur, India, 16–20 December 2016; pp. 1–5.
[22]. Li, C.; Song, M.; Zhang, M.; Luo, Y. Effective replica management for improving reliability and availability in edge-cloud computing environment. J. Parallel Distrib. Comput. 2020, 143, 107–128. [CrossRef]
[23]. Purniemaa, P.; Kannan, R.; Jaisankar, N. Security Threat and Attack in Cloud Infrastructure: A Survey. Int. J. Comput. Sci. Appl. 2013, 2, 1–12.
[24]. Yuhong, L.; Yan, S.; Jungwoo, R.; Syed, R.; Athanasios, V. A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions. J. Comput. Sci. Eng. 2015, 9, 119–133.
[25]. Chirag, M.; Dhiren, P.; Bhavesh, B.; Avi, P.; Muttukrishnan, R. A survey on security issues and solutions at different layers of Cloud computing. J. Supercomput. 2013, 63, 561–592.
[26]. Behl, A.; Behl, K. An analysis of cloud computing security issues. In Proceeding of the World Congress on Information and Communication Technologies, Trivandrum, India, 30 October–2 November 2012; pp. 109–114.