International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Intrusion Detection using Machine Learning

Bhumika Malik[1], Nivedita Singh[2]

[1]bhumika.20scse2030047[at]galgotiasuniversity.edu.in
[2]nivedita.20scse2030050[at]galgotiasuniversity.edu.in

Abstract: ***Aim: This paper aims to evaluate how machine learning is used by many companies to protect and detect various attacks and secure data on the cloud. Background: In this paper, a systematic review is provided of machine learning and its various techniques which are helpful in making the data on cloud secure from various threats such as denial of service attack and data privacy is one of the most common areas in cloud security which should be taken in consideration to protect the data and make cloud secure for every user. Objective: The paper elicitates the requirement of machine learning and identifying various techniques which are used to protect the data on cloud and make it secure for its users to store their data on cloud. Methods: The paper starts with discussing about machine learning and cloud security as an important service provided by cloud. This paper evaluates the potential of machine learning through a case study and discussing techniques in brief which help to make cloud secure for storing data. Also various recent attacks are also analyzed in order to prevent attacks in cloud and provide various methods to improve it. Result: Machine learning plays a key role in enhancing the cloud security capabilities, a platform that uses machine learning in the best possible manner to improve privacy by easily adapting evolving changes. Conclusion: The idea of adapting machine learning in cloud security is prominent and has proved to be. There are various techniques such as vector machines and many others which are widely used in cloud security and also different fields such as in networking. In this paper we have discussed about various other techniques which are preventing and detecting attacks in the cloud.***

Keywords: Cloud, Security, Machine Learning

1. Introduction

Cloud computing is one of the major advancement in technology which offers various services over the internet [1]. The hardware and software data center is called a cloud. When cloud services are available pay per use, then is called a public cloud and when the data is private such as data center of an organization which is not accessible to the general public, then it is called as private cloud [11]. The main objective is to provide their users service of pay only for the services they use, a cloud provides users the on-demand services [1]. Cloud Service Provider (CSP) provide their services using three service models: Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS). Various cloud service providers are Amazon, Google, Microsoft, etc. [10]

With the extension in cloud computing, knowledge about the security state of cloud should be prominent to ensure cloud platform is secure for users to store their data. But, as we all know that we need to keep studying about it, as it is dynamic in nature and changes from time to time [4]. Security is the topmost issue when it comes to advancement in the technology. Information security is one of the premier developing risk which prevents clients to grasp the cloud administration [10]. Major concern of cloud security is to focus on the security issues in cloud computing such as data privacy and encryption, availability of resources under security threat [13]. Maintaining a strong cloud security posture helps organizations to achieve widely recognized benefits of cloud computing.

Machine learning is an application of artificial intelligence (AI) which provides various computer algorithms which learns and improves automatically through experience and by the use of data [1]. Example of machine learning speech recognition, navigation and automatic driving can be imagined through this technology. Models are evaluated over various experimentally generated dataset aggregate. In result, these models may not give a positive result with other data sets [9]. In this paper, we have discussed various techniques of ML which can be used to deal with the issues of cloud security. This review is divided into various sections: Section II includes the literature review, Section III discusses about the techniques to enhance cloud security, Section IV includes the results about this review and Section V concludes what further should be done to enhance the security at cloud platform.

2. Literature Review

A. Cloud Computing Security

In this section, we have discussed the privacy or security issues which may arise in the cloud computing platform because it provides its services on the internet and it may lead to various security issues [1].

The attacks which most often occur in cloud computing are:

Denial of Service (DoS) attack: It is an attempt to affect the availability of service for the users of cloud and the user is not able to respond to requests.

Zombie Attack: In this, the attacker floods the victim by sending requests from innocent hosts in the network.

Phishing Attack: It is a type of attack in which the personal information is collected and manipulated by redirecting them to a false link.

Man-in-the Middle Attack: In this, the attacker accesses the communication path between two users as an intruder and access the information.

There are many other attacks too, such as cloud malware injection attack, breach of confidentiality, authentication attacks, attacks on virtualization, etc.

B. Distributed Machine learning (DML)

Distributed machine learning is a building block of the technologies. It increases the performance, accuracy and also deals with large data [16]. The recent framework of distributed machine learning includes mainly the MapReduce-Based system, Graph Model-Based system and parameter server system [6].

MapReduce-Based systems are widely implemented with the two practical algorithms Hdoop and Spark. Graph model-Based systems are better for parallel machine leraning and it uses more flexible algorithms which are Graphla and Pregel. This method is more complex as compared to other systems [6].

C. Intrusion Detection Systems (IDS)

Intrusion detection system is an application which detects the intrusion i.e., malicious and policy violation activities and reports about it to administrator [3].

Table 1

Survey	Year	Description	Difference
[16]	2020	This paper examines the numerous Cloud infrastructure raised in cloud platforms. Besides, they provide a new class	It covers Cloud computing and its security issues, threats, and provide solutions.
"A Survey on the Security of Cloud Computing"[17]	2019	ficant attacks against possible countermeasures for comparative analysis	It covers Cloud security attacks, threats, and protection methods. Does not cover Machine learning methods
vulnerabilities, and countermeasures: A survey"[18]	2019	security taxonomy, risks, vulnerabilities, and counter in other relevant fields, such as trust-based security architectures, large-scale, IoT, SDN, and Network Function Virtualization (NFV)	It covers a wide aspect of Cloud security issues varying from the vulnerabilities, risks, threats in different fields. But it does not cover machine learning techniques.
"A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures"[19]	2019	This paper conceptual level, data level, and reviews the cloud identities and ses several	It covers Cloud computing and its security issues, threats, and provide solutions.
[20]	2019	among them.	It covers ML techniques on mobile malware detection.
"Cloud security issues and challenges" [21]	2018	issues, and the issues of service models as well.	It covers Cloud security issues and challenges.
Cloud service for CIDPS" [22]	2018	This research	It covers Cloud security in big data.
"A survey of deep learning-based network anomaly detection" [13]	2017	ning techniques analysis to compare accuracies.	It covers Cloud anomaly detection using DL.
"A survey on attack detection on Cloud [23]	2016	threats.	Covers only Cloud computing and its security issues only.
"Security and privacy for big data: A systematic literature review" [24]	2016	g data papers related to security or privacy.	It covers the big data issues in Cloud.
"A review on intrusion detection techniques for Cloud computing and security challenges" [25]	2015	attacks, types of system One of those techniques is ML.	It covers Cloud intrusion detection only.
[26]	2013	computing in detail.	It covers Cloud security only. They do not discuss ML techniques.
"A survey of intrusion detection techniques in Cloud" [27]	2013	discussed, along with the techniques for solving these threats.	Although some of the solutions are ML related, they are not thoroughly discussed.
review" [28]	2013		It covers intrusion detection in Cloud only.
attack detection in Cloud computing" [29]	2012	identifying types are used, best choice.	It covers both Cloud security and ML techniques. However, those experiments are done by the authors and not by related researchers.
attacks in Cloud computing" [1]	2011	solutions using ML techniques.	Although it covers Cloud computing, the proposed solution is limited to one "proactive attack detection."

Host Based IDS: It mainly functions on the internal monitoring of the normal behavior and checking system logs that if there any deviation or changes in the normal behavior.

Network-Based IDS: It mainly functions on the pattern of the packets in which the data is sent and checks if there is pattern other than the patter which seems to be suspicious.

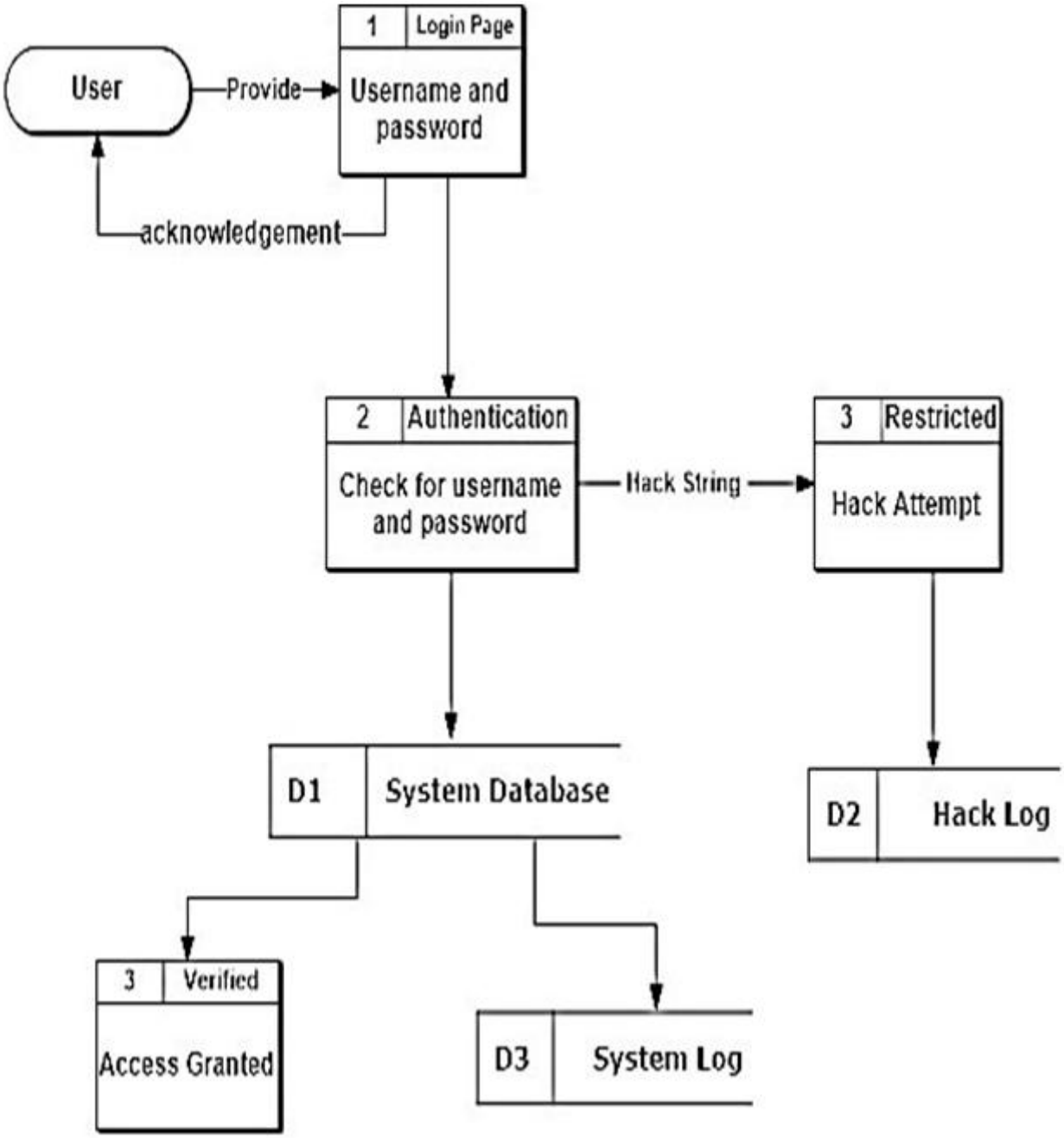
Fuzzy logic is a method which resembles human reasoning. It includes all possibilities of yes and no.It defines some rules and includes Fuzzifier (fuzzy input set) and Defuzzifier (fuzzy output set) [3].

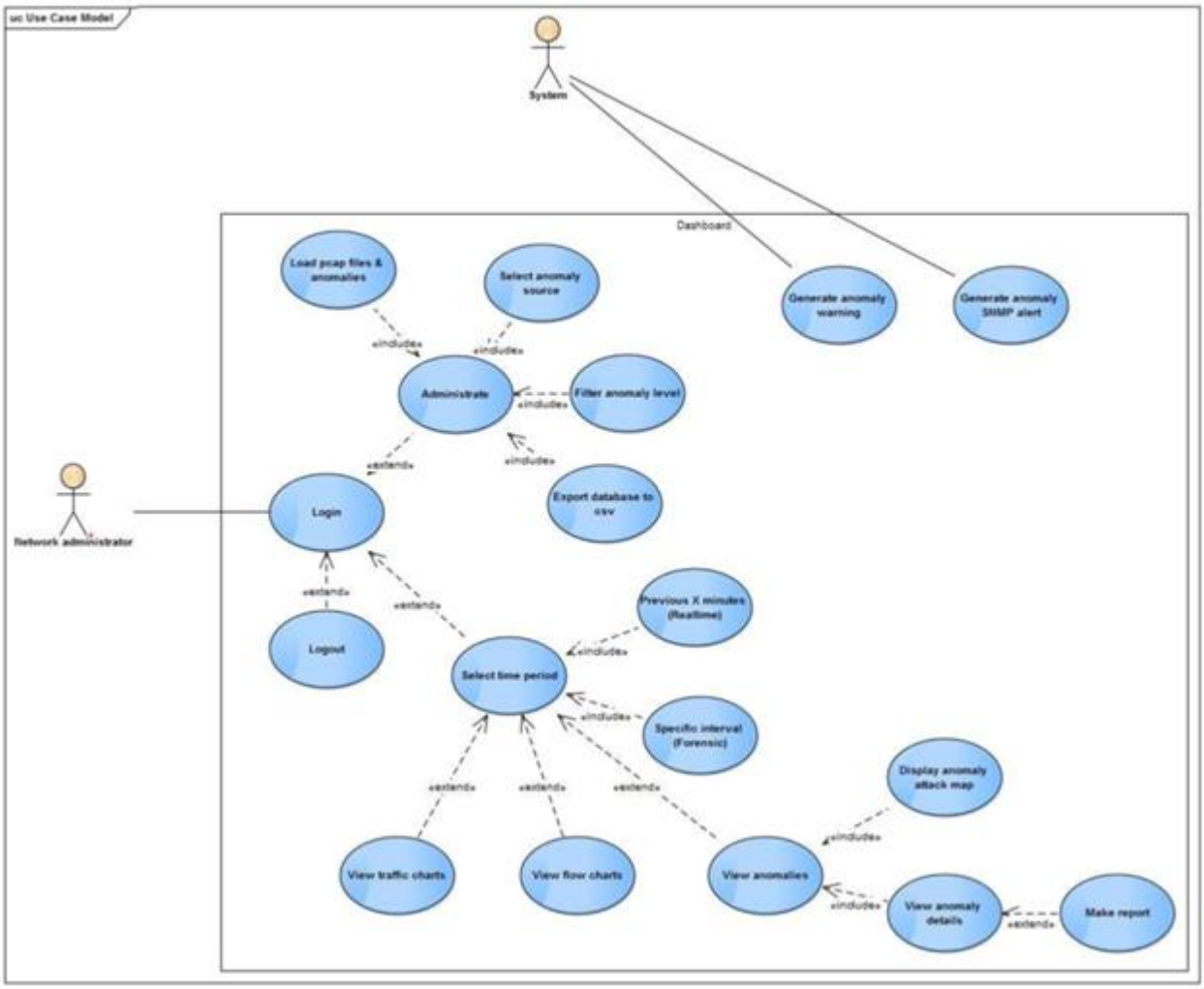
D. Attack Detection For Cloud Using Machine Learning Techniques

ML is used in many ways for detecting the cloud attacks. Table 1 shows the work or surveys/reviews related to cloud security issues or various machine learning techniques which are used for cloud security [1].

3. DFD

The diagram in figure illustrates the flow of data in the system. The user supplies a username and password to gain access into the system after which an acknowledge message is sent to the user specifying if the login was successful or denied. The user credentials goes through an authentication process to determine if it's a hack attempt or a valid user. This information is stored in hack attempt log or system log respectively.





4. Use case Diagram

From the diagram in figure 1.0 show various actors as seen in table 1.0. The actor could be an authorized user, a hacker or system administrator who will only gain access through the login page (user case), the administrator would be able to view the user active on the system, the hack logs, user logs and the user profiles.

References

[1] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," in IEEE Access, vol. 9, pp. 20717-20735, 2021, doi: 10.1109/ACCESS.2021.3054129.

[2] Adnan Qayyum, Aneeqa Ijaz, Muhammad Usama1, Waleed Iqbal, Junaid Qadir, Yehia Elkhatib, Ala Al-Fuqaha, Securing Machine Learning in the Cloud: A Systematic Review of Cloud Machine Learning Security, Big Data, 12 November 2020, Volume 3, https://doi.org/10.3389/fdata.2020.587139.

[3] A. ELMAARADI, A. LYHYAOUI and I. CHAIRI, "New security architecture using hybrid IDS for virtual private clouds," 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS), 2019, pp. 1-5, doi: 10.1109/ICDS47004.2019.8942383.

[4] I. Avdagic and K. Hajdarevic, "Survey on machine learning algorithms as cloud service for CIDPS," 2017 25th Telecommunication Forum (TELFOR), 2017, pp. 1-4, doi: 10.1109/TELFOR.2017.8249467.

[5] T. Y. Win, H. Tianfield and Q. Mair, "Big Data Based Security Analytics for Protecting Virtualized Infrastructures in Cloud Computing," in IEEE Transactions on Big Data, vol. 4, no. 1, pp. 11-25, 1 March 2018, doi: 10.1109/TBDATA.2017.2715335.