Exploring the Role of Machine Learning in Enhancing Cloud Security

M. Amshavalli[1] ; R. Kishore[2] ; S.P. Raguvijay[3] ; S. Sri Shyam[4]
Assistant Professor[1], Students [1 2 3], Department of Computer Science and Engineering,
Erode Sengunthar Engineering College,
Perundurai, Erode, Tamil Nadu, India.

Abstract:- The use and acceptance of cloud computing are growing quickly. Numerous businesses are making investments in this area, either for their own needs or to offer services to others. The rise of the cloud has led to a number of security issues for both consumers and businesses. Machine learning is one method of cloud security (ML).

ML approaches have been applied in a variety of ways to stop or identify online threats and security holes. We present a Systematic Literature Review (SLR) of cloud security and machine learning approaches and techniques in this work. After 63 pertinent papers were examined, the SLR's findings were divided into three primary study areas: I. The many forms of cloud security

Keywords:- *DDOS, Machine Learning, Cloud Security, Privacy, And Security.*

I. INTRODUCTION

A recent technical development is cloud computing, which provides information technology infrastructure, software, and platforms as online services.

Said to be the realization of a long-standing idea, "Cing Us," it is progressively adopted by businesses as private, public, or hybrid clouds. Its primary goal is to enable consumers to use and pay for what they want, offering on-demand services for their infrastructure or software requirements.

Despite being viewed as a significant and positive change in IT architecture, cloud computing still requires a lot of security work to mitigate vulnerabilities.

A significant quantity of corporate and personal data is stored in cloud data centers, thus it is necessary to identify and prevent cloud security risks.

Due to the fact that the associate editor overseeing this manuscript's evaluation and approval.

II. LITERATURE SURVEY

A. An Effective Detection and Prevention System for DDOS TCP Flood Attacks in a Cloud Setting

Assuring the availability and security of project data, services, and resources remains a critical and difficult research subject, notwithstanding the recent sharp rise in the number of cloud projects.

After information theft, distributed denial of service (DDOS) assaults are the second most common type of cybercrime. DDOS TCP flood attacks quickly destroy an entire cloud project by using up all of the cloud's resources and bandwidth. Thus, it is imperative that such assaults in cloud projects be promptly detected and prevented, particularly for e Health clouds.

We provide a novel classifier system in this research that can identify and stop DDOS TCP flood assaults (CS_DDOS) in public clouds. The suggested CS DDOS system provides a way to protect data that is held

B. A Systematic Review of Cloud Computing Security Literature: Threats and Mitigation Techniques

In both academia and business, cloud computing research is now being extensively utilized. Customers and cloud service providers (CSPs) both profit from cloud computing. Numerous studies have been conducted in the literature about the security issues related to cloud computing.

The purpose of this systematic literature review (SLR) is to examine the extant literature on cloud computing security, dangers, and difficulties. This SLR looked at research papers that were published in popular digital libraries from 2010 and 2020. After a careful review of available studies, we chose 80 papers that address the suggested research questions.

This SLR's findings identified seven significant security risks to cloud computing systems. The findings indicated that among the most talked-about subjects in the selected literature were data manipulation and leaks.

C. A Survey of Privacy Protection and Data Security for Cloud Storage

The digital transformation of businesses, the Internet of Things (IOT), smart cities, and the global economy are among the emerging development trends.

Due to the enormous amount of data collected, the strain on data storage is only going to increase, propelling the quick expansion of the whole storage business. The ability to store and manage data makes cloud storage systems an essential component of the modern world. Governments, businesses, and individual users are currently actively moving their data to the cloud. An enormous volume of data may provide enormous riches.

On the other hand, this raises the possibility of risks such data leakage, illegal access, revelation of sensitive information, and privacy disclosure. There are research on data security and privacy protection, but comprehensive surveys on the topic are still lacking.

D. Mscryptonet: Deep Learning with Multi-Scheme Private Preservation in Cloud Computing

A major concern for ubiquitous healthcare systems that rely on collected data and cooperative deep learning amongst several stakeholders is privacy in the Internet of Things. In this study, a novel framework called MSCryptoNet is proposed, which allows the conversion of the state-of-the-art trained neural network to MSCryptoNet models in a privacy-preserving manner, and allows for its scalable execution.

Additionally, we provide a low degree polynomial approach for approximating the activation function, which is essentially employed in convolution neural networks (i.e., Sigmoid and Rectified linear unit). This method is essential for computations in homomorphic encryption schemes. The following situations appear to be the focus of our model: 1) A workable method for requiring the classifier's assessment whose inputs are encrypted using potentially distinct encryption techniques.

E. Next-Generation Neural Networks: Capsule Networks for Text Classification with Routing-by-Agreement

Neural networks are now widely recognized as a crucial component of learning systems technology because to their continual demonstration of high capacity for almost all application cases.

But in order to handle newly presented challenges—such as growing task complexity, explain ability of decision-making processes, expanding issue areas, and delivering strong and resilient systems—neural networks must constantly advance. The novel Capsule Network (Caps Net) technology represents a potential improvement over conventional neural networks. It blends the expressiveness of distributed entity representations with an intelligent and interpretable signal propagation known as routing-by-agreement.

Given that Caps Nets are still a relatively new concept, further study is necessary to fully understand Caps Net theory and develop optimal practices for a variety of application domains. The purpose of this study is to advance caps nets.

F. Deep Learning-Based Cloud-Based Cyber-Physical Intrusion Detection for Vehicles

Interest in the detection of cyber attacks on automobiles is rising.

Vehicles usually have limited processing resources, thus rule-based or lightweight machine learning approaches are suggested as alternatives. We contend that computational offloading, which is frequently employed for mobile devices with limited resources, can overcome this restriction. This gives access to more sophisticated procedures due to the greater processing resources made available.

We illustrate the viability and advantages of outsourcing the ongoing deep learning-based intrusion detection work using a tiny four-wheel robotic land vehicle as a case study. Compared to typical machine learning approaches, our methodology regularly achieves high accuracy and is not restricted to a specific type of attack or the in-vehicle CAN system like earlier work. It utilizes data as input.

G. Posedstacked Sparse Autoencoder in a Hyperband Tuned Deep Neural Network for the Detection of D Dos Attacks Incloud

Cloud computing offers several alluring characteristics, such as completely managed computer system resources and services, as well as elastic and on-demand capabilities.

However, the cloud environment is vulnerable to many cyber-attacks and security concerns connected to cloud model because of its dispersed and dynamic nature as well as flaws in virtualization implementation. A few of these include the inability to access data entering or leaving cloud services, theft and abuse of hosted data, lack of control over access to sensitive data, and advanced threats such as distributed denial of service (DDOS), malware injection assaults, virtual machine escape, and wrapping attacks. One of the most well-known attacks is DDOS.

Although there are several viable methods for detecting DDOS assaults, the frequency and strength of current attacks are growing, and there are always.

H. A Systematic Review, Analysis, and Outlook on Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments

The cloud environment is becoming more and more popular among academics, government agencies, and commercial businesses because it offers maximum scalability, little upfront capital requirements, and other benefits. The cloud environment supports many advantages, but it also has a number of drawbacks.

When it comes to cloud computing and information security, data protection is the main worry. Various approaches have been devised to tackle this problem. Nevertheless, a thorough examination of the current solutions is lacking, therefore it becomes necessary to investigate, categorize, and evaluate the substantial body of prior research in order to determine if these solutions may be used in order to satisfy the criteria. In-depth research, a methodical comparison, and a thorough examination of the most effective methods for safe sharing and safeguarding.

I. An Algorithm for Virtual Machine Consolidation for Cloud Data Center Based on the Ant Colony System and the Extreme Learning Machine

The issue of large-scale data centers' energy use is getting more and more attention. By moving virtual machines from one physical computer to another, virtual machine consolidation may drastically save energy use.

On the other hand, serious Service Level Agreement (SLA) violations might result from excessive virtual machine consolidation. Thus, there is a dilemma that has to be resolved regarding how to efficiently strike a balance between efficient energy use and avoiding SLA breaches. It is NP-hard to solve the virtual machine consolidation problem.

Certain meta-heuristic algorithms can assist in preventing the local optimum state, which the standard heuristic method is prone to. On the other hand, the complexity of the current meta-heuristic algorithms is rather considerable. Therefore, we present a reduced complexity multi-population ant colony system method using the Extreme Learning Machine (ELM) prediction (ELM_MPACS).

J. Cloud Computing Environment: Distributed Machine Learning Oriented Data Integrity Verification Scheme

AI is based on several key technologies, one of which is distributed machine learning (DML). Nevertheless, data integrity is not considered in the current distributed machine learning architecture.

The training model in the distributed machine learning system will be significantly impacted and the training results will be incorrect if network attackers falsify, alter, or delete the data. As such, ensuring data integrity in the DML is essential. To guarantee the integrity of training data, we provide in this work a distributed machine learning oriented data integrity verification technique (DML-DIV).

The Provable Data Possession (PDP) sample auditing technique is the first notion we use to provide data integrity verification, which makes our DML-DIV scheme resistant to fabrication.

III. EXISTING SYSTEM

- Because cloud computing uses the Internet to convey data and host its infrastructure, it is a tremendously large industry.
- It charges according to the demands of the clients and offers services to suit their needs. The fact that consumers are beginning to rely on the Cloud and that businesses can now readily acquire Cloud services underscores its significance. Cloud service companies are concerned that users may abuse their systems to launch attacks.
- The expectations of their companies and the facilities they will receive from a certain provider are the primary factors in choosing a cloud provider. Vulnerabilities in cloud security that an adversary may exploit to get access to the network and other infrastructure resources. A cloud threat is an unfavorable event that might happen maliciously

➢ *Disadvantages*

- The resource-intensive processing can lead to increased energy consumption, affecting the battery life of IoT devices.
- Relying on ECG and PPG signals limits its applicability in scenarios where additional data sources are necessary for comprehensive cardiac monitoring.
- The system's use of DWT and signal quality index calculations adds computational complexity, potentially straining resource-limited IoT devices

IV. PROPOSED SYSTEM

It is simple to make their suggested job better by giving it additional features or making it capable of detecting new kinds of assaults. The suggested method uses support vector machines, which are more accurate and efficient when paired with J48. We suggest a hybrid algorithm for quicker, more accurate, and more efficient outcomes when identifying DDOS assaults using the fundamental feature choices.

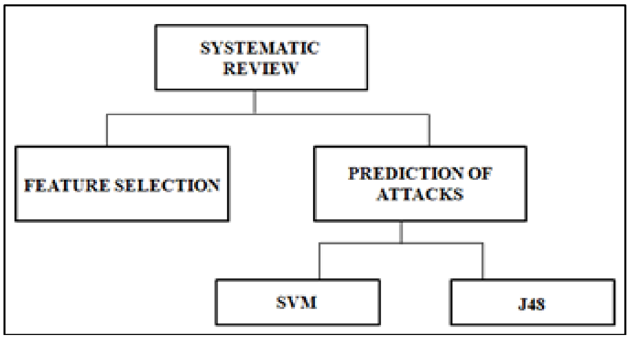
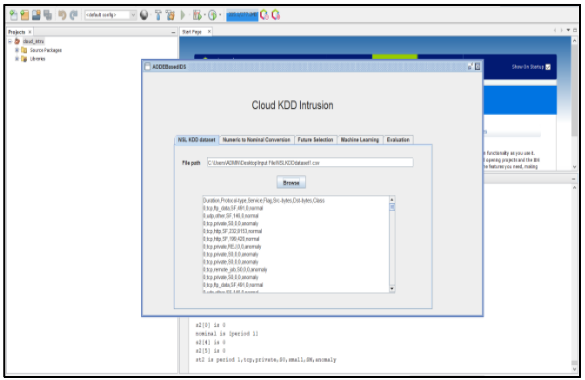


Fig 1 Architecture Diagram

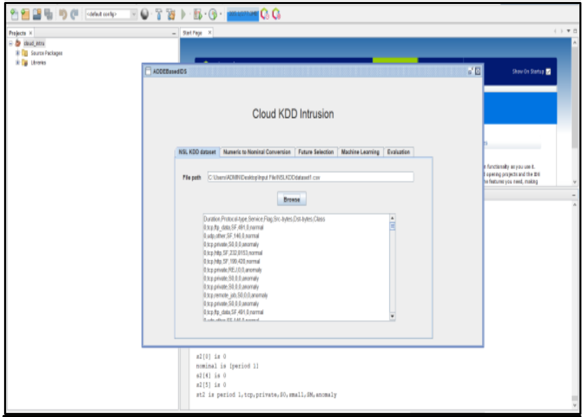
V. SCREENSHOTS



File path C:\Users\ADMIN\Desktop\Input File\NSLKDDdataset1.csv

```
Duration,Protocol-type,Service,Flag,Src-bytes,Dst-bytes,Class
0,tcp,ftp_data,SF,491,0,normal
0,udp,other,SF,146,0,normal
0,tcp,private,S0,0,0,anomaly
0,tcp,http,SF,232,8153,normal
0,tcp,http,SF,199,420,normal
0,tcp,private,REJ,0,0,anomaly
0,tcp,private,S0,0,0,anomaly
0,tcp,private,S0,0,0,anomaly
0,tcp,remote_job,S0,0,0,anomaly
0,tcp,private,S0,0,0,anomaly
0,tcp,ftp_data,SF,491,0,normal
```

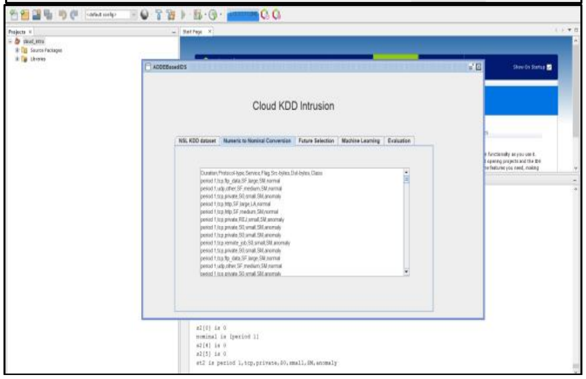
```
s2[0] is 0
nominal is [period 1]
s2[4] is 0
s2[5] is 0
st2 is period 1,tcp,private,S0,small,SM,anomaly
```



File path C:\Users\ADMIN\Desktop\Input File\NSLKDDdataset1.csv

```
Duration,Protocol-type,Service,Flag,Src-bytes,Dst-bytes,Class
0,tcp,ftp_data,SF,491,0,normal
0,udp,other,SF,146,0,normal
0,tcp,private,S0,0,0,anomaly
0,tcp,http,SF,232,8153,normal
0,tcp,http,SF,199,420,normal
0,tcp,private,REJ,0,0,anomaly
0,tcp,private,S0,0,0,anomaly
0,tcp,private,S0,0,0,anomaly
0,tcp,remote_job,S0,0,0,anomaly
0,tcp,private,S0,0,0,anomaly
0,tcp,ftp_data,SF,491,0,normal
```

```
s2[0] is 0
nominal is [period 1]
s2[4] is 0
s2[5] is 0
st2 is period 1,tcp,private,S0,small,SM,anomaly
```



```
Duration,Protocol-type,Service,Flag,Src-bytes,Dst-bytes,Class
period 1,tcp,ftp_data,SF,large,SM,normal
period 1,udp,other,SF,medium,SM,normal
period 1,tcp,private,S0,small,SM,anomaly
period 1,tcp,http,SF,large,LA,normal
period 1,tcp,http,SF,medium,SM,normal
period 1,tcp,private,REJ,small,SM,anomaly
period 1,tcp,private,S0,small,SM,anomaly
period 1,tcp,private,S0,small,SM,anomaly
period 1,tcp,remote_job,S0,small,SM,anomaly
period 1,tcp,private,S0,small,SM,anomaly
period 1,tcp,ftp_data,SF,large,SM,normal
period 1,udp,other,SF,medium,SM,normal
period 1,tcp,private,S0,small,SM,anomaly
```

```
s2[0] is 0
nominal is [period 1]
s2[4] is 0
s2[5] is 0
st2 is period 1,tcp,private,S0,small,SM,anomaly
```

VI. CONCLUSION

We conducted a thorough analysis of the literature to examine ML methods used to cloud security.

The study looked at pertinent works that addressed three research questions: the field of cloud security, the nature of the ML approaches employed, and the ML model's accuracy estimation. After using our selection criteria, we ultimately received 60 research publications. Furthermore, we found that the application of deep learning methods to cloud security has not received much attention.

In this sense, we urge researchers to leverage deep learning.

REFFERENCES

[1]. OWUSU-AGYEMANG. KWABENA, ZHEN QIN, TIANMING ZHUANG, AND ZHIGUANG QIN MSCryptoNet: Multi- Scheme Privacy-Preserving Deep Learning in Cloud Computing, publication February 25, 2019,

[2]. NIKOLAI A. K. STEUR AND FRIEDHELM SCHWENKER, (Member, and IEEE) Next-Generation Neural Networks: Capsule Networks with Routing- by-Agreement for Text Classification publication September 7, 2021

[3]. GEORGE LOUKAS, TUAN VUONG, RYAN HEARTFIELD, GEORGIA SAKELLARI, YONGPIL YOON, AND DIANE GAN Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning Publication December 11, 2017

[4]. AANSHI BHARDWAJ, VEENU MANGAT, (Member, IEEE), AND RENU VIG Hyper band Tuned Deep Neural Network with Well Posed Stacked Sparse Auto Encoder for Detection of DDoS Attacks in Cloud Publication October 5, 2020.

[5]. CHUNG-NAN ASHUTOSH KUMAR SINGH, AND ISHU GUPTA LEE1 AND, RAJKUMAR BUYYA , Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions publication 4 July 2022.

[6]. FAGUI LIU, ZHENJIANG MA, BIN WANG , AND WEIWEI LIN A Virtual Machine Consolidation Algorithm Based on Ant Colony System and Extreme Learning Machine for Cloud Data Center publication December 23, 2019

[7]. XIAO-PING ZHAO AND RUI JIANG Distributed Machine Learning Oriented Data Integrity Verification Scheme in Cloud Computing Environment publication February 4, 2020

[8]. ÁLVARO LÓPEZ GARCÍA, JESÚS MARCO DE LUCAS, MARICA ANTONACCI, WOLFGANG ZU CASTELL, MARIO DAVID , MARCUS HARDT, LARA LLORET IGLESIAS, GERMÁN MOLTÓ, MARCIN PLOCIENNIK , VIET TRAN A Cloud- Based Framework for Machine Learning Workloads and Applications publication January 6, 2020

[9]. MUHAMMAD MEHMOOD, RASHID AMIN, MUHANA MAGBOUL ALI MUSLAM, (Member, IEEE), JIANG XIE, AND HAMZA ALDABBAS Privilege Escalation Attack Detection and Mitigation in Cloud Using Machine Learning publication 8 May 2023

[10]. KAUSHIK SEKARAN, MOHAMMAD S. KHAN, RIZWAN PATAN , AMIR H.

[11]. GANDOMI, PARIMALA VENKATA KRISHNA, AND SURESH KALLAM Improving the Response Time of M-Learning and Cloud Computing Environments Using a Dominant Firefly Approach publication February 12, 2019