International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

Cloud Security Solutions Through Machine Learning- Approaches:A Survey

K. Samunnisa[1], G. Sunil Vijaya Kumar[2], K. Madhavi[3]

[1]Research Scholar
[2]Professor, Department of Computer Science and Engineering, Global college of engineering and technology, Kadapa.
[3]Professor,HOD, Computer Science and Engineering, JNTUA College of Engineering, Ananthapur, A.P

ABSTRACT: Large-scale computation, data storage, virtualization, high efficiency, high reliability, and low prices are among the cloud computing services that are made available to the consumer. The storage of data in cloud is more sensitive to users as it is stored in the third party storage and it is one of the major problems identified. Data protection consists of a variety of regulations, protocols, processes and techniques, which operate together to secure cloud-based services, networks and data. All these protection mechanisms are intended to secure data, secure customer privacy, and promote compliance with regulations and set system and user authentication guidelines. Cloud security issues are DDoS threats, violations of privacy, lack of privacy and insecure access points. Researchers have performed an investigation into many intrusion prevention methods for cloud infrastructure detection of intrusion. Most of them address conventional intrusion and anomaly detection strategies and concentrate on best practice in cloud protection, such as server &security for virtualization, host and middleware, and device and data. The current study concentrates on issues related to cloud computing and machine learning. Problems with potential significance are known as related open problems.

Keywords: Anomaly detection, Cloud Storage, cloud computing, machine learning techniques, Supervised- and Unsupervised-learning

1. INTRODUCTION

In recent years, cloud-based data storage features have become more prominent. Furthermore, because of the cost savings and increased reliability, businesses are moving their data to these servers. Furthermore, it is used in non-traditional industries such as online gaming and social media to handle large computing capacities. Between now and 2024, there will be a 12.64 billion USD global demand for cloud protection. This is powered by the growing usage of cloud computing for data storage and advances in cyber threats [1]. It could be a regulatory-regulatory-governance-and-data-protection-oriented tool or service. 95% of cloud failures will be attributed to the organisation. About 70% of all cloud-based businesses have cloud protection risks, so all enterprises should consider cloud security protection. Cloud computing offers many opportunities, like many other technical technologies. In addition, this means that an almost limitless amount of data, as well as various resources, could be stored. This has met the challenge of resource limitations and lowered transaction costs by exchanging different services in high demand with those who have more of the service. The

cloud's modular design allows for quick information access, smooth connectivity, data control, and cost-efficiency. The quality of services necessitates consistency.

To prevent security threats, the mechanisms in use [2] several questions have arisen about data protection and cyber security, but because mission-critical technologies are moving into the cloud, these questions have now become more pressing.

The application of cloud computing is one of the most important issues technical analysis has dealt with over the past few years. Data storage, network security, and device security are all studied here. A combination of flexibility, universal access, and convenient service provider interaction called cloud computing is described by NIST[3] as being a "platform for flexible resource pooling, universal, on-demand access that can be conveniently provided through various forms of service provider interaction" [4].

One of the facets of cloud computing is that it differentiates between the cloud computing paradigm, in which there are certain types of cloud infrastructure that are dictated by their complexity, ownership, and accessibility, and the other cloud computing aspects, which include things like cloud architecture. Cloud storage is enabled when individual computers or local servers share resources. The cloud's primary purpose and essence are tied to the architecture model. A business model implementing three different types of cloud architectures is known as an implementation model [5].

Computers and networks have a significant impact on our day-to-day lives for the reasons stated above, so data security is a critical field of study. Antivirus applications, firewalls, and IDSs are all used in cyber-security strategies. By using these techniques, threats from the inside and the outside are avoided. An IDS (also known as an intrusion detection system) is a system that is critical to network security because it is the main way to detect changes in the system.

In order to solve the previously stated problems, IDSs are currently being developed using machine learning techniques. ML is a kind of artificial intelligence technology that allows computers to search for large datasets and identify useful information automatically [6]. On the other hand, if adequate training data is available, machine-based IDS (also known as machine-based IPS) can be utilised at a sufficient level, and machine-based learning models are flexible enough to identify attack types and new attacks.

This survey seeks to summarise all the IDSs to date and distil the main ideas of using machine learning to address security issues, while also identifying existing problems and possible future developments [7-9].

This paper discusses previous surveys' shortcomings and offers an in-depth description of threat models, threats, and IDS techniques in a cloud environment. We would like to present the following findings:

- Discuss definitions and problems in cloud defence
- Clarify Cloud IDS Classification System Taxonomy
- Comprehensive IDS Basic Machine Learning Algorithms Investigation
- Machine Learning-based study on IDSs and their problems

Thus, the remainder of the paper is laid out as follows. In Section 2, Cloud Security Categories and Issues are given, while in Section 3, IDS evaluation is described, in Section 4, IDS using machine learning algorithms is addressed, and in Section 5, on machine learning-based IDS, an exploration of the research is presented, and finally, in Section 6, the main issues in cloud security are identified.

2. CLOUD SECURITY CATEGORIES AND ISSUES

Cloud encryption secures the data stability of all public and private databases. Platform as a Service (PaaS), Software as a Service (SaaS), and cloud device security are used to protect cloud applications.
The solution offered in this paper contributes greatly to this analysis by investigating the latest cloud-protection problems and pioneering technology solutions. 28 securities issues, and classified them into five different categories (Table 1). Most up-to-date security strategies and measures are often closely connected.

2.1 Categories and Issues

In the following 5 categories we classify cloud computing security issues, which are also summarized in Table 1. Similar to how [10] classifies the security issues for clouds, the above approach identifies four cloud security concerns.
Category 1: Regulatory and regulating bodies that specify cloud protection policies to protect a cloud operating environment are dealt with in the Class Security Requirements. It includes service level agreements, reviews, and agreements with customers, service providers, and other stakeholders.
Category 2: The network category refers to the method through which users connect to cloud networks in order to do the required calculations. It entails the use of plugins, network connections, and the sharing of login information.
Category 3: The Access Control category is a user-focused sector that deals with recognition, authorization, and authorization issues.
Category 4: Cloud Computing refers to security issues in SaaS, PaaS, and IaaS, and is especially relevant in the virtualization context.
Category 5: Data security and confidentiality are addressed in the privacy division.

Table 1 Cloud Security Categories.

Category No	Category	Description
Category 1	Security Standards	It describes the safeguards required to protect against cyberattacks in the cloud. Cloud storage policies are configured with a new system for better protection, with no impact on security or performance.
Category 2	Network	This includes network attacks, such as server connection failure, distributed denial of service (DDoS), network flooding, web application vulnerabilities, and so on.
Category 3	Access Control	Manages security and access control. User identity and data storage protection are problems it deals with.
Category 4	Cloud Infrastructure	Contains information about cloud infrastructure-specific threats. Consider, for example, tampered binaries and insiders with privileges (IaaS, PaaS, and SaaS).
Category 5	Data	The features mentioned above are used to address data security issues, especially regarding data transfer, completeness, encryption, and data protection.

One of the most important components of cloud computing reliability is auditability, however we don't have a cloud provider audit network [11, 12]. Consumers must be able to control the entire operation when the vendor provides a service to a third party that lacks obvious features. Service Level Agreements (SLA) and legislative frameworks are not integrated into cloud computing operations [12, 13]. Security standards (C1) and regulatory bodies are part of Service Level Agreements (SLA) and legislative frameworks, respectively.

Because cloud computing is more prone than traditional computer paradigms to target networks, the network category (C2) is seen as the most serious safety hazard in clouds [14]. In addition, cloud activities are intertwined and largely reliant on networking. Security problems with cloud networks are also given more attention in this review than other security groups.

Because many cloud service providers rely solely on rapid and low-cost performance [15], Quality of Service (QoS) is an unaddressed issue [13]. In this job, we consider QoS in the context of any feature or operation that has a direct or indirect impact on security. In order for many providers to exchange system configurations, a little failure in the configuration of one or more cloud components can have significant consequences [16].

Data redundancy[17], data retention and leakage[18], data location[19], data replication [16], privacy [19], data protection[20], and data availability[20] are all significant and essential problems that require data to be appropriately stored, shared, secured, managed, and available in times of need.

3. EVALUATION OF CLOUD-BASED IDS

Several scholars have adapted the standard IDS Method to the cloud world "The European Union Agency for Network and Information Security (ENISA)" has been working hard to overcome many cloud-related security issues. It gives customers knowledge that lets them identify, analyze and handle risks as they transition to the clouds. It also offers consultancy services on SLAs to maximize safety benefits. ENISA also conducts joint projects with different partners to identify core cloud services and evaluate in those situations the consequences of the cloud service failure.

3.1 Intrusion Detection Systems (IDS)

For IDS, an intruder involves an attempt to access information about computer networks or to unlawfully or unlawful harm to system operations.

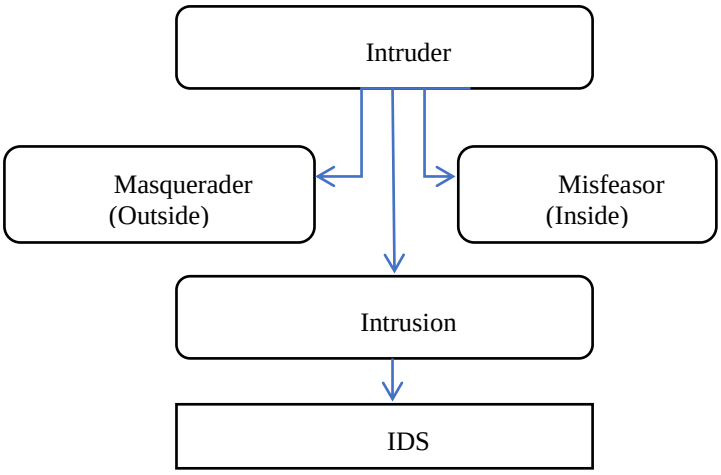

Figure 1. IDS System Structure

An IDS[21] is a data safety programme intended to identify a wide variety of flaws, from alleged compromises by external parties to device exploitation and harassment by insiders, as shown in Figure 1. IDS' essential functions are to track hosts and networks, evaluate computer system behaviours, produce warnings and respond to unusual behaviours. As IDSs are typically used to close secure network nodes (e.g. switches in major network areas), because of their control of relevant hosts and networks.

An IDS classification method, such as an approach based on identification, exists, and another, such as a method based on data sources, does not. The potential for IDS to break down can be broken down into signature-based or misuse-based IDS as well as anomaly-based IDS. Host-based and network-based IDSs can be classified according to data source-based methods [22]. Classification is focused on the data source, with the identification system serving as a secondary classification feature. This visual demonstrates the current IDS grouping, as seen in Figure 2. Machine learning techniques are studied here, with an emphasis on identification techniques. In addition, in Section 4, you will be able to gain an in-depth understanding of machine learning techniques and their applicability to IDSs, using a wide range of data.

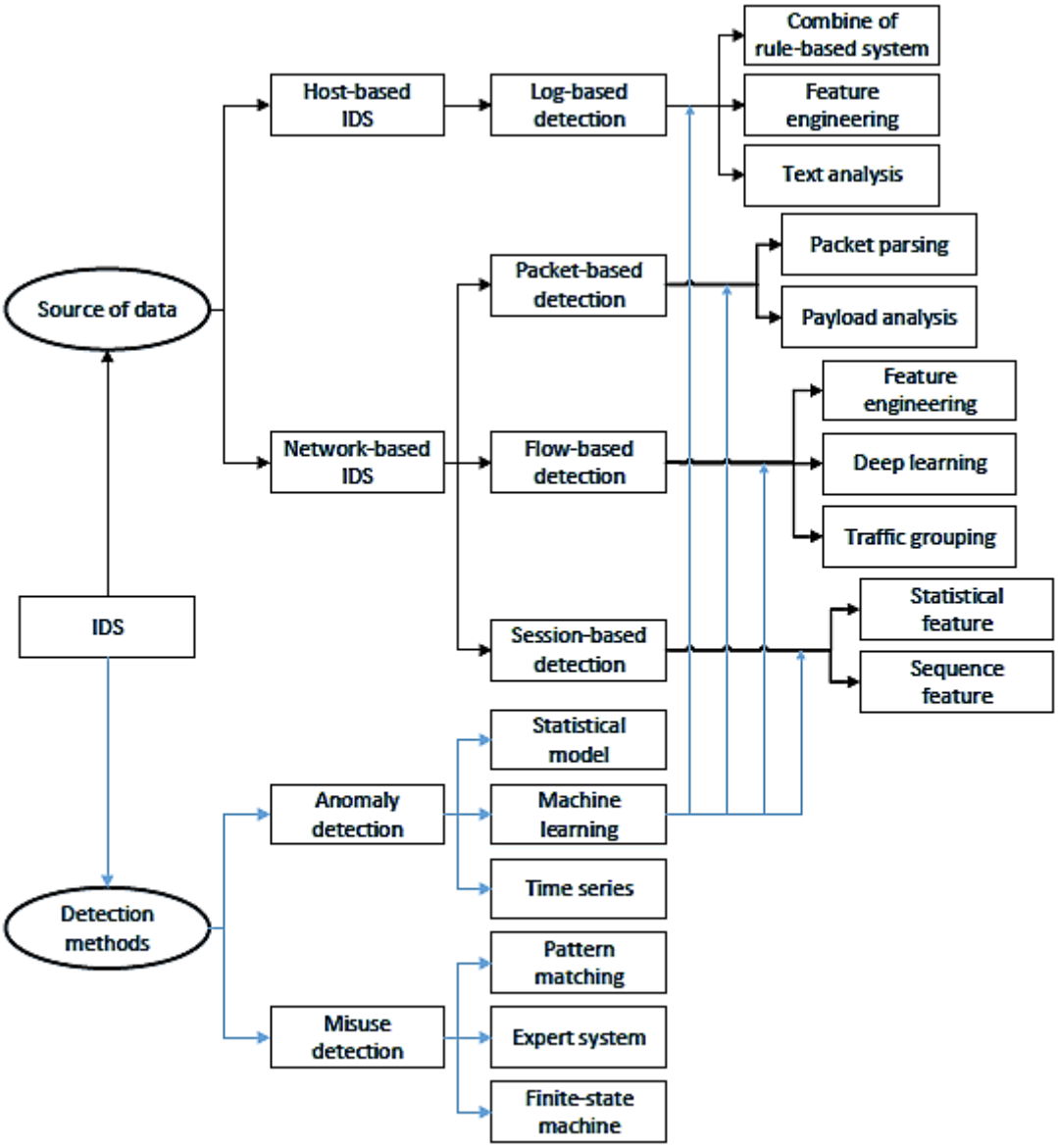

Figure 2. IDS Classification System

3.2 Classification by Detection Methods

Misuse detection is sometimes considered a signature-based detection—the underlying principle of describing attacks as signatures. The method of identification correlates with sample signatures using a signature database. The key challenge in developing frameworks for misuse identification is creating successful signatures. The benefit of abuse detection is that it has a low false alarm rate and discusses in-depth threat forms and potential reasons; the drawbacks are the high missed alert rate, the ability to track unexpected threats and the need to hold an extensive signature database.

The advantages of anomaly detection are high generalization and the ability to spot unexpected threats. However, their limitations are high false alarm rates and unable to provide any explanation for an abnormality.

International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

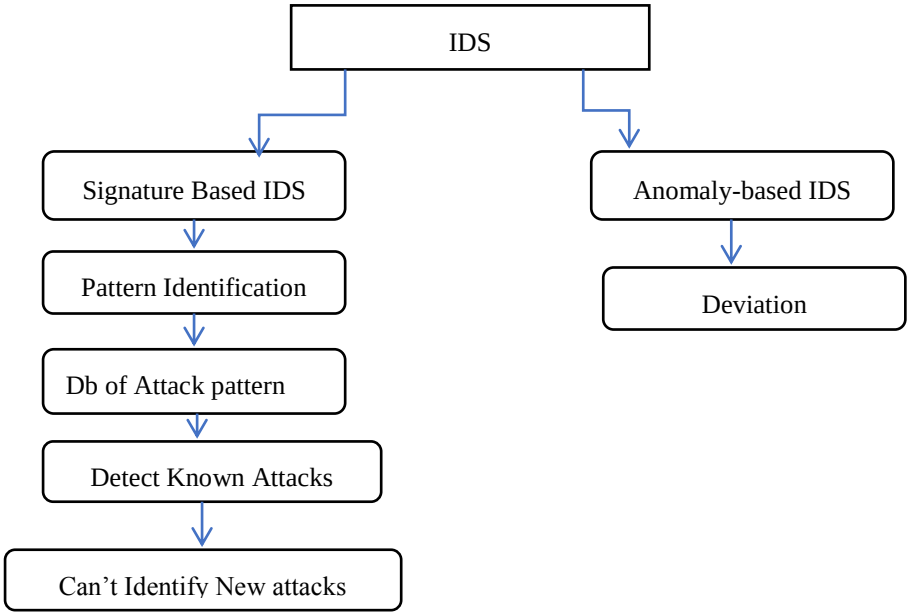

Figure 3. IDS Detection Classifications

As seen in Figure 3, misuse identification involves pattern-based, specialist framework and finite-state machine-based approaches for taxonomy-based Detection. Anomaly analysis involves approaches focused on mathematical simulation, machine learning, and time series.

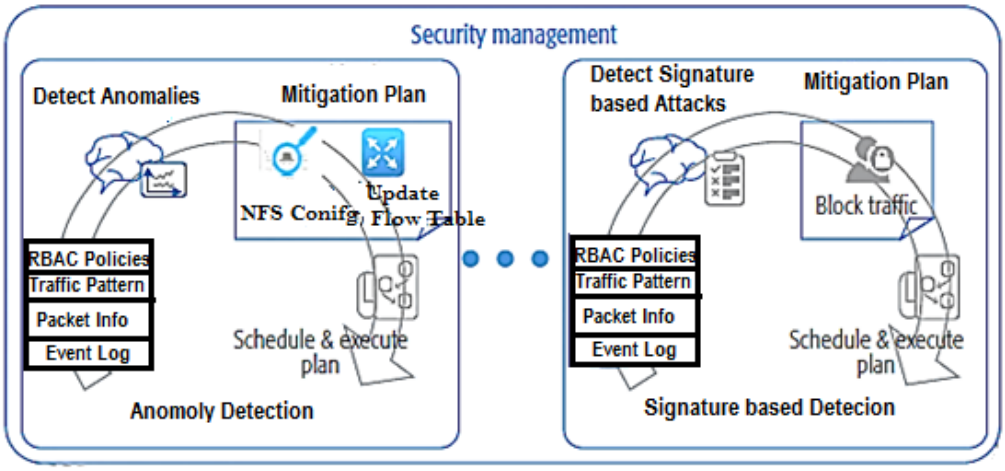

Figure4. Security management Architecture

Security Management: The most common network security measure is to look for emerging and novel threats. The network is open to zero-day attacks due to the way vulnerability management is set up. This vulnerability is absolutely necessary, as new threats appear on a daily basis. The benefits of an established safety protocol are clear, and in this regard, ML was thoroughly explored in Figure 4. Prior research has focused on the use of machine learning for the detection of misuse patterns, in order to learn various attack characteristics from historical data and establish fundamental rules for the identification of different attacks.

There was also talk about how to catch zero-day attacks using ML. Standard behaviour patterns are identified and deviations from the average are then studied.

4. COMMON MACHINE LEARNING ALGORITHMS IN IDS

4.1 Machine Learning Models

Two significant forms of machine learning exist supervised and unregulated learning. Learning supervised depends on valuable knowledge in classified results. Classification is the most common task in supervised learning (which is used most commonly in IDS); however, manual classification of data is costly and time-consuming. The absence of adequate classified data thus constitutes the key bottleneck for supervised learning. In comparison, unattended research derives useful knowledge from unlabelleddata, making training results much more comfortable to access. However, unmonitored learning performance is significantly lower than in supervised learning performance. Figure 5 displays the popular machine learning algorithms used in IDSs.

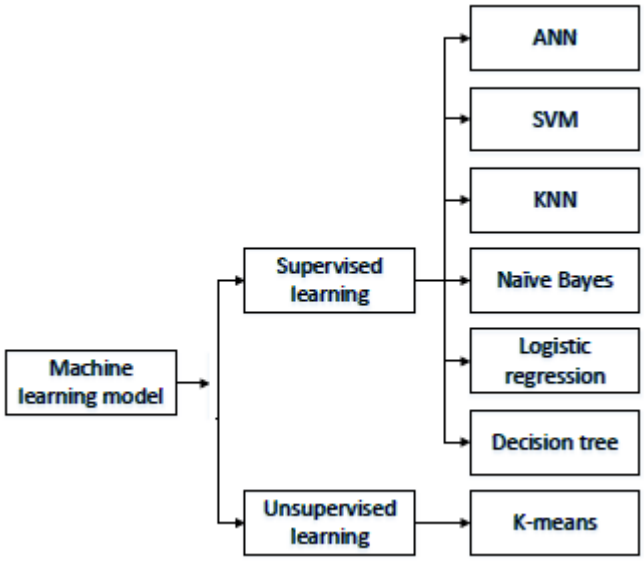

Figure 5.Classification of machine learning algorithms.

4.2. Performance Evaluation Metrics (PEM)

There are several factors involved in evaluating machine learning methods. The models are chosen based on the selection of the best metrics. When attempting to measure the effectiveness of an IDS, multiple metrics are also used simultaneously.

Accuracy is measured as the ratio of samples that are correct to all of the samples that are in the dataset. To have an accurate dataset, use an accurate measure. However, in practise, samples from normal distributions are far more common than samples that do not follow a normal distribution; precision may not be the performance criterion.

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+FP+FN+TN}}$$

Precision (P) in detecting attacks is established by the relationship between true positive samples and forecast positive samples.

$$P = \frac{TP}{TP+FP}$$

Recall (R) It is defined as the ratio of the total number of true positives to the total number of positive results, and the detection rate is referred to as. IDS models need to be able to detect attacks to be effective.

$$R = \frac{TP}{TP+FN}$$

F-measure (F) is defined as the harmonic average of the precision and the recall.

$$F = \frac{2*P*R}{P+R}$$

The false-negative rate (FNR) In relation to the total positive samples, the FNR is defined as the ratio of False Negative Samples to Total Positive Samples. A missing warning rate in threat detection is also known as the FNR.

$$FNR = \frac{FN}{TP + FN}$$

The false-positive ratio (FPR)is defined as the ratio of false-positive to positive samples expected. When it comes to attack detection, the FPR is also known as the false alarm rate. Here's how that looks:

$$FPR = \frac{FP}{TP + FP}$$

A true positive is a T.P. true prediction, an F.P. is a T.N. false prediction, and a false negative is an F.N. true prediction. An intrusion detection system (IDS) looks for attacks; thus, attacks' samples are considered positive and non-attacks' samples are considered negative. These techniques use accuracy, recall (or identification rate), and FNR (or missing alarm rate) in the attack detection process (or incorrect alarm rate).

4.3 Benchmark Datasets in IDS

In order for machine learning to succeed, the input data must be consistent. Machine learning begins with data comprehension. For IDSs, the data obtained should be straightforward to collect and present network and host information. Data sources for IDSs include packets, sessions, and logs. This data collection has a complex design and is time-consuming to make. Many researchers may use a benchmark dataset more than once if it is created. Simplicity is only one of the advantages, as it also enables the use of comparison data sets.

(1) Authoritative comparison data sets make experimental findings more compelling.

(2) Several recent studies have been carried out using standard comparison datasets that make it easy to compare current findings with previous research.

(1) DARPA1998

.This dataset [23]the DARPA1998 dataset, created by MIT Lincoln Laboratory] is a commonly used benchmark dataset in IDS studies. There are five labels to choose from: standard, denial of service (DOS), sample, User to Root (U2R), and local remote (R2L). Since standard machine learning models cannot directly include raw packets, the KDD99 dataset offers a solution to this problem.

(2) KDD99

The KDD99 [24] dataset is the most widely used intrusion detection system (IDS) benchmark. Like DARPA1998, the codes used in KDD99 are similar. Features, as explained in KDD99, are classified into four types: basic characteristics, application attributes,

machine-related information, and time-related information. Unfortunately, the KDD99 dataset has several errors. KDD data is out of date, because the network has recently changed.
(3) NSL-KDD
In order to fix the limitations of the KDD99 data collection, the NSL-KDD was developed. For NSL-KDD, the selected documents were carefully chosen based on the KDD99 project. Due to the elimination of classification bias, different class records in the NSL-KDD are matched. To ensure that the number of records is kept to a minimum, the NSL-KDD has eliminated duplicate and obsolete documents. It manages, to some extent, the issues of data fragmentation and redundancy by implementing the NSL-KDD. Though this is the case, new data is not used in the NSL-KDD, and minority samples are thus no longer up to date.

5. RESEARCH ON MACHINE LEARNING-BASED IDSS

Data-driven approaches employ machine learning, the first step of which is to understand the data. In this section, we have several ways of applying machine learning to IDS architecture based on the type of data used as the classification thread. Attack behaviour such as host and network behaviour are included in related data types. The device logs reflect the habits of the host, and the network activities reflect the activity on the network. Attacks are made up of different types, each with a distinct pattern. As a result, you should select data sources that can be used to recognise various attacks based on the threat characteristics.
Flow data is useful for the identification of a DOS attack because of this. A secret channel consists of operations that carry session data between two separate I.P. addresses, which are better suited for detection of session data.

5.1 Packet-Based Attack Detection

Network communication works with packets, which are the basic units of information exchange. Packet files contain binary files, so the first time they are scanned, they are unreadable. A packet has a header and data inside. I.P., ports, and other protocol-specific fields are all standardised fields in the headers. A required payload protocol is specified in the application layer's application data section.
Packet-based IDS data sources provide three benefits: U2L and R2L attacks can be easily detected because of the fact that packets contain contact information. I.P.s and timestamps are included in packets to help determine where an attack originates. Packs can be tracked in real-time without the need to cache them. A common misconception is that each packet represents the entire state of communication or the context of each packet. As a result, it is nearly impossible to identify DDOS attacks. The primary techniques for packet-based identification comprise packet decoding and payload processing.

5.2 Machine learning Centric Secure Cloud Management

Table 2Machine Learning focused, secure, and cloud-managed

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

		SVM

Table 2. Describes the Centric Protected Cloud Security Machine Learning for two forms of IDS classification, i.e. signatures and anomaly-based threat identification. Techniques such as N.N., D.T., B.N., SVM, N.N., DNN, K-means, (Collaborative) D.T., (Collaborative) B.N., and SVM for the identification of an abnormality are proposed.

Table 3Following is a quick summary of machine learning-based IDSs:

Authors	Data Source	Datasets	Classification Methods	Machine Learning Algorithms
Mayhew et al. [24]	Packet	Private dataset	Packet parsing	SVM and K-means
Hu et al. [25]	Packet	DARPA 2000	Packet parsing	Fuzzy C-means
Min et al. [26]	Packet	ISCX 2012	Payload analysis	CNN
Zeng et al. [27]	Packet	ISCX 2012	Payload analysis	CNN, LSTM, and auto-encoder
Yu et al. [28]	Packet	CTU-UNB	Payload analysis	Auto-encoder
Rigak et al. [29]	Packet	Private dataset	Payload analysis	GAN
Goeschel et al. [30]	Flow	KDD99	Statistic feature for flow	SVM, decision tree, and Naïve Bayes
Kuttranont et al. [41]	Flow	KDD99	Statistic feature for flow	KNN
Peng et al. [32]	Flow	KDD99	Statistic feature for flow	K-means
Teng et al. [33]	Flow	KDD99	Traffic grouping	SVM
Ma et al. [34]	Flow	KDD99 and NSL-KDD	Traffic grouping	DNN
Ahmim et al. [35]	Session	CICIDS 2017	Statistic feature for session	DT
Alseiari et al. [36]	Session	Private dataset	Statistic feature for session	K-means
Yuan et al. [37]	Session	ISCX 2012	Sequence feature for session	CNN and LSTM
Radford et al. [38]	Session	ISCX IDS	Sequence feature for session	LSTM
Wang et al. [39]	Session	DARPA 1998 and ISCX 2012	Sequence feature for session	CNN
Meng et al. [40]	Log	Private dataset	Rule-based	KNN

6. CLOUD SECURITY CHALLENGES

The complexities of cloud protection are part of ongoing research. Related open concerns as potential ranges are identified:

Security-based Data Classification: Multiple users' data may be stored in a cloud storage data centre. Classification of data is done based on the sensitivity of the data. The classification system should cover multiple issues such as how frequently a person uses the resource, how frequently a piece of information changes, and whether a person has exclusive use of the resource for their organisation. After data has been identified and tagged, the protection level associated with this tagged data feature can be added. In order to comply

with this standard, a data system must have authentication, encryption, privacy, and storage, as well as any other requirements which are dependent on the data's form.

Identity management system: It is necessary for both providers and customers of cloud services to have a secure, trust-based identity management system. This is in addition to issues reported with an unrelated identity management system. The call for a trust-based identity management scheme applies to ensuring the identification and delivery, preservation and control of life cycles.

Safe, cloud infrastructure solution: Due to security concerns, a secure cloud storage system presents a significant challenge. The cloud computing system requires a steady and dependable approach to be achieved.

Technology Optimization Uses: Security and virtualization concerns as well as cloud resource optimization must also be discussed and addressed.

7. CONCLUSION

We look at emerging cloud protection issues and new security strategies in this paper. Firewalls, malicious insiders, faulty plugins, multi-tenancy applications, side channels, insecure browsers, and usability are some of the primary challenges to cloud-based security. After we've organised the various security concerns into five separate categories, including security requirements, network, connectivity, cloud infrastructure, and data, we proceed to organise these further into ten distinct elements.

It is necessary to guarantee the integrity of the data and cloud resources in all cloud components to support strong cloud protection. As more analysis is being done to address security issues in the cloud, it's generating more data to be examined. On the other hand, in order to have a stable cloud infrastructure, there are numerous opportunities that remain open. One of the key considerations for starting cloud computing is cloud networking, networking, anonymity, and application and web resources.

Machine learning models have been a tremendous help in research and have played an integral role in the field. We are investigating the IDS taxonomy, which incorporates data sources as a central concept to demonstrate various machine learning algorithms. Based on these taxonomies, we further expanded our intrusion detection system, monitoring different data streams such as logs, packets, flow, and sessions. An IDS must select the correct type of data according to the type of threat it detects.

8. REFERENCES

[1] https://www.prnewswire.com/news-releases/the-global-cloud-security-market-to-reach-usd-1264-billion-by-2024-300558185.html (Accessed on 10thApril 2020)

[2] Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Compute Electr Eng 71:28–42

[3] Mell P, Grance T (2018) SP 800-145, The NIST Definition of cloud computing | CSRC (online) Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-145/fnal. Accessed 11 Dec 2018

[4] Xu X (2012) From cloud computing to cloud manufacturing. Robot Comput Integr Manuf 28(1):75–86.

[5] Bhamare D, Samaka M, Erbad A, Jain R, Gupta L, Chan HA (2017) Optimal virtual network function placement in multi-cloud service function chaining architecture. Comput Commun 102:1–16

[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] 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.
[8] Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.;Wang, C.(2018) Machine learning and deep learning methods for cybersecurity. IEEE Access, 6, 35365–35381.
[9] Agrawal, S.; Agrawal, J.(2015)Survey on anomaly detection using data mining techniques. Procedia Comput. Sci., 60, 708–713.
[10] Sengupta, S.; Kaulgud, V.; Sharma, V.S.(2011) Cloud computing securityTrends and research directions. In Proceedings of the IEEE World Congress on Services (SERVICES), Washington, DC, USA, 4–9; pp. 524–531.
[11] Braun, V.; Clarke, V. (2006) Using thematic analysis in psychology. *Qual. Res. Psychol.* , 77–101.
[12] A Survey on Cloud Computing Security, Challenges and threats|Whitepapers|TechRepublic. Available online: http://www.techrepublic.com/whitepapers/a-survey-on-cloud- computingsecurity-challenges-and-threats/3483757 (accessed on 18 April 2020).
[13] Thalmann, S.; Bachlechner, D.; Demetz, L.; Maier, R.(2012)"Challenges in cross-organizational security management". In Proceedings of the 45th Hawaii International Conference on System Science (HICSS), Maui, HI, USA, 4–7; pp. 5480–5489.
[14] Wang, J.-J.; Mu, S.(2011) Security issues and countermeasures in cloud computing. In Proceedings of the IEEE International Conference on Grey Systems and Intelligent Services (GSIS), Nanjing, China, 15–18 ; pp. 843–846.
[15] Lv, H.; Hu, Y.(2011)"Analysis and research about cloud computing security protect policy". In Proceedings of the International Conference on Intelligence Science and Information Engineering (ISIE), Wuhan, China, 20–21; pp. 214–216.
[16] Jain, P.; Rane, D.; Patidar, S.(2011) A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment. In Proceedings of theWorld Congress on Information and Communication Technologies (WICT), Mumbai, India, 11– 14; pp. 456–461.
[17] Behl, A.(2011) Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In Proceedings of the 2011 World Congress on Information andCommunication Technologies (WICT), Mumbai, India, 11–14; pp. 217–222.
[18] Mathisen, E.(2011) Security challenges and solutions in cloud computing. In Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference (DEST), Daejeon, Korea; pp. 208–212.
[19] Mahmood, Z. (2011) Data location and security issues in cloud computing. In Proceedings of the International Conference on Emerging Intelligent Data and Web Technologies (EIDWT), Tirana,Albania, 7–9; pp. 49–54.
[20] Denning, D.E(1987) An intrusion-detection model. IEEE Trans. Softw. Eng. 222–232.
[21] Heberlein, L.T.; Dias, G.V.; Levitt, K.N.; Mukherjee, B.; Wood, J.; Wolber, D.(1990) A network security monitor. In Proceedings of the IEEE Computer Society

Symposium on Research in Security and Privacy, Oakland, CA, USA, 7–9; pp. 296–304.
[22] Kuang, F.; Zhang, S.; Jin, Z.; Xu,W.(2015) A novel SVM by combining kernel principal component analysis and improved chaotic particle swarm optimization for intrusion detection. Soft Comput., 19, 1187–1199.
[23] KDD99 Dataset. 1999. Available online:
[24] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed on 16 March 2020).
[25] NSL-KDD99 Dataset. 2009. Available online: https://www.unb.ca/cic/datasets/nsl.html (accessed on 16 March 2020).
[26] Hu, L.; Li, T.; Xie, N.; Hu, J. (2015) False positive elimination in intrusion detection based on clustering. In Proceedings of the 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, China; pp. 519–523.
[27] Min, E.; Long, J.; Liu, Q.; Cui, J.; Chen, W.(2018), TR-IDS: Anomaly-based intrusion detection through text-convolutional neural network and random forest. Secur. Commun. Netw, 4943509.
[28] Zeng, Y.; Gu, H.; Wei, W.; Guo, Y. Deep (2019) Full Range: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework. IEEE Access, 7, 45182–45190.
[29] Yu, Y.; Long, J.; Cai, Z.(2017) Network intrusion detection through stacking dilated convolutional autoencoders. Secur. Commun. Netw. **2017**, 2017, 4184196.
[30] Rigaki, M.; Garcia, S.(2018) Bringing a gan to a knife-fight: Adapting malware communication to avoid Detection. In Proceedings of the 2018 IEEE Security and PrivacyWorkshops (SPW), San Francisco, CA, USA, pp. 70–75.
[31] Goeschel, K.(2016) Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive Bayes for off-line analysis. In Proceedings of the SoutheastCon 2016, Norfolk, VA, USA,; pp. 1–6.
[32] Kuttranont, P.; Boonprakob, K.; Phaudphut, C.; Permpol, S.; Aimtongkhamand, P.; KoKaew, U.;Waikham, B.; So-In, C.(2017) Parallel KNN and Neighborhood Classification Implementations on GPU for Network Intrusion Detection. J. Telecommun. Electron. Comput. Eng. (JTEC), 9, 29–33.
[33] Peng, K.; Leung, V.C.; Huang, Q(2018). Clustering approach based on mini batch kmeans for intrusion detection system over big data. IEEE Access **2018**, 6, 11897–11906.
[34] Teng, S.; Wu, N.; Zhu, H.; Teng, L.; Zhang, W.(2017) SVM-DT-based adaptive and collaborative intrusion detection. IEEE/CAA J. Autom. Sin., 5, 108–118.
[35] Ma, T.; Wang, F.; Cheng, J.; Yu, Y.; Chen, X(2016) A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks. Sensors **2016**, 16, 1701.
[36] Ahmim, A.; Maglaras, L.; Ferrag, M.A.; Derdour, M.; Janicke, H.(2019) A novel hierarchical intrusion detection system based on decision tree and rules-based models. In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, pp. 228–233.
[37] Alseiari, F.A.A.; Aung, Z. (2015) Real-time anomaly-based distributed intrusion detection systems for advanced Metering Infrastructure utilizing stream data mining. In Proceedings of the 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), Offenburg, Germany,pp. 148–153.

[38] Yuan, X.; Li, C.; Li, X.(2017) DeepDefense: identifying DDoS attack via deep learning. In Proceedings of the 2017 IEEE International Conference on Smart Computing (SMARTCOMP), Hong Kong, China; pp. 1–8.
[39] Radford, B.J.; Apolonio, L.M.; Trias, A.J.; Simpson, J.A.(2018) Network traffic anomaly detection using recurrent neural networks. arXiv:1803.10769.
[40] Wang, W.; Sheng, Y.; Wang, J.; Zeng, X.; Ye, X.; Huang, Y.; Zhu, M.(2017) HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. IEEE Access , 6, 1792–1806.
[41] Meng, W.; Li, W.; Kwok, L.F(2015) .Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection. Secur. Commun. Netw. 8, 3883–3895.
[42] McElwee, S.; Heaton, J.; Fraley, J.; Cannady, J.(2017) Deep learning for prioritizing and responding to intrusion detection alerts. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, pp. 1–5.
[43] Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA (2012) Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Computers& security 31(3):357–374
[44] Sharafaldin, A. H. Lashkari, and A. A. Ghorbani,(2018) Toward generating a new intrusion detection dataset and intrusion traffic characterization," in ICISSP, pp. 108–116