A REVIEW OF CLOUD COMPUTING SECURITY : THREATS ATTACKS AND ALGORITHMS

Umma Khatuna Jannat, M. Mohnakumar*

Abstract

Cloud technology is fast expanding that allows customers to access dependable and scalable on-demand services while incurring lower infrastructure costs. Even though the cloud providers have a heap of benefits, also a heap of disadvantages, such as security threats. The major disadvantage in cloud computing security is Threatsattacks, which are the consequence of the aforementioned shortcomings. Cloud Malware Injection Attacks, Cloud Domain Hijacking, Cloud Data Confidentiality, Cloud Integrity of Data, Cloud Data Availability, Unknown Risk Profile, Man- in- the-Cloud Attacks, CAPTCHA Breaking and Hacking Attacks on Google are only little examples of security Threatsattacks. Support Vector Machine (SVM), Naive Bayes, Decision Tree, Logistic Regression, and Ensemble approaches can be used to detect this Threatsattack in the cloud and these are the machine learning algorithms. We have primarily concentrated on various security threats, cloud-based attacks, and the methods used to identify these Threatsattacks in this work.

Keywords: cybersecurity, threats, attacks, algorithm, security in the cloud.

I INTRODUCTION

In the cloud computing industry, the cloud is a burgeoning technology [1]. It alludes to the use of a computer with an internet connection to access information technology and software applications. The cloud is made up of three components: Software as a Service (SAAS), Platform as a Service (PAAS), and Infrastructure as a Service (IAAS). The three types of cloud computing include each aforementioned service. The services are hosted in a data center to the cloud specialist organizations so that the enterprise or individual customers can access them via a network connection. Companies that offer various cloud services are known as cloud specialist organizations. IBM, AWS, Cisco, Apple, SAP, Google, Microsoft, and Oracle are some of the top cloud specialist organizations. However, rather than hosting applications aimed at others, SalesForce and Apple are more concerned with developing applications. Corporations such as IBM, Google, SAP, and Microsoft provide altogether three cloud services, whilst the rest of the firms only supply two or one. Organizations should have an actual Threatsattacks detection system in place to fend off harmful insiders. This system should be able to identify and remediate before they become dangerous insiders spread Threatsattacks. Unfortunately, the field of Threatsattacks is not well-understood. Furthermore, the detecting techniques or procedures that can be used, just as the limitations of current solutions, have still to be investigated. Thus, a thorough examination of previous threats discovery methods is required [2]. The present situation is mostly owing to a misunderstanding of the valid situation threat and the potential harm it can cause to organisations. Security breaches are a single of the drawbacks of cloud security. This difficulty arises from cloud data storage across multiple geographical locations. We discussed numerous kinds of cloud-based Threats attacks such as Cloud Domain Hijacking, Cloud Malware Injection Attacks, Abuse and Nefarious Use of Cloud Services, Cloud Data Loss, Cloud Shared Technology or Shared Dangers, Cloud Data Confidentiality, Cloud Data Integrity, Cloud Data Availability, Unknown Risk Profile, Man-in-the-Cloud

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

Attacks, Cloud Account Hijacking, CAPTCHA Breaking, and Hacking Attacks on Google. We additionally examine various machine learning algorithms for detecting security Threats attacks, such as Naive Bayes, K-means Clustering, SVM, Decision Tree, Fuzzy Logic, K-Nearest Neighbors (KNN) algorithm, TF-IDF algorithm, One-Class Support Vector Machine (OCSVM), and Markov Model and Hidden Markov algorithm.

II RELATED WORK

A. CLOUD COMPUTING DEPLOYMENT MODELS

The following are some of the three main deployment computational models in the cloud architecture:

- **Private Cloud**

This infrastructure is on a private network and is managed by the company, either in its internal enterprise data center or through the cloud provider. It could take place on-site or off-site. It is more dependable since only the organisation that owns it has access to monitor and regulate service delivery parameters. It aims to address data security issues and provide users more control, but it doesn't provide benefits like cheaper capital and operating costs.

- **Public Cloud**

A cloud provider owns and manages this infrastructure. It is intended for a wide range of audiences, including both groups and the general public. On a pay-per-use basis, the resources are dynamically provided on-demand. It is unsecure because it is vulnerable to malicious Threatsattacks. Scalability, geographical independence, adaptability, and the lack of initial infrastructure investment are just a few of the benefits it provides to its customers.

- **Hybrid Cloud**

This infrastructure consists of a network of clouds connected by standardised technologies to share data and applications regardless of who owns them or where they are located. By combining the assistance of each while simultaneously resolving the limitations, it enables greater flexibility and control over the application.

- **Community Cloud**

This cloud architecture was created to be used by various enterprises within a single community with shared interests. Everyone has free access to applications and data on the community cloud. Several cloud deployment models are being created in response to the diverse needs of different users. Such a paradigm is exemplified by a virtual private cloud. It's a method of connecting resources across a virtual private network while using public cloud infrastructure in a private manner (VPN).

B. SERVICE DELIVERY MODELS IN CLOUD COMPUTING

The SAAS, PAAS, and IAAS service framework encompasses altogether services offered by the cloud. These are well-defined as follows:

- **Software-as-a-Service (SaaS)**

The top layer of the SPI service framework is SaaS, which allows service providers to remotely deploy apps on customers devices and access them via interfaces without having to handle the underlying infrastructure. SaaS applications must safeguard data in a variety of ways, including WS (Web Service) security, XML encryption, Secure Sockets Layer (SSL), and other methods for data protection. Microsoft Online, Google Docs, Rackspace, Salesforce and Facebook and other services are examples.

- **Platform as a Service (PaaS)**

The SPI service platform's PaaS layer allows customers to create and deploy the apps despite having no control over the underlying infrastructure or computing resources. PaaS providers provide a pre-configured collection of server applications, such as PHP, Apache, Linux, MySQL, as well as limited J2EE, Ruby, and other technologies. Just a few examples include Google App Engine, Microsoft Windows Azure, Amazon S3, force.com, and Rackspace.

Infrastructure as a Service (IaaS)

IaaS refers to the SPI service framework's bottom layer, where cloud providers deliver on-demand services like storage, networks, computing power, and other computational resources. Consumers can install and run any software or operating system they wish, only paying for what they use rather than the infrastructure. IaaS is supported by virtualization technology, which consists of a virtualization layer and a virtualized resource layer (virtual computers, virtual storage, and virtual networks). Just a few examples include Google Cloud Storage, Microsoft Azure, Amazon EC2, GoGrid, and Rackspace.

- **The Hardware Layer**

The cloud physical resources, which are frequently placed in data centers, are controlled by this layer, which sits beneath the stack. Hardware configuration, fault tolerance, traffic management, as well as power and cooling resource management, are all potential challenges .

Cloud computing now faces security and privacy issues. Cloud technology is a significant field since it conveys and hosts its services through the internet. It delivers facilities that are tailored to the necessities of its customers and charges correspondingly [3]. Now a day’s cloud computing technology is more significant as consumers become more reliant on it and organisations can now easily use cloud services.

Gaps in cloud computing are defined as trust difficulties between consumers and cloud providers when customers fear policies that are hidden from them [4]. Cloud providers are concerned that consumers may gain an advantage use their cloud services to carry out Threatsattacks. The expectations of the businesses for the services it is receiving from a certain provider are among the most significant aspects to consider when choosing a cloud service provider. Vulnerabilities are security holes in the cloud that an attacker could take advantage of to obtain access to the network and other infrastructure resources [3]. A cloud threat is a potentially damaging event that might be intentional or inadvertent [3] [4]. The exploitation of vulnerabilities may influence cloud computing accessibility and financial benefits [3][4]. An attack entails a cloud resource depletion activity, and vulnerability exploitation may affect cloud technical and financial benefits accessibility.

Cloud computing security is a major concern that can result in serious Threatsattacks [5][6]. These have ramifications, such as permitting network attacks, providing intruders access control, allowing illegal service access, and exposing sensitive data. All of these put the cloud at threat, either directly or indirectly, such as in the workplace. Securing the cloud from these risks and prevents any damage; the attacks it can be carried out must be discovered and understood.

We looked at related papers that used algorithms to look at cloud security vulnerabilities. A method for resolving problems and increasing the performance of cloud systems [7]. Information indifference continues to be a result of information instability by the outsider who restores, maintains, and forms the information. Artificial Neural Networks (ANNs) are used to sort through the jumbled data and examined cloud security challenges and models here it looked into the unique security challenges that have arisen as a result of the organizations move to distributed computing [8]. However, the critical advancement of the cloud without the involvement of anyone else has the potential for considerable security. Malware security threats are solved using algorithms [9]. The researchers presented a barrier architecture that employs three algorithms, which were chosen based on high-accuracy malware detection. In a mobile cloud environment, the author presented a comprehensive analysis of interruption recognition systems that employ a computational insight technique [10].

The following are the most commonly mentioned Threatsattacks in cloud computing: Fig: 1

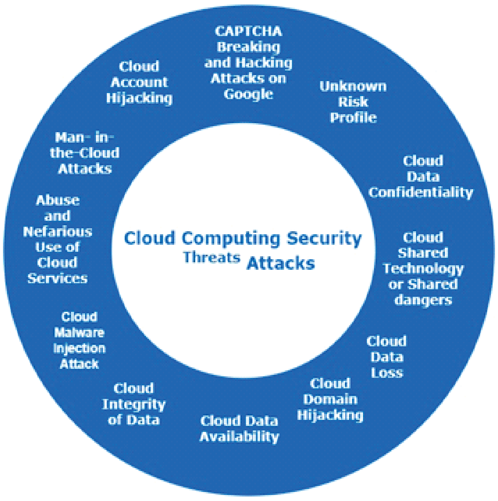
CAPTCHA Breaking and Hacking Attacks on Google
Cloud Account Hijacking
Unknown Risk Profile
Man- in-the-Cloud Attacks
Cloud Data Confidentiality
Abuse and Nefarious Use of Cloud Services
Cloud Computing Security
Threats Attacks
Cloud Shared Technology or Shared dangers
Cloud Malware Injection Attack
Cloud Data Loss
Cloud Integrity of Data
Cloud Domain Hijacking
Cloud Data Availability

Fig: 1 Cloud Computing Security Threatsattacks

III METHODOLOGY

Kitchenham and Charters methodology [11] was utilised to conduct a Systematic Literature Review (SLR) in this study. The procedure is divided into several segments using their approaches, each of which contains multiple stages.

The sections that follow and show how this paper followed the review methodology.

A. Research Questions

From 2016 to 2021, this SLR intends to outline and clarify the cloud computing concepts its Threatsattacks and algorithm in cloud security. The following two research questions (RQ1, RQ2) are posed.

RQ1: What are the recent Threats attacks?

- To get an outline of the recent Threats attacks designed and incorporated.

RQ2: In cloud computing, what algorithms are used?

- To develop an outline of the cloud security algorithm

These RQs analyze the common features among the studies.

B. Strategy for the Search

The following topics are discussed in this portion of the paper: The research questions major search phrases are discovered. To replace main terms, new terminology has been defined. Boolean logic is used in the form of search operators to make search results more relevant. (OR, AND). We utilised search phrases like "cloud security" AND "(Cloud Threats" OR "Attacks")" to find results relevant to the cloud security algorithm.

C. Resources for Conducting Surveys

The following digital libraries are utilised in this research: in the search for the required research papers:

- IEEE Xplore
- Scopus
- Google Scholar
- ACM Digital Library
- Springer Online

D. Study Selection

Based on the precise search requirements, we initially obtained 190 search studies. Based on inclusion/exclusion criteria, 53 publications were used in this literature study. As shown in Table 1, performed additional strain to ensure that is simply relevant materials were included in this literature review.

Inclusion criteria	Exclusion criteria
Cloud attacks and threats	Cloud-based security papers in a way that is not related to cloud security issues
Using cloud security area algorithms	Papers on cloud security that do not use algorithms
Only journal and conference articles should be included.	Publications that have not been peer-reviewed

Table I Shows the Criteria for Inclusion and Exclusion.

E. Quality Assessment Rules (QARs)

The use of quality evaluation guidelines was the last step in determining the final selection of publications that will be included in this research. To assess the publications quality and relevance to our research, we devised five QARs, each of which is rated out of five. The following values are assigned to each QAR score: "completely answered" = 4.5, "above average" = 3.5, "average" = 3, "below average" = 1 and "not answered" = 0. A score of less than 3 indicates that the document was not included in this review.

The following QARs were employed in this study:

1. Are the study's aims described clearly in the article?
2. Does the paper have a good structure?
3. Is there enough background information in the article?
4. Is there a well-defined domain of cloud security?
5. Are cloud computing algorithms sufficiently explained?
6. Are the experiment's findings and conclusions presented in a clear and straight forward manner?

As a result, we received 53 papers with a quality score.

F. Strategy for Data Extraction

The purpose of this step is to respond to each article's research questions in a semi-structured manner. Every article has the following information: title, publication year, paper number , domain, publishing type, RQ1 and RQ2. It's worth noting that not all of the articles addressed all of the research questions.

IV CLOUD SECURITY THREATS ATTACKS

While there are numerous Threats attacks in the cloud environment, we have divided well-known current Threats attacks into the following categories.

RQ1.What are the Recent Threats attacks

A. Abuse and Nefarious Use of Cloud Services

Many businesses offer free trial use of cloud resources. Researchers discovered that malevolent users utilise such anonymous and routine registration processes to access cloud computing resources and carry out undesirable operations. By carrying out their harmful actions in the shadow of a cloud computing environment , cybercriminals get more immunity. Currently, PaaS is a good number of affected service layers [12], but this will eventually spread to the IaaS platform. DDoS, Password cracking, botnet monitoring, and malicious data hosting are several of the elementary attacks that are thrown using clouds to carry available such abuses [13][14]. Malicious actors have used IaaS infrastructures to host botnets, trojan horses, and malware. As a result of these operations, the block of IaaS network addresses has been banned.

B. Cloud Malware injection Attack

Its goal is to infect a cloud service provider's system with a harmful program or service or virtual machine [14][15]. It could be used for any purpose the attacker desires, ranging from complete functionality modifications to obstructing to eavesdropping and data alteration . Running a service instance integrity check for incoming requests is a feasible countermeasure technique for dealing with this problem. For example, compare the hash value of the original service instance image file to the hash values of all new service instance images.

C. Cloud Domain Hijacking

Cloud domain hijacking, sometimes known as domain spoofing, is an attack. In a situation in which a third party steals a company's web address without the true owner's permission, the other party changes the formalisation of another domain name [16]. The true owner is denied administrative access as a result of this. The authentic web address is used by scammers for any purpose they want.

A cloud domain can be lost to someone else under seemingly innocuous circumstances, such as when a cloud domain expires and someone else registers it right afterward.

When the legitimate owner of a domain unwittingly loses it, it is thought to be a true cloud domain hijacking. As a consequence of a phishing or other social engineering scam, people offer their cloud domain system credentials. This hijacking can also occur when a partnership between a group of two or more persons who have access to the cloud doming registration collapses and one party rushes to change access credentials, locking out the other.

D. Cloud Data Confidentiality

When information is shared between different clients, devices, and applications, confidentiality and distinctions are made. Various phases of risk diversification are introduced here through mass management and execution of various functions (Asset Allocation: CPU-Central Processing Unit) [17][18]. Because standard security systems and data planning are crucial to the unlawful use of information, partitioning of cloud-based information is detected through customer authentication [12].

E. Cloud Integrity of Data

By just enabling something, data courtesy assures that data gets erased and repaired. Because the number of objects and cloud objects is growing, authorization is becoming increasingly critical for authorized objects to transmit information [17] [18]. When cloud-based assets can be differentiated effectively amongst customers, various security challenges occur [12] to protect the data. A security breach can also be caused by a lack of encryption or a broken key management system.

F. Cloud Data Availability

Licensed circles can access cloud management on demand, regardless of whether other things are allowed to work incorrectly or if there is a security breach. To assess SaaS vendor access, they must examine the validation process and address board shortage issues [19][20]. In cloud administration, various factors should be considered [17] [12], such as information and data management limits, transmission capacity, and speed of access to the system.

G. Leakage and Data Loss

Data loss in the cloud can occur in a variety of ways. Delete records, unlink records, remove encoding keys, and so on are only a few examples. All of these factors could result in data loss [21][22]. If data loss occurs among priority cloud users who are using the facility for data storage, the situation worsens. Furthermore, data leakage safety must be developed to ensure that sensitive and confidential information does not fall into the wrong hands. The problem is substantial due to the volume of information access activities and the type of data information stored on clouds. To reduce the risk caused by such a threat, strict access controls must be set, with data flow encrypted and integrity validated. In addition, data must be stored safely, and data integrity must be monitored regularly. This issue is typically considered a danger across all cloud service layers.

Malicious insiders, Service Interruption through hijacking, and unknown risk profiles are some of the additional dangers found in previous studies on the cloud by academics and industry [12]. The threats that result in recognised cloud attacks, on the other hand, originate from one of the four dangers described in: A taxonomy of attacks has been produced based on research of the cloud threat scenario, which identifies many well-known attacks and remedies, as well as analysis of the risks associated with cloud computing based on the cloud service layer and the placement of security threats [20].

H. Cloud Account Hijacking

Cloud account hijacking is nothing new [20][22]. Phishing, fraud, and exploiting software flaws are still effective attack strategies. Because credentials and passwords are frequently reused, the impact of such attacks is amplified. Account and service hijacking, which is frequently done with stolen credentials, is still a major threat [13]. Attackers can typically become access to vital sections of deployed cloud computing systems using stolen credentials [12]. Putting those service's confidentiality, integrity, and availability at risk. Organizations must conscious of these strategies, should be aware of a common defense-in-depth security approach, to limit the damage caused by a breach.

I. Cloud Shared Technology or Shared dangers

Attacks targeting the shared technology prevalent in cloud computing settings have surfaced in recent years [12][20]. Strong compartmentalization was never intended for disc partitions, CPU caches, GPUs, or other shared elements. As a result, attackers are concentrating their efforts on disrupting the operations of other cloud clients and gaining illegal access to data [23].

J. Unknown Risk Profile

This risk can occur in tandem with large benefits such as time savings from owning and managing infrastructure. Users, on the other hand, are unlikely to perform patching, auditing, or other security-related tasks, resulting in an unknown risk profile that could expose important vulnerabilities [20] . A single cornerstone of cloud technology is that it permits firms to concentrate on their core business capabilities by reducing hardware and software ownership and maintenance. This has clear financial and operational advantages that must be carefully assessed against competing security risks - a task made more difficult by the fact that cloud installations are frequently motivated by anticipated benefits, with organisations neglecting security implications. Software versions, code updates, security procedures, vulnerability profiles, intrusion attempts, and security design are all significant aspects to consider when assessing a company's security posture.

Benefits and functionality in a cloud service may be widely touted but what about the complexities of internal security protocols compliance, configuration hardening, patching, auditing, and logging? Who has access to data and related logs and how are they stored? In the middle of a security breach, what information, if any, will the vendor reveal? Such queries are frequently misunderstood or ignored, leaving clients with an unknown risk profile that could involve major threats [21].

K. Man- in- the-Cloud Attacks

Any attacker can access the data exchange between two parties if the Secure Socket Layer (SSL) is not correctly set up. An attacker can gain access to data communication between data centers in the cloud [21]. To limit the possibility of a man-in-the-cloud attack, data encryption and correct SSL settings connection checks between authorised gatherings can be helpful.

L. CAPTCHA breaking and Hacking Attacks on Google

CAPTCHA stands for "completely automated public Turing test to identify computers from humans," and it's used to figure out whether a user is a malicious programme or a real person [24]. It's one of the most prevalent security strategies for detecting malicious software like Trojans, Worms, and Botnets. The attacker can crack CAPTCHAs with an audio system, speech-to-text conversion software, and image and video-based techniques. Letter overlap can be used to avoid vertical segmentation attacks. When it comes to related characters, the OCR has a hard difficulty identifying words. Because it can utilise a multitude of fonts and alphabets, it's difficult to decipher. If the string length is long, it will be more difficult to decipher CAPTCHA. Dots, colors, circles, lines, and rectangles, among other things, may make it more difficult to decipher the perturbative background [22]. Google Dorking is a term for hacking on Google. It's a hacking system that uses the Google search engine to find security holes in a system's configuration. Hackers can use searches to find security holes and learn more about the target they want to attack .

V ALGORITHM

The algorithm enables software applications to predict outcomes accurately without having to be explicitly designed. There are two types of algorithms: classification algorithms and clustering algorithms. The Decision Tree, Naive Bayes, Logistic Regression, Support Vector Machine (SVM), and Ensemble Approaches are some of the classification algorithms. We will describe some of the algorithms in this article. It can use in cloud computing security.

RQ2: Which Algorithms are used in Cloud Computing?

A. One Class Support Vector Machine

The problem of rare classes can be addressed with OCSVM by creating a model that only analyses non-threat or normal data. It focuses on the semantic content of each action, whereas the KNN technique concentrates on the action type. As a result, OCSVM was chosen since the data are uneven and it is uncertain if the action is normal or malicious [24].

Only static data streams with bounded lengths are suitable for the OCSVM technique. Insider threat data, on the contrary, is frequently ongoing, and the pattern of threats changes over time. To put it another way, data is made up of unbounded length streams.

B. TF-IDF

In documents, the TF-IDF offers or recognises sensitive or crucial words. TF-IDF examines significance in the user's log file of intercepted system calls [25].

Since TF-IDF adds the similarity of documents in a place with a word count, it may be sluggish for big vocabularies. It is assumed that various word counts give evidence that is independent of resemblance. Semantically similar words are ignored by TF-IDF.

C. Hidden Markov Model (HMM)

The Markov model adequately describes the state's subsequent changes. As a result of its ability to recognise temporal patterns, HMM models have been widely used in a variety of fields, including bioinformatics and computational linguistics. HMM is well-suited to capturing sequential behavior and has been successful in pattern reorganization. It includes algorithms for learning parameters from a sequence set that has been observed, as well as a probability estimate for seeing a particular sequence [26].

With the growth in several states, HMM computational cost rises.

D. K-Nearest Neighbors

In comparison to the KNN classifier has a faster training time than other classifiers, such as neural networks. and classification phase with a smaller computational overhead. This makes it desirable for platforms with low resources, such as the intrusion detection system node [27].

Because information can be disguised in routine behaviors through manipulation. In the several elements of detecting insider threats, the KNN approach is ineffective. Using the KNN approach necessitates a thorough understanding of how many clusters exist in the data, as well as several trials to determine the ideal cluster K number. Because of the random algorithm initialization, clustering may differ between runs.

E. Principal Component Analysis (PCA)

PCA is a technique for reducing dimensionality and cluster characteristics that are comparable. It's a popular way to deal with data having a lot of dimensions. This approach is a powerful tool for finding outliers [28, 29]. It can be as simple as breaking down a large set of features into a series of odd assessment scores [30].

One of PCA drawbacks is, it is usually seen as a black-box method, making the relationship between the generated PCA space and the original feature space difficult to comprehend. For model building, training, and change, PCA, like other mathematically based detection models such as Bayesian networks, requires extensive experience and in-depth understanding. This information is neither inexpensive nor readily available.

F. Gaussian Mixture Model (GMM)

The model can explain why certain observations are categorised as anomalous using the GMM technique. Furthermore, the model parameters and anticipated outcomes give analysts a clear picture of how the technique makes decisions. GMM can be used to model a dataset with a complex probability distribution [19].

It takes a long time to compute. The maximum value for the area has been reached. One of GMM major flaws is its statistical inefficiency when modelling data on or near a nonlinear manifold in the data space.

G. Bayesian Algorithms

Decent for calculating event that is mutually exclusive probabilities in a sample set with any other occurrence [30]. In modeling insider threat detection systems, BN is capable of abstracting from specific properties that meet desired parameters and predict their effectiveness in organisations for simplicity, privacy, and portability [31].

For the construction, training, and refining of most detection models based on mathematical approaches, such as PCA, and Bayesian Networks, substantial experience, and in-depth understanding are required. This knowledge is neither cost-effective nor readily available. Experts may disagree about a certain event or the way of causality between two events. For example, some experts may consider behavior to be normal, while others may believe the reverse.

H. Support Vector Machine (SVM)

The main key feature of SVM that makes them appealing for cybersecurity is their low classification latencies, which are measured in microseconds on present systems. Classifier training helps to get better classification performance [32]. Another enticing characteristic is that SVM are based on a convex optimization formulation with single minima. The classification borders and support vectors are also represented geometrically by SVM. SVM with less training data can yield a better classification result.

In the face of the fact that k-means and SVM classifiers provide an optimum mix of excellence and efficacy. It is tough to operate and is not user-friendly to understand by a human [32]. Parameterization can be difficult in some instances. When compared to other methods, SVM training might be time demanding. SVM necessitates a great deal of communication.

I. Decision Tree (DT)

Human operators can easily and intuitively read a DT [16]. It is simple to communicate with and maintain. There are only a few simple, easy-to-understand parameters that must be used. Can make quick forecasts.

DT uses a significant quantity of memory. DT is prone to overfitting by nature. It creates high-variance models, which should be avoided by pruning the branches. DT is unable to progress in little steps.

VI CONCLUSION

This research suggests that there are two sides to this coin. The cloud industry is rapidly expanding, garnering increasing amounts of local and foreign investment. Simultaneously, it is being implemented in practically every industry. All of this has a significant impact on the worldwide market and is shaping the future development of technologies. Because of its vast development and investment possibilities, as well as the vast amount of data it contains. In terms of information security, privacy, and Threats attacks issues, it is one of the most vulnerable sectors of technology.

On the contrary, when clients and service providers use or deliver cloud services, there are numerous obstacles to overcome. Some problems have recently arisen, which we are attempting to explain. We also attempt to explain several algorithms with their strong and weak points.

However, given there is a huge difference between existing security techniques offered by service providers and the Threats attacks methods employed by cybercriminals, we must wait and see whether this trend is beneficial or bad for security issues. There is tremendous room for improvement, and cloud service providers and the government must work together to address this issue and provide users with a better, safer, and more reliable service.

REFERENCES

[1] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. (2020). A review of machine learning algorithms for cloud computing security. Electronics, 9(9), 1379.

[2] Ko, L.L.; Divakaran, D.M.; Liau, Y.S.; Thing, V.L.L. Insider threat detection and its future directions. Int. J. Secur. Netw. 2017, 12, 168–187.

[3] Nassif, A. B., Talib, M. A., Nassir, Q., Albadani, H., & Albab, F. D. (2021). Machine Learning for Cloud Security: A Systematic Review. IEEE Access.

[4] Khan, N., & Al-Yasiri, A. (2018). Cloud security threats and techniques to strengthen cloud computing adoption framework. In Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 268-285). IGI Global.

[5] Nanane, M. V., Mune, A. R., & Khandade, M. G. (2019). SECURITY ATTACKS DETECTION IN CLOUD USING MACHINE LEARNING ALGORITHMS: A SURVEY. International Engineering Journal For Research & Development, 4(7), 6-6.

[6] 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.

[7] Selamat, N.; Ali, F. Comparison of malware detection techniques using machine learning algorithm. Indones. J.Electr. Eng. Comput. Sci. 2019, 16, 435.

[8] Shamshirband, S.; Fathi, M.; Chronopoulos, A.T.; Montieri, A.; Palumbo, F.; Pescapè, A. Computational Intelligence Intrusion Detection Techniques in Mobile Cloud Computing Environments: Review, Taxonomy, and Open Research Issues. J. Inf. Secur. Appl. 2019, 1–52.

[9] B. Kitchenham and S. Charters, "Guidelines for performing Systematic Literature reviews in Software Engineering Version 2.3," Engineering, vol. 45, no. 4ve, p. 1051, 2007, doi: 10.1145/1134285.1134500.

[10] Shyam, G. K., & Doddi, S. (2019). Achieving Cloud Security Solutions through Machine and Non-Machine Learning Techniques: A Survey. Journal of Engineering Science & Technology Review, 12(3).

[11] Bharadwaj, D. R., Bhattacharya, A., & Chakkaravarthy, M. (2018, November). Cloud threat defense–A threat protection and security compliance solution. In 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) (pp. 95-99). IEEE.

[12] Dey, S., & Sen, S. K. (2017). Four dimensional security and vulnerability matrix for cloud (4-SVM). system, 5, 6.

[13] Akshaya, M. S., & Padmavathi, G. (2019). Taxonomy of security attacks and risk assessment of cloud computing. In Advances in big data and cloud computing (pp. 37-59). Springer, Singapore.

[14] Alowaisheq, E., Tang, S., Wang, Z., Alharbi, F., Liao, X., & Wang, X. (2020, October). Zombie Awakening: Stealthy Hijacking of Active Domains through DNS Hosting Referral. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (pp. 1307-1322).

[15] Vistro, D. M., Rehman, A. U., Mehmood, S., Idrees, M., & Munawar, A. (2020). A LITERATURE REVIEW ON SECURITY ISSUES IN CLOUD COMPUTING: OPPORTUNITIES AND CHALLENGES. Journal of Critical Reviews, 7(10), 1446-1455.

[16] Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., ... & Sarkar, P. (2018, January). Cloud computing security challenges & solutions-A survey. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 347-356). IEEE.

[17] Haider, W., Moustafa, N., Keshk, M., Fernandez, A., Choo, K. K. R., & Wahab, A. (2020). FGMC-HADS: Fuzzy Gaussian mixture-based correntropy models for detecting zero-day attacks from linux systems. Computers & Security, 96, 101906.

[18] Patel, R. V., Bhoi, D., & Pawar, C. S. (2020). Security Hazards, Attacks and Its Prevention Techniques in Cloud Computing: A Detail Review.

[19] Nassif, A. B., Talib, M. A., Nassir, Q., Albadani, H., & Albab, F. D. (2021). Machine Learning for Cloud Security: A Systematic Review. IEEE Access.

[20] Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET Communications, 14(7), 1185-1191.

[21] Suvarna, D., & Pathak, S. (2019, June). Threat Modeling for Breaking of CAPTCHA System. In International Conference on Intelligent Computing, Information and Control Systems (pp. 94-104). Springer, Cham.

[22]Zaytsev, A.; Malyuk, A.; Miloslavskaya, N. Critical Analysis in the Research Area of Insider Threats. In Proceedings of the 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, Czech Republic, 21–23 August 2017; pp. 288–296.

[23] Leu, F.Y.; Tsai, K.L.; Hsiao, Y.T.; Yang, C.T. An internal intrusion detection and protection system by using data mining and forensic techniques. IEEE Syst. J. 2017, 11, 427–438.

[24] Rashid, T.; Agrafiotis, I.; Nurse, J.R.C. A new take on detecting insider threats: Exploring the use of Hidden Markov Models. In Proceedings of the MIST '16 Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats ACM, Vienna, Austria, 28 October 2016; pp. 47–56.

[25]Li, W.; Meng, W.; Kwok, L.F.; IP, H.H.S. Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model. J. Netw. Comput. Appl. 2017, 77, 135–145.

[26] Dahmane, M.; Foucher, S. Combating insider threats by user profiling from activity logging data. In Proceedings of the Proceedings-2018 1st International Conference on Data Intelligence and Security, ICDIS 2018, South Padre Island, TX, USA, 8–10 April 2018; pp. 194–199.

[27] Legg, P.A.; Buckley, O.; Goldsmith, M.; Creese, S. Automated Insider Threat Detection System Using User and Role-Based Profile Assessment. IEEE Syst. J. 2017, 11, 503–512.

[28] Wani, A. R., Rana, Q. P., Saxena, U., & Pandey, N. (2019, February). Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques. In 2019 Amity International conference on artificial intelligence (AICAI) (pp. 870-875). IEEE.

[29] Roberts, S.C.; Holodnak, J.T.; Nguyen, T.; Yuditskaya, S.; Milosavljevic, M.; Streilein, W.W. A Model-Based Approach to Predicting the Performance of Insider Threat Detection Systems. In Proceedings of the 2016 IEEE Security and Privacy Workshops (SPW), Oxford, UK, 8 July 2016; pp. 314–323.

[30] Zhang, M., Song, W., & Zhang, J. (2020). A secure clinical diagnosis with privacy-preserving multiclass support vector machine in clouds. IEEE Systems Journal.

[31] Aktas, M. S. (2018). Hybrid cloud computing monitoring software architecture. Concurrency and Computation: Practice and Experience, 30(21), e4694.

[32] Yang, D., Wei, H., Zhu, Y., Li, P., & Tan, J. C. (2018). Virtual private cloud based power-dispatching automation system—Architecture and application. IEEE Transactions on Industrial Informatics, 15(3), 1756-1766.