**Cyber Security in Cloud Computing: Studies and Solutions**

|  |  |
| --- | --- |
| Sakthivel V\*  School of Computer Science and Engineering  Vellore Institute of Technology  Chennai, India  mvsakthi@gmail.com | Prakash P  School of Computer Science and Engineering  Vellore Institute of Technology  Chennai, India |

**ABSTRACT**

There are several cloud service providers, and the cloud services are broken down into three categories: infrastructure as a service, platform as a service, and software as a service (SaaS) (IaaS). The cloud service providers that offer IaaS are Google Cloud, Microsoft Azure, and Amazon Web Service (AWS). SAP Cloud Platform, Oracle Cloud Platform, and Google App Engine are three cloud service companies that offer PaaS. Salesforce.com, Microsoft Office 365, and Adobe Creative Cloud are SaaS providers. The four categories of cloud deployment models are public, private, hybrid, and community cloud. It is possible to use machine learning (ML), big data analytics, and deep learning (DL) approaches to address security concerns in the context of cloud computing. We also discuss security concerns, which are categorised based on three main categories: data, applications, network, and service. Additionally, we provide a study of recent cybersecurity attacks in the cloud and consider some of the issues and analyse and apply Artificial Intelligence (AI), Machine Learning (ML), Big Data Analyses, and Security Models in this proposed research.

**Keywords:** Cloud Computing, Artificial Intelligence (AI), Deep Learning (DL), Machine Learning (ML), Big Data Analytics, Data’s, Servers, Security, Cybersecurity, Attacks, Resources

1. **Introduction**

The era of cloud computing is happening now as many of the organizations**,** individuals, and most of the IoT devices rely on cloud providers these days. As the use of cloud is very popular for it’s advantages as the cost is drastically reduced compared to the traditional computers, as we have to buy each and everything according to our need, whereas in cloud you just need a stable internet connection, access it from anywhere and you just pay for what you use; flexibility , increased collaboration, insights, low maintenance or almost no maintenance you just have to review the usage, mobility, disaster recovery, scalability, and most importantly back up and restore. IoT devices totally rely on cloud as it generates very high amount of data and computing’s like analytics and processing of the data’s. The usage of IoT devices are drastically increasing in recent times so the demand of cloud is getting higher and higher day by day. There are numerous cloud providers for providing the cloud services and the cloud services are classified into three categories namely Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). The cloud providers those provide IaaS are Amazon Web Service (AWS), Microsoft Azure and Google Cloud. Cloud providers providing PaaS are Oracle Cloud Platform, SAP Cloud Platform, and Google App Engine. SaaS providers are Salesforce.com, Microsoft Office 365 and Adobe Creative Cloud. The deployment model of cloud is divided into 4 types namely public, private, hybrid and community cloud. There are cloud actors who are responsible for the maintenance of business relationship with the users (individual or organizations) and the cloud providers, there are 5 cloud actors namely consumer, provider, auditor, broker and carrier.

**Cloud**

Data Centers

**Clients**

**Provisioning altogether**

Delegations and Regulations of provisioning

Provisioning of resources, and UI

Service Dashboard

Monitoring

**Figure1. A generic architecture of cloud**

When seen from the client's viewpoint, cloud computing resembles the overall architecture in Figure1. While trust delegations and reputation systems maintain the security of the data and information, the cloud hosts datacenters and offers the client with the needed resources and data. Client auditors keep an eye on the IT infrastructure's efficiency and security. Customers may choose and utilise the cloud computing services they need from a service catalogue made available by the cloud service providers. Figure 2 depicts a tier-based architecture with several cloud deployment options, such as private, public, and hybrid clouds. where we have access to IaaS, PaaS, and SaaS services using any device with an internet connection.

Computer network security is the practice of preventing infiltration by employing protocols, techniques, and processes that are intended to keep unauthorized parties out of computer networks, systems, software, and data. Information systems, computers, devices, programmes, data, and networks are targets of cyberattacks from both within and beyond the network's perimeter. Cybersecurity is the practise of preventing, detecting, and reacting to these attacks. One of the most crucial cybersecurity applications is virus and intrusion detection. The whole system is just as secure as its weakest link when it comes to cyber security.

A company's access limits and security measures should be contained by its objectives. We'll go through some of the most prevalent types of cybercrime in this piece, including cryptojacking, data breaches, denial-of-service attacks, insider threats, account theft, insecure software, and a lack of sufficient training. The paper's latter parts address some of the assaults and their AI/ML/DL-based defences. Virtualization, containerization, network monitoring, data security, and threat detection are some of these problems.

Software as a Service

Platform as a Service

**INTERNET**

**Private Clouds**

**Hybrid Clouds**

**Public Clouds**

Provisioning of resources and data

Infrastructure as a Service

**Figure2. Layered architecture of cloud**

1. **A Detailed study of Cloud**

Cloud computing is an evolution in computer science for the next generation, and it can also be used as data centres for the generations to come. Previously, grid computing was used to solve large problems with parallel computing; the stream was made by global alliance; then utility computing was used; through metered service computing resources are offered; then applications are purchased via subscription on the internet; and now cloud computing.

1. **Cloud Deployment**

The public cloud, the private cloud, the hybrid cloud, and the community cloud are the four primary deployment models for cloud computing.

Public clouds are those that are constructed over the internet and allow any user who has paid for the service to have access to the cloud. Public clouds are those that are owned by service providers and can be accessed by paying for a subscription. These clouds provide a remote interface that is open to the public and can be used to create and manage instances of virtual machines inside the confines of a proprietary architecture. In addition to this, it provides a curated collection of business processes, and public clouds support multitenancy. Any kind of service, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), may be provided by Public. Because it is a public cloud, there is always the possibility that the data may be stolen or misused. Because of this, using a public cloud is best suited for individuals and for small businesses that do not deal with any sensitive data or data that has to be safeguarded. Therefore, computing any sensitive data on a public cloud is not a good option.

GoogleAppEngine (GAE), Amazon WebServices (AWS), Microsoft Azure, IBM BlueCloud, and Salesforce.com's Force.com are just a few of the companies that provide public cloud computing as a service.

Private clouds are those that are constructed within the confines of an intranet that belongs to a single company; this company also owns and administers the cloud internally, and access to it is restricted to the company that owns the cloud as well as any partners the company may have. Those users inside an organisation who are making use of cloud computing have more organisational freedom, as well as more efficient, convenient, and adaptable private infrastructures to operate service loads. There are two different kinds of private clouds: ones that are hosted on-premises and ones that are outsourced. The data stored in a private cloud are better protected from unauthorised access since they are only made available to authorised members of the company and are not visible to any other parties. Therefore, sensitive data may be used here without fear of compromise to the SLA (Service Level Agreements) that have been established.HPE, GreenLake, and Azure Stack are just a few of the companies that provide private cloud computing as a service.

A hybrid cloud is one that combines public and private cloud computing resources. It is also possible for private clouds to offer hybrid cloud models. This is accomplished by augmenting the local infrastructure with computing resources sourced from an external public cloud. Offers access to customers as well as the partner network and other parties. Businesses are able to make use of their already established information technology infrastructures, keep sensitive data on-site, and organically expand and contract by procuring external resources and releasing them when they are no longer required thanks to the use of hybrid clouds. A heterogeneous distributed system that is the product of a private cloud and the integration of extra services or resources from one or more public clouds.

Rackspace, VMware, EMC, Fujitsu, NTT, and CenturyLink are a few of the hybrid cloud service providers that are now available.

A Community Cloud is a distributed system that is created by integrating the services of multiple clouds to address the specific needs of an organisation, a community, or a business sector. This system can be managed by the organisation itself or by a third party, and the infrastructure can either be on-premises or off-premises.

Rackspace, Hitachi, Fujitsu, Google, EMC, and Microsoft are just few of the names that fall under the category of community cloud service providers.T

1. **Cloud Services**

There are three types of delivery of services in cloud namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). In **Figure3** the detailed description of the services and which of the services are managed by either the client or the service provider is given.

1. **Cyber Security in Cloud Computing**

Cloud Computing  means outsourcing and trusting a vendor to keep your data and transactions safe. Cybersecurity means keeping it all close, trusting on-site staff, procedures, and protocols to do the job. Cybersecurity is a combination of process, technologies and operations to protect information, resources, data and networks from internal or external threats, attacks or unauthorized access. Cybersecurity consists of the confidentiality, and availability of computing resources, networks, software programs, and data into a descriptive collection of policies, technologies, processes, and techniques to prevent the occurrence of an attack. Cloud providers are responsible for the security of the client’s data, they should provide a best cybersecurity for gaining a customer’s trust. If any attack or threats happen in cloud, providers are responsible any attack or threats happen in cloud, providers are responsible totally and penalty should be paid or compensation should be paid for the loss that client’s suffers. So cybersecurity should be a great priority for the cloud provider.

Some of the techniques currently used by the cloud provider are using passwords for logging in, two factor authenticator, having backup cloud, training the users for validating suspicious emails, suspicious documents, suspicious links and double checking while sending an email or text related to cloud services, network segmentation\ and providing firewalls.

**SaaS**

**On - Site**

**PaaS**

**IaaS**

Apps

Apps

Apps

Apps

Data

Data

Data

Data

Running Tme

Running Time

Running Time

Running Time

Middleware

Middleware

Middleware

Middleware

OS

OS

OS

OS

Virtualising

Virtualising

Virtualising

Virtualising

Servers

Servers

Servers

Servers

Data Storage

Data Storage

Data Storage

Data Storage

Networking Support

Networking Support

Networking Support

Networking Support

Managed by provider

Managed by the product consumer

**Figure3. Cloud Services**

1. **CyberSecurity attacks in Cloud Computing.**

Cybersecurity attacks are internal or external threats, harm, attacks or unauthorised access which may lead to exploiting the data, resources, devices, information and systems and networks. This attack may happen in any layer of the cloud service from the server side to the client side anywhere an attack may be performed either by individuals or a group who have high skills in doing it they are commonly known as cybercriminals or hackers. Cybercriminals have various motives when some carry out attacks for personal and financial gains or acting in the name of social and political cause. Some attacks are a result of cyberwarfare conducted by nation against their opponents.

Some of the largest cybersecurity attacks in recent years:

• CAM4 – 2020

10.8 billion private records comprising 7 terabytes of data from the adult live streaming website CAM4 were exposed in March 2020 as a result of a cloud cyberattack. The breached database included data such as usernames, email addresses, payment history, IP addresses, and more.

• AIS 2020 (Advanced Information Service)

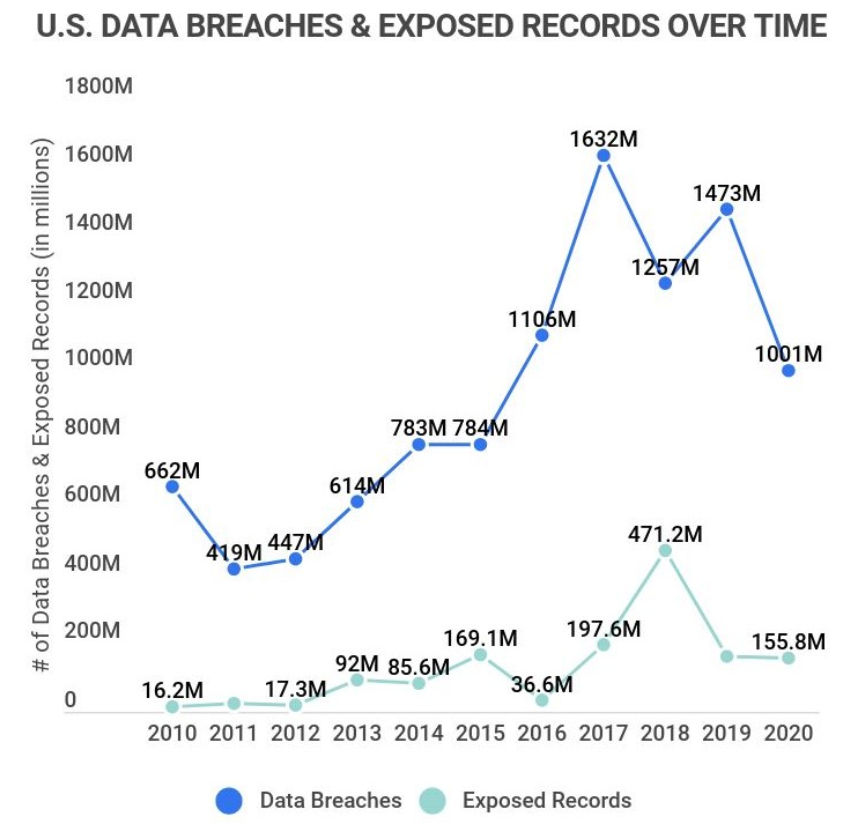
Using the well-known search engines BinaryEdge and Shodan, Justin Paine looked through possible data breaches and found onto the AIS data leak. According to Paine, the stolen database included 8.3 billion network flow records and DNS query logs that belonged to AWN customers of the Thailand-based telecommunications company.

• Holdnet Laboratories: 2020

One of the most humorous cloud data breaches in 2020 was the Keepnet Labs data breach, which included a hacked ElasticSearch database whose leaked data had already been exposed in prior breaches. A portion of the database included 5 billion entries, while another contained 15 million records.

• Microsoft—2019

The email addresses, IP addresses, and support case data of 250 million customers were made public due to a security compromise in December 2019, according to a statement from Microsoft on January 22, 2020.



**Figure 4. CyberAttacks happened from 2010 to 2020 in U.S.**

In **Figure4** the graph shows the cyberattacks happened in U.S from the time line 2010 to 2020, as we can see the data breaches are decreasing since the AI/ML/DL techiniques are evolving the cloud providers are trying to give the best security features in the cloud environment.

Some of the key cybersecurity attacks that are discussed in this paper:

• Cryptojacking.

The new kind of hacking known as cryptojacking may be carried out in complete secrecy and is exceedingly easy to execute. Hackers have found methods to access cloud computing services and utilise the processing power of such platforms for their own benefit. The most significant issue is that hackers using your cloud system's computer resources will cause your operations to slow down, but other than that, everything else will continue to work properly. This suggests that it can provide the impression that nothing sinister or out of the ordinary is taking place, and that the only problems the computers are having are those linked to processing. As a result of the fact that many people mistake the symptoms of cryptojacking with those of an update or a slower internet connection, it might be difficult for these individuals to identify the real problem.

• A data breach.

When a user's data are used not only by the user but also by someone else, a data breach has occurred. Data breaches take place when a user's data are in the possession of a third party and the user and another user share resources. In the event that a database or its associated data have a vulnerability, this might put the privacy and safety of the data of other individuals at risk.

• The destruction of data.

The loss of data is yet another significant issue that might develop with cloud security. When there is a data loss, the information that users have saved is lost, but when there is a data breach, the information is stolen. The user may choose data security, for instance, in order to safeguard the information they have stored. However, if the encryption key is misplaced, there is a possibility that data may be lost.

• Denial of Service Attacks, as well as Distributed Denial of Service Attacks (DDoS) (DDoS).

One of the attacks that might occur in cloud computing that is among the most damaging is called a denial of service attack (DoS). These might cause the cloud services to be taken down, leaving them unavailable to users, customers, and the whole organisation. When hackers get into a system, they flood it with an excessive amount of web traffic, sometimes to the point that the servers of the users can't manage it. If everything about the system is hosted in the cloud, management of the business or service could be challenging.

• Phishing Attacks.

Like the word refers phishing is like fishing which, where the one who suffer from the attack is like a fish and the attacker is the fish catcher and he uses baits like spam email, spam links, or any texts which misleads to get into a trap where the accounts is been hijacked or an abusive behaviour is shown in which the attacker utilize some cloud services to host.

• Insider threats.

Some of the problems not only are attacked from the outside also it may originate from inside the organisation. Insider threats can be malicious and dangerous like the staffs going rude, also it can happen due to the negligence or common human errors. Also the company should have a proper off-boarding process which when someone leaves the company they should be sure that their access to any crucial data is removed and the credentials is no longer can be used to login in any platforms or services.

• Hijacking accounts.

The great threat to companies using cloud computing is the hijacking the accounts. If the cyberattacker steals the access to the system through any of the staffs account, they could gain the full access to the information and data of the systems and servers without the organisations knowledge. The attacker use phishing and password cracking in order to get the credentials of the account. One way of reduce the risk of hijacking account is through proper permissions management it means that every account in the company should only be given access to the information that they need to do their job.

• Insecure applications.

Sometimes some external applications may be threat to the company, third-party applications can be a serious cloud security risk , so the employees need an expert advice before using an application, the team should take the cybersecurity experts to establish whether the application is suitable for the network before installing. Do not encourage on the employees to take their own decisions.

• Insecure API’s.

Due to the growth of Application Programming Interface (API) usage, securing API’s are very important, misconfiguration, errors, lack of authentication and unauthorised access of API’s can lead to data breaches and vulnerabilities. These can lead to the malicious activities of vulnerable interfaces. Organisations are rapidly in the process of adopting API’s with improved connectivity and agility. The risk of the insecure API varies depending on the usage and data associated with the API, as well as how fast the vulnerability is detected. The most commonly reported business impact is the unintended exposure of sensitive or private data left unsecured by the API.

• Inadequate training.

Most of the attacks are from outsiders and some are from the insiders, so the employees should have an training of tackling a cybersecurity attacks. The team should have known the list of attacks possible, possible ways of attacking, pre requisite for defending a attack and to know the solution after an attack has happened. The employees are the first line of defence against any attack, so they need to be in up to date of the information and recent threats. It is not only simply getting knowledge for phishing and setting strong passwords are not enough a separate team for educating the cybersecurity attacks and solutions should be recruited and used wisely by the companies.

1. **Solutions based on AI/DL/ML to Cyber Security attacks.**

Machine learning is divided into 3 parts of algorithms supervised, unsupervised and semi – supervised algorithms. Main characteristic of machine learning is to train and deploy large sets of production models for relationships among data.

Machine learning and artificial intelligence technologies to process the data and find anomalies, prioritise their workloads and processes more effectively.

Machine learning is a subset of artificial intelligence, which has two models static and dynamic.

Static machine learning is providing a artificial intelligence solution with offline training, which is suitable for detecting and managing environments that are static (i.e. which does not change).

Dynamic machine learning is also known as deep learning solutions train themselves in online. Deep learning uses huge data resources containing malicious behaviours and cognitive patterns. Big data resources for machine learning are data of many years about how threats attacks on a network or a system.

The use of deep learning is growing as the need for malware detection with low error rates, cloud providers are starting to supply antimalware solutions with dynamic machine learning. So when organizations are getting service from a cloud provider they should ensure that they are getting genuine dynamic ML that has been maintained and provide proper defence.

A machine learning model for securing the data by encrypting the data and employ cloud servers to perform high-order back-propagation algorithm on encrypted data for deep computational model training . A new scheme which guarantees the security of encrypted cloud data.

Machine learning algorithm – Artificial Neural Network (ANN) can be used for detecting and mitigating the unknown and known Denial of Service attacks in cloud environments based on the patterns that Distributed Denial of Service (DDoS) attack traffic from real traffic.

Support vector machine (SVM), random forest, K-means clustering, fisher’s linear discriminant classifier, bayes network, linear regression, polynomial regression, decision tree, neural network logistic regression, fuzzy C- means, K-nearest neighbours, linear means and linear kernel are some of the machine learning techniques used for the cyber security in cloud computing.

1. **Conclusion**

Cybersecurity in cloud computing is the most critical issue in data and resources privacy. The cloud providers are more concentrating now a days in the security of cloud as the users are demanding for more security and privacy from the providers. So the security should be the key feature of the future cloud computing. Although there are many security features provided by the providers still the attacks are increasing day by day. Most of the attacks are outer and some of the attacks are inner attacks that is happening from inside the premises knowingly or unknowingly and most of the outer attacks are from phishing and intentional attacks by hackers for their own financial benefits. As the artificial intelligence, machine learning and deep learning are evolving nowadays they can be used to tackle and used as a defence mechanisms and also can be used to recover from the attacks.

1. **References**
2. Jitendra Singh (2014), *Cyber-Attacks in Cloud Computing: A Case Study.*
3. Daniel G. Arce (2020) *, Cybersecurity and platform competition in the cloud.*
4. *Gabriel Kabanda (2021), Performance of Machine Learning and Big Data Analytics Paradigms in Cybersecurity and Cloud Computing Platforms.*
5. Waqas Ahmad 1 , Aamir Rasool 2 , Abdul Rehman Javed 3 , Thar Baker 4, and Zunera Jalil 5 (2021)*, Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey.*
6. Ali Bou Nassif 1, Mannar Abu Talib 2, Qassim Nasir 3, Halah Albadani 4, Fatima Mohamad Dakalbab 5 *, Machine Learning for Cloud Security: A Systematic Review*
7. <https://www.triskelelabs.com/blog/cloud-cyber-attacks-the-latest-cloud-computing-security-issues#:~:text=Any%20cyber%20attack%20that%20targets,SaaS%2C%20IaaS%2C%20and%20PaaS>.
8. <https://www.zippia.com/advice/cybersecurity-statistics/>