Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2024, 11(9):103-110

Research Article ISSN: 2394 - 658X

Investigation on Cloud Security Frameworks, Problems and Proposed Solutions

Vedaprada Raghunath

IT Director, IMR soft LLC, USA.
vedapradaphd@gmail.com

ABSTRACT

Security is becoming more of an issue with cloud computing due to its fast expansion. The purpose of this research article is to analyse cloud security frameworks, discuss problems related to the cloud, and offer recommendations for fixing them. In order to make well-informed choices about the selection and implementation of appropriate security measures for cloud-based systems, this research expands our understanding of the different frameworks. The paper starts by providing an overview of cloud technology, discussing its benefits and drawbacks, and then moves on to analyse the many cloud security frameworks that are now available. The framework's strengths, weaknesses, scope, strategy, implementation phases, and necessary tools are all thoroughly examined through a comprehensive comparison. This document offers a comprehensive overview of several well-architected frameworks, including COBIT5, NIST, ISO, CSA, STAR, and AWS. Finding and analysing common cloud security concerns is the focus of the study's later sections. The following are some of the potential entry points for attacks in a cloud environment. Along with that, this section covers the dangers posed by the most common cloud security risks and how they impact cloud platforms. Additionally, it offers solutions and suggestions to lessen the problems that have been identified.

Keywords: Cloud security; security frameworks; NIST; COBIT; ISO; AWS; ENISA

INTRODUCTION

The emerging technology known as cloud computing (CC) is only loosely related to grid computing (GC) and other ideas such as utility computing, distributed computing, and cluster computing [1]. Virtualization of resources should be the end result of GC and CC when applied correctly. Despite sharing a common goal, GC and CC couldn't be more dissimilar in execution. While CC primarily aims to optimise overall computing capacity, GC primarily aims to maximise computing [2]. Additionally, CC provides a way to handle a wide range of organisational needs with its dynamically extensible servers and apps [3]. Everywhere in the world, average people are getting on board with popular cloud computing (CC) services such as AWS, IBM Watson, Dropbox, iCloud, Google Apps, Azure, etc. The new paradigm that CC has introduced enables its users to build or store apps on the move and access them from any Internet-connected device, anywhere in the world, at any time [4].

The services that CC offers to access or interact with cloud apps are easy and customisable, depending on the customer's requirements. Applications to perform user-regular tasks, infrastructure to store and process firm data, and a platform for application building are all under CC's purview, depending on user needs.

Data kept in local repositories will be transferred to a distant data centre when a client opts to utilise cloud services [5]. The services offered by cloud providers make it possible to view or manage data stored in faraway locations. It is now crystal evident that data transmission to a distant server via a channel (the internet) is required for any user wishing to store or analyse data in the cloud [6]. Extreme caution must be exercised in handling and storing this data in order to forestall data breaches.

Data sent and processed on the cloud is more vulnerable than data saved or processed locally if adequate security measures are not in place [7]. Anyone with malicious intent can intercept data in transit to or from the cloud by eavesdropping on the user's connection to the remote server. By establishing a second account (via the usage of the virtualized infrastructure that CC offers) within the same provider, he can further get access to users' accounts and

sensitive data [8]. The fact that cloud computing caters to a wide range of customers means that data loss is a real possibility when utilising these systems (nave, expert, malevolent, etc.).

It is clear from the preceding discussion that organisations should not deploy CC until the security issues associated with cloud adoption and cloud interoperability have been resolved [9]. The majority of organisations view security as a critical issue that requires attention, according to a non-exhaustive search on CC problems [10]. There will always be further vulnerabilities discovered and exploited, no matter how robust the security measures are. Therefore, it is crucial to identify security concerns, make improvements, and update solutions in order to adopt CC.

LITERATURE REVIEW

The authors presented a method in [11-13] to detect and avoid attacks using three machine learning methods, including J48, naïve Bayes, and oneR approaches.

J48 was the algorithm that had the highest classification performance across all of these distinct algorithms, with an accuracy of 94.5 percent and a sensitivity of 94%. Nevertheless, this strategy is only designed to be used for attacks that are web-based.

Further, a literature review on machine learning (ML) for cybersecurity was recently conducted by the authors of [14-16] due to the rapid, if not exponential, advancement of ML's application to combat cybersecurity threats. As a result, by using various machine learning methodologies, this work shows that cybersecurity development has tremendous prospects. Indeed, in order to prevent, identify, and lessen the impact of distributed denial of service attacks, the authors of [17-19] laid forth a strategy that employs machine learning techniques.

Nevertheless, the findings indicate that the accuracy of this investigation did not surpass 76%, despite the fact that a variety of algorithms were utilised.

Real-time operations cannot tolerate the mistaken rejection of routine processes or genuine traffic. This is not acceptable. Because of this, the authors of [20-21] developed an algorithm that has a specificity of one hundred percent and can identify zero false positives, which allows it to both detect and prevent attacks. However, while calculating performance, the authors only looked at false positives, ignoring other important metrics like accuracy and sensitivity.

Furthermore, a method that was published in [22-23] was recently developed to assure the integrity of distributed compute outsourcing in several fields, such as grid computing and volunteer computing, as well as to detect cheaters and malicious attacks. In order to protect against malicious attacks, the primary concept relies on the manipulation of inputs through the addition or mixing of noise. The authors used a game-theory based methodology to test the suggested strategy; the accuracy was consistently below 61.24 percent.

In their paper, the authors of [24-26] presented a methodology for identifying DDoS attacks in an SDN setting. This structure employs a combination of K-means and K-nearest neighbours based machine learning techniques. Classification results in this study are remarkable (98 percent accuracy, 98 percent sensitivity, and 97 percent specificity), however the approach is only applicable to DDoS attacks.

However, in order to presuppose higher degrees of security and detection capacity against assaults, the writers of [27-29] developed a novel method for testing detection models. This approach aims to provide end-to-end encryption for detection models by making use of lattice-based cryptography. To achieve their goal of assessing the classification performance, the authors built a protocol on decision trees that had been trained on several real-world datasets.

The results demonstrated a remarkable performance in terms of categorization, with an accuracy of 99% and a sensitivity of 98%. On the other hand, this protocol was developed solely for intrusion detection systems; hence, it cannot be generalised to other detection models.

An artificial intelligence-based method was proposed by the authors of [28] for the purpose of identifying insider assaults in an Internet of Things (IoT) environment. This algorithm makes use of distance measurement techniques that have qualities that are associated with artificial intelligence technologies. As a consequence of the simulation, it was determined that the accuracy of this study did not reach fifty percent.

In addition, the authors of [30-33] proposed a new system that they named fuzzy Gaussian mixture-based Corr entropy. Linux hosts can be protected from both known and zero-day threats using this solution, which was specifically developed for that purpose. An essential classification performance is provided by the experimental findings, which are nearly 97% in terms of sensitivity, specificity, and accuracy. Nevertheless, this technology is only capable of protecting Linux hosts.

CLOUD SECURITY CHALLENGES IN DIFFERENT CLOUD ENVIRONMENTS

In general, there are three distinct types of cloud environments: public clouds, private clouds, and hybrid clouds. These three options allow you several security setups that are in line with the shared responsibility paradigm. This model details the allocation of resources, the transfer and storage of data, the creation of connections, and the people in charge of security.

Public cloud

Public cloud hosting is typically provided by external firms such as Amazon Web Services (AWS), Google Cloud, or Microsoft Azure. While these services offer efficient and cost-effective authentication management and access control, the security of these services could be compromised due to their use of the shared resources paradigm.

To ensure the safety of your environment, you will need to find a way to overcome the difficulties that are associated with the implementation of new security tools. Some tools are offered at no cost, while others have expenses associated with their operation. If you want to take care of that responsibility, you either need to learn how to utilise the tools or hire an expert to do it for you. In that case, security vulnerabilities could be caused by incorrect configuration or improper use of the tools.

Private clouds

Contrarily, there is no universally accepted difference between the security of public and private clouds. While security measures are already part of the service ecosystem for public cloud services, the onus for protecting private cloud environments lies squarely on the shoulders of the in-house staff.

When it comes to security, businesses who fail to execute routine maintenance and updates will leave themselves vulnerable to potential security flaws. Additional security concerns may arise as a result of the absence of transparency in certain private cloud configurations. Software upgrades, for instance, have the potential to introduce security vulnerabilities. Social engineering attacks and access breaches are particularly problematic for private clouds because of their high level of vulnerability.

Hybrid clouds

In a hybrid cloud, features from both public and private clouds coexist in one setting. An increased level of control over their data and resources is afforded to businesses by this method. It is possible for hybrid clouds to become simple targets for assaults if the network execution is not done properly, if the security protocols are not effective, and if the management chains are disrupted. Compliance becomes a difficult process due to the fact that hybrid clouds integrate many services within a single structure. This is because each environment is unique, but these environments are required to adhere to the same regulations. When it comes to hybrid networks, any setting that transports data within them is open to cyberattacks and eavesdropping. Data leakage, inadequate risk assessment, inadequate data redundancy, and the lack of encryption make hybrid clouds highly susceptible to attacks.

CLOUD SECURITY RISKS

Security is a major concern with cloud systems because of the increased access to sensitive data and the lack of control over the network. The most typical threats to systems hosted in the cloud are as follows:

Data breaches – Cloud infrastructure has been linked to numerous high-profile data breaches. An organisation runs the risk of having sensitive data stolen or lost if its cloud resources are not secure, as they can be put on the open Internet.

Contractual breaches – In certain cases, parties may agree in writing to a set of conditions that govern their shared data usage, including who may access what data. An instance of this would be the unauthorised movement of data from local to cloud servers. These businesses risk losing money or being held legally liable if an attack causes them to break their obligations.

Data loss – Cloud security doesn't solve every problem with data loss, but it does make backup and disaster recovery easier and cheaper. Cloud settings offer more data redundancy and storage capacity across numerous cloud data centres compared to on-premise systems.

Gaps in compliance – By requiring businesses to adhere to a predetermined set of security regulations, compliance standards aid in the prevention of data breaches. The complexity and opaque nature of cloud infrastructures causes many organisations to have serious compliance gaps.

Hacked interfaces and insecure APIs – Central to cloud computing are application programming interfaces and interaction points. Application programming interfaces (APIs) facilitate system integration, but they also provide hackers with a backdoor.

Malware infections – used by cybercriminals to gain access to protected accounts and systems, wipe data, and steal personal and financial data. When stealing sensitive information, cybercriminals often exploit cloud services as a gateway.

Identity management and weak authentication – Cloud authentication security relies on the ability to manage identities across several services. Data breaches and issues with access authorization arise when cybercriminals are able to easily access critical systems and credentials because of inadequate identity management.

Insufficient due diligence and shared vulnerabilities – Moving to the cloud without verifying that the security measures of the cloud provider adhere to industry standards or provide essential controls might result in serious security breaches and shared vulnerabilities that anybody can exploit.

Abuse and misuse – Security breaches can occur when firms use cheap infrastructure or pirated software.

Data migration complexity and misconfiguration – The intricacy of cloud migrations makes them particularly vulnerable to setup errors, which can compromise security, particularly when migrating data to and from the cloud. Data can be exposed due to a lack of knowledge or supervision over security settings.

CORE PRINCIPLES OF A CLOUD SECURITY ARCHITECTURE

Protecting cloud resources from security risks requires a well-designed cloud security system that incorporates the necessary policies, procedures, and tools. The following should be included as fundamental principles:

Security by design – Secure controls should be built into cloud architecture so that they cannot be compromised by security misconfigurations. For instance, if a cloud storage container contains sensitive data, the administrator should not be able to grant access to the public Internet. All outside entrances must be sealed.

Visibility – Conventional security measures are inadequate for the multi-cloud and hybrid-cloud deployments that many organisations employ. A well-rounded plan takes into consideration the methods and resources needed to keep tabs on every aspect of a company's cloud-based infrastructure.

Unified management – Since security professionals are frequently understaffed and overworked, it is imperative that cloud security solutions offer uniform administration interfaces. Cloud security solutions vary greatly, and teams need a way to manage them all from a single interface.

Network security – It is the responsibility of the company to ensure the security of data transfers to and from cloud resources, as well as between public cloud and on-premise networks. A philosophy of shared accountability underpins cloud operations. If you want to make it harder for an attacker to spread laterally once they get into your network, segmenting your networks is a must.

Agility – Cloud computing facilitates the creation and implementation of novel solutions. This nimbleness shouldn't be impeded by security. Businesses can take advantage of security solutions built for the cloud that work in tandem with agile development processes.

Automation – rapid deployment and updating of cloud security controls relies heavily on automation. Misconfigurations and other security holes can be found and fixed instantly with its help.

Compliance – Legislation and regulations like GDPR, CCPA, and PCI/DSS ensure the security of cloud data and procedures. In order to manage compliance across several cloud providers, organisations often require third-party solutions, even though they can use solutions provided by cloud providers.

CLOUD SECURITY SOLUTIONS TYPES

Organisations may safeguard their cloud deployments with the help of these standard technologies.

Cloud Workload Protection Platform (CWPP)

Secure your cloud workloads with CWPP, a security solution that reveals resources across multiple clouds, verifies proper deployment, and implements necessary security controls.

Active security tasks can be carried out by CWPP, such as application and operating system hardening, vulnerability detection and remediation, application whitelisting, and integrity checks.

Cloud Security Posture Management (CSPM)

CSPM verifies cloud infrastructures for potential compliance risks and configuration errors. Its principal goal is to automate security configuration and provide centralised control over configurations that impact compliance or security. The majority of CSPM implementations use cloud computing. It does more than just list cloud resources; it also lets you set and enforce policies across the entire organisation and check resources (such databases, storage buckets, or compute instances) for potentially harmful configuration errors. It is possible to perform risk assessments using criteria established by organisations like ISO, NIST, and CSI Benchmarks.

Cloud Access Security Broker (CASB)

Organisations can benefit from CASB's ability to identify and manage their SaaS applications. Common applications include detecting sensitive data transfers to and from cloud applications and shadow IT (the illegal usage of cloud services). In order to support the unique APIs and ecosystems of their SaaS applications, many organisations utilise numerous CASB solutions. Authentication to stop unauthorised access to content, web application firewalls (WAF) to stop threats at the application layer, data loss prevention (DLP) to find and stop data exfiltration, and traditional firewalls are all parts of CASB solutions that work together to make sure network traffic going to and from the cloud is secure.

eXtended Detection and Response (XDR)

Cloud, on-premises, and endpoint systems are all within XDR's comprehensive security platform's purview. Its purpose is to make it possible to see, detect, and respond to dangers in any environment, not just the IT one. It can collect data from cloud networks and interface with endpoints like containers and compute machines in the cloud. When used in conjunction with other cloud security solutions, XDR can detect complex or concealed threats, particularly those that lurk in system-to-system interfaces. It can compile information from multiple sources to build a full picture of an assault, allowing you to see suspicious activity in one system that could be hiding a more serious threat.

SaaS Security Posture Management (SSPM)

A suite of SaaS applications can benefit from SSPM's visibility, monitoring, and assistance in fixing security vulnerabilities. SaaS security control gaps, such as misconfiguration and non-compliance with common organisations and standards like PCI DSS, SOC 2, and Centre for Internet Security (CIS) benchmarks, can be found and fixed with the use of SSPM.

Managed Detection and Response (MDR)

Threat detection and removal (MDR) is a managed service that does just that.

Both cloud and on-premises infrastructures can benefit from its usage. The use of endpoint detection and response (EDR) technologies and the expertise of human operators and maintenance staff are common components of MDR services. By utilising MDR security platforms, organisations can enjoy the advantages of a state-of-the-art security operations centre (SOC) with continuous monitoring capabilities, all without the burden and expense of running their own SOC. Advantages to organisation security offered by MDR services include:

- Advanced analytics
- Threat intelligence
- Human security expertise
- Incident investigation experience
- Incident response experience

Cloud data security

Data stored in the cloud, regardless of supplier, must adhere to certain regulations set out by cloud data security software. Data can be protected both while stored in the cloud and while being transferred to and from the cloud. A component of cloud data security systems, data loss prevention (DLP) can centrally manage data encryption, governance, and rights for sensitive data and detect suspicious behaviours that could cause sensitive data to be lost or stolen.

Cloud monitoring

Without cloud monitoring tools, a cloud security plan is lacking. Organisations must constantly keep an eye on their cloud-based resources in order to gain visibility (to know what's running and where) and spot anomalies (security issues).

In the cloud, you can find five primary forms of monitoring:

- A database's accessibility, utilisation, performance, and availability in the cloud can be monitored.
- Website monitoring entails keeping tabs on the accessibility, performance, traffic, and users of websites and online applications hosted in the cloud.
- Keeping an eye on virtual networks at the firewall, load balancer, and router levels is essential for cloud security.
- By keeping tabs on your cloud storage, you can see how various apps, databases, services, and compute instances are using it.
- Just like with servers physically located on-premises, virtual machines in the cloud need to have their availability, traffic, and access to compute instances monitored.

Cloud compliance

To ensure they are meeting their cloud compliance standards, organisations can use cloud compliance software. It reveals whether cloud services might be in breach of particular compliance regulations by providing insight into workloads operating on private and public clouds, as well as network traffic and configurations. While CWPP and cloud compliance systems have certain similarities, CWPP is unique in that it is concerned with managing and enforcing security measures within the cloud. Cloud compliance solutions, in contrast, are passive tools that can notify users of violations, provide guidance on how to resolve them, and generate thorough audits and reports.

Cloud backup and disaster recovery

An efficient cloud security programme must include cloud backup. Protecting cloud assets from threats like malware and ransomware, as well as accidental or malicious manipulation or destruction, can be made easier using this.

With cloud backup, a company can upload an exact replica of its files or even its whole system, including containers and virtual machines, to the cloud. In the event that the original data becomes corrupted, the backup copy can be easily restored from a cloud data centre. Storage capacity, data transmission bandwidth, and access frequency are the main factors that determine the cost of cloud backup services. You can use them to back up resources in the cloud as well as those on your own servers. Disaster recovery is another critical use case for cloud backup. Historically, in the event of a disaster, it was necessary to set up a whole separate data centre and move all of your data there. For lesser-known groups, this was simply too costly. An appealing substitute is cloud disaster recovery solutions, which enable businesses to simply create cloud-based system duplicates and activate them as needed in the event of a disaster.

CLOUD SECURITY BEST PRACTICES FOR MAJOR CLOUD COMPUTING PLATFORMS

Most cloud-based businesses use one of the three major cloud providers: Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform. Security best practices and technologies are part of the extensive ecosystems offered by each of these cloud providers. Here are some broad rules to follow when trying to strengthen security in a public cloud setting before we get into the particulars of each cloud provider:

Network segmentation – division of networks into subnets to enhance safety and performance. After segmentation is set up, you can isolate systems and components by assessing the resources that are available and using a zone technique.

Identity and access management (IAM) – reduce potential security threats including account takeovers and unauthorised access. Robust identity and access management systems facilitate the establishment and maintenance of access controls, including role-based authorization and multi-factor authentication. In order to keep track of who has access to what in the cloud, access control lists (ACLs) are necessary.

Training your staff – Workers must be aware of the security hazards associated with company technology and take personal responsibility for how they utilise it. Train employees to use complex passwords, spot malicious communications, and deal with shadow IT. The individual and the firm are both put at risk when unauthorised cloud services are used.

Implementation of cloud security policies – Specify the necessary safety protocols, how to properly utilise all services, what types of data can be stored in the cloud, and how much permission each user has.

Endpoint security – keeps an eye on user actions in the cloud and safeguards endpoints. Interception of intrusions, firewalls, access control, and anti-malware software can help you build a solid defence.

Data encryption – Data is at risk of assaults both while in transit and when stored, thus encryption is a crucial security measure.

Audits and penetration testing – makes sure your security architecture is still up to snuff and can help you find places to make improvements. To ensure that only authorised persons are shown in the access logs and to assess the capabilities and compliance of suppliers with your SLA, it is recommended to conduct audits and tests.

Cloud disaster recovery – make sure data is safe by establishing reliable backup systems. Check that your data backup, retention, and recovery policies are compatible with those of your cloud provider.

Plan for compliance – ensure that you are well-versed in and equipped to follow all relevant guidelines, standards, and laws. Get a good grasp on what it takes to become compliant in the cloud before you blindly trust cloud vendors' claims regarding compliance.

AWS security best practices

1) Limit security groups

Access to AWS resources is restricted by security groups. Allow only those IP addresses and ports that are absolutely necessary for components to function. Amazon Web Services (AWS) Config and AWS Firewall Manager allow you to apply your virtual private cloud (VPC) network policies and WAF rules to resources that are accessible from the public Internet.

2) Automate backup

To safeguard data from threats like ransomware, unintentional loss, and corruption, backups are a must-have security measure. All of Amazon's primary services, including RDS, DynamoDB, Elastic File Service (EFS), and Elastic Block Storage (EBS), may be centralised through the AWS Backup service. On top of that, Amazon gives you access to backup capabilities through API and CLI.

3) Centralize logs

Logs and events from every Amazon service can be found in Amazon CloudTrail. Store all of your logs in S3 buckets, including CloudTrail, load balancer, and other monitoring service data, as well as your own cloud-native app logs. The best way to analyse and correlate logs across all Amazon services is to create a central log archive. You can create security alerts using the data by using a SIEM system, which stands for security information and event management.

4) Isolate Kubernetes Nodes

Isolating Kubernetes nodes is another best practice, especially when using Amazon Elastic Kubernetes Service (EKS) to host Kubernetes clusters. One robust orchestration tool for handling containerised apps is Kubernetes. But if not protected correctly, it may also be a way in which attacks could enter.

When nodes are isolated, they are separated into several security groups or VPCs. By lowering the stakes, the attack surface is decreased in the event of a security breach. The intruder will have a hard time compromising other nodes in the network after they have infiltrated one. To further regulate data transfer inside a Kubernetes cluster, network policies are recommended.

5) Scan Container Images

Vulnerabilities may be present in container images and could be used by malicious actors. The security of your AWS system relies heavily on checking container images for vulnerabilities.

Fargate, a serverless compute engine, is a popular choice for running containers on AWS. Run containers without worrying about the underlying infrastructure thanks to this. For additional information, check out the Amazon blog post. One useful feature is CloudFormation, which can automate image scanning for all containers deployed to Amazon Fargate.

CONCLUSION AND FUTURE WORK

Cloud computing, a field that is both fraught with challenges and of the utmost importance, is still in its infancy at the moment, and a great deal of research challenges have not yet been identified. This is something that we acknowledge as being completely accurate. Different types of algorithms are utilised for the purpose of addressing security concern as a result of this reconsideration. An issue is there even when encryption has been introduced. In order to protect against the dangers, modern encryption techniques are being utilised. Prior to the transmission of the data, the encryption will need to be applied at the client environment in the future.

REFERENCES

[1]. Akbar, H., Zubair, M., & Malik, M. S. (2023). The Security Issues and challenges in Cloud Computing. International Journal for Electronic Crime Investigation, 7(1), 13-32.

[2]. Gimba, U. A., Ariffrin, N. A. M., Musa, A., & Babangida, L. (2023). Comprehensive analysis of security issues in cloud-based Internet of Things: A survey. Journal of Computer Science & Computational Mathematics, 13(2).

[3]. Joshi, M., Budhani, S., Tewari, N., & Prakash, S. (2021, April). Analytical review of data security in cloud computing. In 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 362-366). IEEE.

[4]. Imad M. Abbadi and Cornelius Namiluko. Dynamics of trust in Clouds— Challenges and research agenda. In Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, pages 110–115, 2011. 46

[5]. Hussain Al-Aqrabi, Lu Liu, Jie Xu, Richard Hill, Nick Antonopoulos, and Yongzhao Zhan. Investigation of IT security and compliance challenges in security-as-a-service for cloud computing. In Object/Component/ServiceOriented Real-Time Distributed Computing Workshops (ISORCW), 2012 15th IEEE International Symposium on, pages 124–129, 2012. 33, 37, 40, 44, 49, 75

[6]. M. Al Morsy, J. Grundy, and I. M¨uller. An analysis of the cloud computing security problem. In the proc. of the 2010 Asia Pacific Cloud Workshop, Colocated with APSEC2010, Australia, 2010. 42, 43, 45, 48, 68, 69

[7]. Aiiad Ahmad Albeshri and William Caelli. Mutual protection in a cloud computing environment. In IEEE 12th International Conference on High Performance Computing and Communications (HPCC 2010), pages 641– 646, 2010. 11, 27, 33, 37, 46, 52, 62, 75

[8]. Abdulrahman Almutairi, Muhammad Sarfraz, Saleh Basalamah, Walid Aref, and Arif Ghafoor. A distributed access control architecture for cloud computing. Software, IEEE, 29(2):36–44, 2012. 51, 72

[9]. William; Athley Ambrose. Cloud Computing: Security Risks, SLA, and Trust. 2010. With Cloud Computing becoming a popular term on the Information Technology (IT) market, security and accountability has becomeimportant issues to highlight. In our research we review these concept ... 10, 15, 18

[10]. T. Andrei and R. Jain. Cloud computing challenges and related security issues. A Survey Paper. DOI= http://www. cse. wustl. edu/ jain/cse571- 09/ftp/cloud. pdf. 25, 26, 32

[11]. S. Sharma, P. Zavarsky and S. Butakov (2020) "Machine Learning based Intrusion Detection System for Web-Based Attacks", in Proceedings of the 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (pp. 227–230). https://doi.org/10.1109/BigDataSecurityHPSC-IDS49724.2020.00048.

[12]. H. Bahassi, N. Edddermoug, A. Mansour and M. Azmi (2022) "Toward an exhaustive review on Machine Learning for Cybersecurity". Procedia Computer Science 203: 583-587.

[13]. M. Ali, F. Benamrane, D.K. Luong, Y. Hu, J. Li and K. Abdo (2019) "An AI based Approach to Secure SDN Enabled Future Avionics Communications Network Against DDoS Attacks", in Proceedings of the 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC) (pp. 1–7). https://doi.org/10.1109/DASC43569.2019.9081639.

[14]. M. Sayad Haghighi, F. Farivar and A. Jolfaei (2020) "A Machine Learning-based Approach to Build Zero False-Positive IPSs for Industrial IoT and CPS with a Case Study on Power Grids Security". IEEE Transactions on Industry Applications pp. 1–1. https://doi.org/10.1109/TIA.2020.3011397.

[15]. A.T. Haghighat and M. Shajari (2020) "Service Integrity Assurance for Distributed Computation Outsourcing". IEEE Transactions on Services Computing 13: 1166–1179. https://doi.org/10.1109/TSC.2017.2771469.
[16]. L. Tan, Y. Pan, J. Wu, J. Zhou, H. Jiang and Y. Deng (2020) "A New Framework for DDoS Attack Detection and Defense in SDN Environment". IEEE Access 8: 161908–161919. https://doi.org/10.1109/ACCESS.2020.3021435.
[17]. W. Haider, N. Moustafa, M. Keshk, A. Fernandez, K.K.R. Choo and A. Wahab (2020) "FGMC-HADS: Fuzzy Gaussian mixture-based correntropy models for detecting zero-day attacks from linux systems". Computers and Security 96: 101906. https://doi.org/10.1016/j.cose.2020.101906.
[18]. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)
[19]. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D. Dissertation.University of South Alabama.
[20]. GPB GRADXS, N RAO, Behaviour Based Credit Card Fraud Detection Design And Analysis By Using Deep Stacked Autoencoder Based Harris Grey Wolf (Hgw) Method, Scandinavian Journal of Information Systems 35 (1), 1-8.
[21]. R Pulimamidi, GP Buddha, Applications of Artificial Intelligence Based Technologies in The Healthcare Industry, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4513-4519.
[22]. R Pulimamidi, GP Buddha, AI-Enabled Health Systems: Transforming Personalized Medicine And Wellness, Tuijin Jishu/Journal of Propulsion Technology 44 (3), 4520-4526.
[23]. GP Buddha, SP Kumar, CMR Reddy, Electronic system for authorization and use of cross-linked resource instruments, US Patent App. 17/203,879.
[24]. Nadella, G. S. (2023). Validating the Overall Impact of IS on Educators in U.S. High Schools Using IS-Impact Model – A Quantitative PLS-SEM Approach, DAI-A 85/7(E), Dissertation Abstracts International, Ann Arbor, ISBN 9798381388480, 189, 2023.
[25]. Gonaygunta, Hari, Factors Influencing the Adoption of Machine Learning Algorithms to Detect Cyber Threats in the Banking Industry, DAI-A 85/7(E), Dissertation Abstracts International, Ann Arbor, United States, ISBN 9798381387865, 142, 2023.
[26]. Hari Gonaygunta (2023) Machine Learning Algorithms for Detection of Cyber Threats using Logistic Regression, 10.47893/ijssan.2023.1229.
[27]. Hari Gonaygunta, Pawankumar Sharma, (2021) Role of AI in product management automation and effectiveness, https://doi.org/10.2139/ssrn.4637857.
[28]. Sri Charan Yarlagadda, Role of Artificial Intelligence, Automation, and Machine Learning in Sustainable Plastics Packaging markets: Progress, Trends, and Directions, International Journal on Recent and Innovation Trends in Computing and Communication, Vol:11, Issue 9s, Pages: 818–828, 2023.
[29]. Sri Charan Yarlagadda, The Use of Artificial Intelligence and Machine Learning in Creating a Roadmap Towards a Circular Economy for Plastics, International Journal on Recent and Innovation Trends in Computing and Communication, Vol:11, Issue 9s, Pages: 829-836, 2023.
[30]. B. Nagaraj, A. Kalaivani, S. B. R, S. Akila, H. K. Sachdev, and S. K. N, "The Emerging Role of Artificial intelligence in STEM Higher Education: A Critical review," International Research Journal of Multidisciplinary Technovation, pp. 1–19, Aug. 2023, doi: 10.54392/irjmt2351.
[31]. D. Sivabalaselvamani, K. Nanthini, Bharath Kumar Nagaraj, K. H. Gokul Kannan, K. Hariharan, M. Mallingeshwaran, Healthcare Monitoring and Analysis Using ThingSpeak IoT Platform: Capturing and Analyzing Sensor Data for Enhanced Patient Care, IGI Global eEditorial Discovery, Pages: 25, 2024. DOI: 10.4018/979-8-3693-1694-8.ch008.
[32]. Amol Kulkarni, Amazon Athena Serverless Architecture and Troubleshooting, International Journal of Computer Trends and Technology, Vol, 71, issue, 5, pages 57-61, 2023.
[33]. Amazon Redshift Performance Tuning and Optimization, International Journal of Computer Trends and Technology, vol, 71, issue, 2, pages, 40-44, 2023.