International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Strategies for Monitoring the Cloud for Distributed Denial of Service Attacks

[1]Vimalkumar Rathod, [2]Anil Prajapati, [3]Rinkalben Prajapati, [4]Mayureeben Rathva

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: Cloud computing services are developing in various industries in recent years due to their availability, reliability, and adaptability. As a result, the majority of organizations are trusting this emerging technology for rapid production jobs. However, the transformation of local level computing to remote level computing will lead to numerous security issues for cloud customers and providers, from data security and availability. However, Denial of Service (DoS) and Distributed Denial of Service attacks (DDoS) are considered significant types of damage to the cloud environment that tremendously cripple cloud services and resources. Hence, this novel research work provides four contributions for maximization of performance and cloud services' availability to legitimate users and guaranteeing a quick and primitive attack identification rate. Initially, it contributes to proposing a novel method with the combination of prominent methodologies such as SHA256 and Improved-Kernal Online Anomaly Detection, which are proposed and make use to generate distinctive entries' into the cloud environment to categorize the malicious user and regular users

Keywords: *Distributed Denial of Service, Improved-Kernal, Anomaly Detection, Cloud computing, Blockchain, Software Define Network*

Introduction

The emergence of storage, infrastructure, processing, and other services has led to the widespread acknowledgment of cloud computing among individuals and organisations. It gives clients the ability to create and modify online business applications by remotely accessing software and hardware resources via the Internet. It also provides a centralised collection of resources that are available to clients on a pay-per-use basis. Its widespread usage can be attributed to its enormous capacity for data storage and the upkeep of several services[1][2]. It's also a great way to relieve limited and restricted resources because of the confirmation of the cost-effectiveness and quality of services provided. The foundation of cloud computing is comprised of three service areas. For the end customer, it offers software, platform, and infrastructure services. Resources like as storage and real and virtual computers are accessible at the infrastructure level. To construct PaaS applications, the cloud also provides a runtime environment[3].

Companies have a plethora of fascinating options these days to transition to cloud-based operations. Even more companies have turned to it in the past ten years due to its improved efficiency, scalability, and faster time to market. As part of their digital strategy, it aids in the achievement of long-term objectives. Which cloud model is best for a company will rely on its demands in terms of computing and business, though. From the many cloud service deployment options available, selecting the best one is crucial[4][5]. This would guarantee that the performance, scalability, privacy, security, compliance, and cost-effectiveness that your company needs are met. Finding out which specific problems that various deployment types can tackle is a crucial thing to research and learn about. Which mode—public, private, hybrid, or community is used determines how the cloud is deployed[6]. The selection of the best cloud path for a given organisation is mostly dependent upon cloud integrators. Cloud deployment models like "Minimal investment:" have a number of advantages. This on-demand solution is ideal for industries and other organisations that require rapid access to cloud resources because it has low upfront costs. "Installation of Hardware:" Cloud service providers, or CSPs, are the ones who fund the entire infrastructure. Due to the advantages of scalability, flexibility, and cost-effectiveness, the use of cloud computing services has increased dramatically in recent years across a wide range of businesses. Distributed Denial of Service (DDoS) assaults have emerged as one of the most dangerous dangers as a result of the exponential increase in cloud usage[7][8].Attacks known as denial-of-service (DDoS) present a serious danger to cloud service availability and integrity because they involve a

[1]*Assistant Professor, Information Technology Department, Government Engineering College Modasa*
vimalrathod1982@gmail.com
[2]*Assistant Professor, Information Technology Department, Government Engineering College Modasa*
anil.apit18@gmail.com
[3]*Assistant Professor, Computer Engineering Department, Government Engineering College Modasa*
rinkal.prajapati@gecmodasa.ac.in
[4]*Assistant Professor, Computer Engineering Department, Government Engineering College Modasa*
mayurirathva@gmail.com

coordinated flood of malicious traffic from several sources directed at a target system. Cloud service providers and their clients may suffer large financial losses as well as harm to their reputations from these attacks, which have the potential to overwhelm network infrastructure, deplete computational resources, and impede access to vital apps and data.Suitably designed monitoring solutions for the cloud environment are essential to combating this ever-changing threat scenario[9]. To ensure the uninterrupted functioning of cloud services and lessen the negative effects on users and businesses, proactive detection and mitigation of DDoS assaults are crucial. The goal of this study is to monitor cloud infrastructure and identify and mitigate DDoS attacks as soon as possible using a variety of methodologies and techniques. Organisations can enhance their resistance to distributed denial of service (DDoS) attacks and guarantee the continuous provision of essential cloud services by utilising sophisticated monitoring tools, anomaly detection algorithms, and timely traffic analysis[10][11].

In order to improve the detection and mitigation capabilities, new methodologies are proposed in this study along with a thorough review of the current approaches to cloud monitoring for DDoS assaults, emphasising their advantages and disadvantages. By using case studies and practical evaluations, we hope to offer insightful information about best practices for protecting cloud environments against DDoS attacks, allowing businesses to take full advantage of cloud computing while being protected from malicious activity[12].

Private cloud: Typically, this type of cloud is defined as one that the association can manage and operate. The organisation may have a third party. Third parties can be granted permitted legitimate privileges by the customer in order to enhance it. By limiting cloud customers to only one business, private clouds aim to create a tightly controlled perimeter around themselves. These clouds provide a specific operating environment with all the benefits and capabilities of the cloud, and they were provided by a firm or their assigned services[13].

Public cloud:In a public cloud, the service provider limits the use of the cloud's resources, but any client with an account with the cloud administrator has the potential to use the cloud's services. One or more of these groups academics, businesses, or government agencies may be responsible for the administration, maintenance, and operation of this cloud type. A CSP is the one who gave you access to the public cloud, which may provide you with all the benefits of flexibility and the cloud's accountability model in either a dedicated or imparted work environment[14].

Analysis of security challenges in Cloud Computing

Because the cloud provides its services by making available useful resources, it is important to make good use of these resources in order to prevent security issues from lowering the cloud's performance and dependability. Because of the nature of shared resources in the cloud, it is challenging to design a foolproof method of protecting sensitive information. Many security incidents happened on the cloud in the past. The frequency of cloud disruptions has been on the rise over the last six years, according to a comprehensive assessment by a cloud security alliance[15]. To accomplish multitenancy, cloud computing uses a virtual setting. This idea is a barrier to build a security system that protects the services and data. The cloud provider does not allow its customers to use an intrusion detection system (IDS) or security observer/monitor that extends into the administrative services layer at the back of the virtualized cloud environment due to transparency concerns[16]. Customers of cloud services lose control of their data the moment it is saved in the distant storage space. Customers may not be up-to-date on all the security flaws, vulnerabilities, and malware events just yet. The current mitigation strategies for identifying the different harmful hazards have also advanced. Important aspects of cloud computing security include data availability, secrecy, controllability of access, and security.

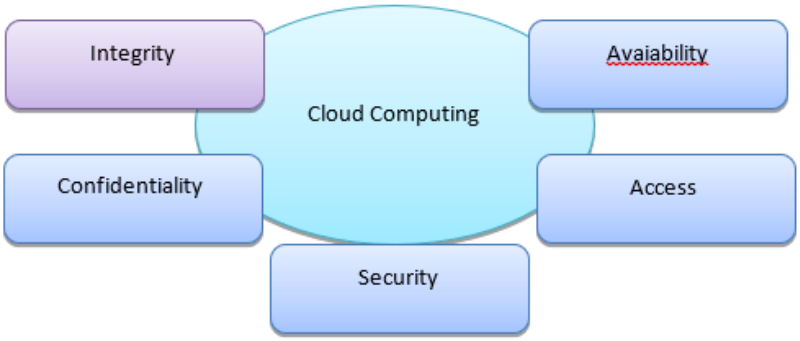

Fig1. Fundamental Elements in Cloud computing

The term "data integrity" refers to the process by which a system guarantees that the data stored there is accurate and unaltered from the original source. Similarly, availability refers to the steps taken to guarantee that resources and data are accessible to applications and end users at all times. Malicious actions also render resources inaccessible. Confidentiality also prevents information from falling into the wrong hands. A data seller may be picky about who has access to his data if access is controllable[17]. The major source of consumer worries surrounding cloud technology is security, which is integral to all of these significant cloud aspects. Both cloud service providers and their customers are potential points of failure when it comes to data security in the cloud. As a result, the importance of data security is growing in relation to the future advancements in cloud computing technology for businesses, industries, and governments[18].

Security challenges in Platform-as-a-Service (PaaS)

Providers of platform as a service (PaaS) let their clients build apps and documents on top of their infrastructure. But the service provider still has the option to implement any security measures below the application level, such NIDS or HIDS. Assuring and supporting efficiently that the information stays unavailable/inaccessible across apps is the provider's responsibility. Platform as a service makes it possible for developers and cloud users to build apps.

Security challenges in Infrastructure-as-a-Service (IaaS)

Internet as a service provides access to virtualized computer resources via the web. The resources it offers are very adaptable and may scale up or down depending on the situation. Because of this situation, IaaS is suitable with any kind of workload. Additionally, the absence of a security flaw in the virtualization administrator gives the client better control over privacy and security with this service. There are a number of real-world security concerns with the virtualized setting.

Impact of DDoS attack on cloud computing

Concerning the security and privacy issues, Denial-of-Service (DoS) attacks and their distributed version Distributed-Denial-of-Service (DDoS) attacks are considered more notorious malicious activities. These malicious activities have the potential to seriously disrupt the availability of cloud services and resources. Because of the attack's inclination to develop in sophistication and ease of deployment, attack mitigation measures have remained a research problem till now. This attack attempts to make the service unavailable to legitimate users by consuming cloud resources even though security professionals have been working tirelessly to address this issue for quite some time, DDoS attacks are becoming more common and have a greater impact as of late. Distinct cloud clients' virtual machines may be hosted on one or another physical host at the cloud facility. This scenario creates the provision of the cloud very weak against such attacks when compared to standalone systems. When a distinct VM is used to insert malicious data, this is the goal. If that VM launches a Denial of Service attack on a physical host, it may lead to problems for other VMs on the same host. DDoS is more powerful than DoS since it is focused on a single source, and the malicious user creates an armed army in the form of bots to attack. A botnet is a network of robots that have been set up.

Types of DDoS attacks Intruders nowadays generate several different forms of DDoS attacks, that can be classified as follows

Volumetric attacks This category of attacks is a common sort of DDoS attack. The attacker can send a stream of packets to a certain server. Because of the restriction on connection routers, authentic users will have a difficult time accessing the server. Bits per second is a unit of measurement for the size of an attack. UDP, ICMP Flood attacks, and spoofed packet massive floods are fall under these categories of attacks

Protocol attacks These attacks deplete the target machine's computational power, memory, and other resources. However, these activities will lead to longer queues. Packets/second are commonly used to measure the severity of protocol difficulties. , Smurf assault, Ping of Death, SYN Flood, and fragmented packet attacks are examples of these attacks.

Application-based attack The primary goal is to collapse the server by flooding a large number of legal queries or messages to the specific server. The application-level attack's severity is measured in requests/second. Zero-day DDoS and Slowloris are two instances of these categories of attacks

Significance of DDoS attack mitigation approaches in cloud computing

The internet has always been vulnerable to distributed denial of service (DDoS) attacks because of its open architecture, and their frequency and size are only growing. Therefore, using effective and comprehensive mitigation methods to prevent such attacks in the cloud is a vital need. To protect a server or organisation against denial-of-service (DoS) and distributed denial-of-service (DDoS) assaults, mitigation is the process of reducing the impact of an impending attack so that it does not cause any more damage or losses. Although distributed denial of service (DDoS) assaults are among the most serious threats, their frequency, intensity, and duration

have all grown in recent years. The OSI model's transport and network layers were once the only targets of distributed denial of service attacks. However, application layers are becoming more and more targeted by modern kinds of DDoS assaults. Because Layer 7 DDoS assaults tend to be low-level and moderate, they are notoriously difficult to detect and counter. DDoS assaults are often undetectable at first glance. In modern times, it is much more difficult for malicious users to impersonate authorised users, making it possible to pass off their traffic as legitimate—this is especially true for application-layer assaults. Most distributed denial of service (DDoS) assaults nowadays begin moderately and won't generate an unanticipated surge, making them difficult to see at first. Because of this, complex distributed denial of service attacks might render the targeted cloud server inoperable, leading to extended outages. As a result, the ability to quickly identify an approaching strike is crucial for evading or reducing its impact. Nevertheless, reaction times for DDoS protection and detection services might vary; significantly, there is a considerable minimum service response time for relief. As a result, a lot of studies focus on learning from DDoS assaults and how to stop them from happening again. Furthermore, more powerful defence is required, which calls for more effective methods of reducing DDoS attacks. The focus of this study is on decentralised security methods that are strong, efficient, and able to withstand DDoS assaults in a virtual setting.

Since the cloud makes use of and expands upon the present IT architecture, applications, and operating system, it is vulnerable to traditional data technology events. Since the cloud computing platform incorporates many new innovations that may lead to new forms of misuse, it faces new security challenges in addition to its old risks. Cloud computing is an example of a shared resource platform that introduces new types of dangers. Of all the assaults, distributed denial of service (DDoS) attacks are the most damaging to cloud service and resource accessibility. Malicious DDoS attacks have been on the rise in recent years. Denial-of-service (DoS) attacks have long been thought of as one of the most enduring security concerns. The danger of this hostile action is still high and grows gradually, despite the fact that several mitigating strategies have been suggested in both academia and business. In order to do this, bad actors usually use Botnets. "Subjecting" host systems, or bots, are directed and controlled by a master, or botmaster, to carry out malicious activities inside the network, resulting in botnets. Recently, these botnets have been wreaking havoc on cloud infrastructures, rendering cloud services unavailable to their rightful owners. A more sophisticated, decentralised, and beautiful approach to cloud security is required to ward against these harmful endeavours.

The new paradigm of cloud computing is accessible to a wide range of consumers. This technology can be easily modified, however it does have a number of security flaws. Despite several security issues, DDoS attacks are quite common and easy to initiate. A hostile person may launch a distributed denial of service attack (DDoS) without specialised technological expertise. The frequency of attacks in the cloud is increased by this theme. By analysing incoming traffic and resource consumption, this study aims to identify DDoS assaults in the cloud environment via the use of strong and decentralised security methods. This study presents four approaches to the problem of distributed denial of service (DDoS) attacks in the cloud. Instead of using different ideas, all the solutions are designed to achieve the same research objective. We use common performance measures like detection time, specificity, accuracy, and sensitivity to evaluate all of the suggested approaches. The results demonstrate that the suggested approaches provide sufficient performance and better outcomes.

Securing Cloud From DDOS Attacks Using Hashbased Techniques And I-KOAD Mechanisms

Cloud computing is the most user-friendly approach for customers to deal with their requirements individually through the internet. To utilize various cloud services, customers need a browser with an internet connection. In recent days the cloud services like Gmail, Hotmail, Yahoo mail, Facebook, Dropbox, etc. are extensively used. In a cloud scenario, VM is a public resource. VMs became very vulnerable to DDoS malicious activities, and their efficiency suffered immensely. As a result, there is a critical necessity to enhance the security measures for detecting and preventing DDoS attacks on virtual machines. The key to such a system is to provide quick and effective identification with a low percentage of false alarms while also assuring that genuine entries are not impacted. This work primarily attempts to answer the following significant questions:

1. How to identify and mitigate DDoS attacks in VMs by using hash-based mechanisms?

2. Are VMs more vulnerable to DDoS attacks? If so, to what extent does their performance damage? To that aim, robust and efficient work based on the hash algorithm SHA256 is proposed and implemented in this study to generate unique hash keys for each user request into virtual machines to recognize intruders.

Mechanism for categorization of DDoS attack flow from the normal flow

To compare the effects on the virtual machine's processing time, performance cost, and accumulated bandwidth under normal and attack conditions, we are

simulating distributed denial of service (DDoS) attacks on an instance of the virtual machine. On demand, or on a pay-per-use basis, cloud services are made available to cloud clients. Virtual computers housed in the cloud react to all client requests for cloud services. The virtual machine's processing time, bandwidth requirements, and overall cost will all rise in the event of a distributed denial of service (DDoS) assault. But in this case, actual users won't be able to have their requests or tasks done since service is denied. As a result of these malicious assaults, the customer is forced to pay more to access the cloud resources and services, which are provided to cloud customers on a pay-per-use basis. When it comes to meeting the demands of its clients, CSP falls short as well. Virtualization technology is therefore present in the vast majority of data centres. Conversely, it is unclear if virtual computers are more susceptible to outside threats. What is the threshold beyond which the virtual machine's performance starts to suffer? To detect, categorise, evaluate, and test the resilience of virtual computers to a common DOS assault, we create a pair of hash-based techniques. Every single virtual computer in the cloud has the suggested DDoS attack detection method installed. Using a hash algorithm like SHA256, this safe method may execute suspicion-based traffic shaping. This method may block all unauthorised access to the virtual machine and let in only authorised traffic.

Network Flow Analysis To Classify DDoS Attacks In Cloud Environment

Over the last few years, cloud technology has gained in popularity and acceptability. Nevertheless, the economic issue is accompanied by the usefulness of this virtual technology. The pay-per-use assessment system is one of the key elements of virtual technology that aids in reducing the financial challenges that cloud service providers face. Furthermore, malevolent users are primarily concerned with cloud clients' economic viability. As a result, such users are capable of affecting cloud-based service access and utilization. DDoS attacks are what they're called. This paper provides a unique technique for detecting and mitigating DDoS attacks on virtual services that are based on traffic analysis on the victim side. Furthermore, feature production, ranking, training, and validation are all included in an intelligent DoS detection system comprising data generation modules. Experiments were performed employing real-time datasets to evaluate the suggested methodology's execution. The findings indicate that our suggested technique accurately detects and mitigates DDoS attacks with low overhead.

DDoS Attack Classification Mechanism

The proposed DDoS traffic flow analysis detection system in a cloud environment is described in the section. Data classification is a critical element of network security. With an appropriate classification of data, the network scheme's privacy and security can precisely separate genuine traffic from illegitimate traffic. Moreover, they can be compelling in securing the system from various malicious attacks. A data classifier works by evaluating individual features of a given data test and arranging them into predefined classes. A quality of a given dataset is characterized as a {future/attribute, Value} tuple, which is illustrative of one variable of the dataset. In this work, we introduced a dependency estimator as a pre-processor. The DE-Cloud (Dependency Estimator) attack detection system involves a packet capturer module responsible for capturing novel incoming traffic in the cloud system. The identified packets are pre-processing to extricate TCP/IP packet header information and statistical data from collecting a sequence of a given network connection. Next, feature generation and selection are performed on the pre-processed data to recognize crucial features for classifier training and produce other features based on factual system data from the last step. The dataset is then automatically considered 'genuine and 'malicious,' based on characterized standards, and the classifiers are trained on the ratio of the whole dataset. Finally, the classifier performance is evaluated with other classifiers based on the classification phase output.

Identification of DDoS activity flow in a cloud environment

The goal of the DDoS malicious activity is to put a cloud environment in financial viability. This vicious approach is not the same as overflowing or greater DDoS attacks in terms of concept. This harmful activity must reduce the amount of entering network threats in the suspicious attack stream to avoid the IDS's terrible loss but can continue the attack for an indefinite period. We have taken into account the following suppositions for the structure and advancement of our proposed approach. It isn't workable for the malicious user order to duplicate genuine customers' behavior deprived of having genuine access to the weblog of the targeted server. An adequate number of attackers over the Internet is accessible to accomplish the malicious activity. In this manner, requests for the attack are sent utilizing the actual IP addresses. Every customer can be treated genuinely except if they are evidenced as attackers. The removal of a viable component of incoming traffic is done for distribution sampling Differentiating the features of arriving real traffic and harmful traffic requires examining both scenarios (illegitimate and legitimate). we conducted several investigations and conducted a few studies on real-world datasets to determine the characteristics that can distinguish between genuine and

malicious network attacks. We came up with the following conclusions based on the testing methods.

a) Contrary to bot circulation, genuine entries are spread over a larger geological area. As a result, real traffic's source Ip spread is more segregated than attack traffic's IPs. As a result, the mean difference (standard deviation) of valid trafficfrom the source IP is greater than the mean difference of attack traffic from thesource IP

b) The packet size of requests and reactions of the cloud customers and servers are noted. Nevertheless, malicious users generally produce similar-sized packets irrespective of the server's reply. In addition, the type of content enabled on the server, as well as the type of content specified by the cloud customer, influences the real packet size transaction between a client and a cloud service. As a result, it is difficult for a criminal user to construct his botnet in such a way that harmful packets have the same packet size distribution as genuine cloud customers. As a result, the distribution of packet size of valid traffic is more scattered than dangerous traffic's packet size distribution. As a result, the usual distribution of genuine packets is greater than that of attack packets

Distributed denial of service (DDoS) assaults aim to overwhelm servers by flooding them with attack packets, which they then process and eventually exhaust their resources. Cloud providers bear the financial burden of processing the malicious messages. The applications running in the leased environment of cloud users are not being monitored by the providers. Therefore, in order to prevent any financial uncertainty, it is the obligation of the cloud customer to monitor and respond to any fraudulent activity in their rented cloud space.

The proposed defence system's goal is to detect distributed denial of service (DDoS) assaults and provide a response strategy to mitigate their effects. There are two parts to our proposed plan of action. There are two time windows in which DDoS attack flows may be detected whenever a client submits a request. During the first stage, there are both attack and normal phases. The first part gets the typical phase browsing settings. (such as the typical packet size, average client request rate per second, average packet length, etc.) of genuine client users in order to compile the legitimate list, as well as the IP addresses of authentic consumers. A customer may have access to services without asking thanks to this valid list. When an assault is underway, the metrics of suspect users are compared to those of typical flow consumers. Based on the comparison of the findings, we generate two types of clients: genuine clients who belong to the entry valid list and blocked/illegitimate users. A list of potential buyers has been compiled. Phase 2 assists in reducing the impact of the fake DDoS assault by making available data from earlier stages.

Conclusion

The threat of Distributed Denial of Service (DDoS) attacks continues to loom large over cloud computing environments, posing significant challenges to the availability, reliability, and security of critical services. Through the exploration of various monitoring strategies and techniques, this research has underscored the importance of proactive measures in detecting and mitigating DDoS attacks to safeguard cloud infrastructures and uphold service continuity.Our examination of existing approaches has revealed the effectiveness of real-time traffic analysis, anomaly detection algorithms, and machine learning-based methodologies in enhancing the detection capabilities and reducing response times to DDoS incidents. By leveraging these advanced monitoring tools and techniques, organizations can bolster their defenses against evolving DDoS threats and mitigate the impact on cloud services and users.

References

[1] Alqarni, A. A. (2022). Majority Vote-Based Ensemble Approach for Distributed Denial of Service Attack Detection in Cloud Computing. Journal of Cyber Security and Mobility, 5(4) pp. 265-278.

[2] Antonelli, F., Cortellessa, V., Gribaudo, M., Pinciroli, R., Trivedi, K.S. and Trubiani, C., (2020). Analytical modeling of performance indices under epistemic uncertainty applied to cloud computing systems. Future Generation Computer Systems, 102(2), pp.746-761.

[3] Argyraki, K.J. and Cheriton, D.R., 2005, April. Active Internet Traffic Filtering: RealTime Response to Denial-of-Service Attacks. In USENIX annual technical conference, general track. 38(3) pp.46-61.

[4] Asosheh, A. and Ramezani, N., 2008. A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. WSEAS Transactions on Computers, 7(4), pp.281-290.

[5] Bawany, N.Z., Shamsi, J.A. and Salah, K., (2017). DDoS attack detection and mitigation using SDN: methods, practices, and solutions. Arabian Journal for Science and Engineering, 42(2), pp.425-441.

[6] Bharot, N., Verma, P., Sharma, S. and Suraparaju, V., 2018. Distributed denial-of-service attack detection and mitigation using feature selection and intensive care request processing unit. Arabian Journal for Science and Engineering, 43(2), pp.959-967.

[7] Bhandari, M., Gutte, V. S., &Mundhe, P. (2022). A Survey Paper on Characteristics and Technique Used for Enhancement of Cloud Computıng and

Their Security Issues. In Pervasive Computing and Social Networking (pp. 217-230). Springer, Singapore.

[8] Bhushan, K. and Gupta, B.B., (2019). Network flow analysis for detection and mitigation of Fraudulent Resource Consumption (FRC) attacks in multimedia cloud computing. Multimedia Tools and Applications, 78(4), pp.4267-4298

[9] Chai, X., Wang, Y., Yan, C., Zhao, Y., Chen, W. and Wang, X., 2020, July. DQMOTAG: Deep Reinforcement Learning-based Moving Target Defense Against DDoS Attacks. In 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC) IEEE 56(8) pp. 375-379.

[10] Chang, V., Kuo, Y.H. and Ramachandran, M., 2016. Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems, 57(2), pp.24-41.

[11] Kautish, S., Reyana, A., &Vidyarthi, A. (2022). SDMTA: Attack Detection and Mitigation Mechanism for DDoS Vulnerabilities in Hybrid Cloud Environment. IEEE Transactions on Industrial Informatics. 4(3) pp.12-19 Khan, M.A., 2016. A survey of security issues for cloud computing. Journal of network and computer applications, 71(3), pp.11-29.

[12] Khan, N. and Al-Yasiri, A., (2016). Identifying cloud security threats to strengthen cloud computing adoption framework. Procedia Computer Science, 94(2), pp.485-490.

[13] Khan, S., Gani, A., Wahab, A.W.A. and Singh, P.K., 2018. Feature selection of denial-ofservice attacks using entropy and granular computing. Arabian Journal for Science and Engineering, 43(2), pp.499-508

[14] Nissim, N., Lahav, O., Cohen, A., Elovici, Y. and Rokach, L., (2019). Volatile memory analysis using the MinHash method for efficient and secured detection of malware in private cloud. Computers & Security, 87(2), p.101590

[15] K. Ingole and D. Padole, "Design Approaches for Internet of Things Based System Model for Agricultural Applications," 2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP), Nagpur, India, 2023, pp. 1-5, doi: 10.1109/ICETET-SIP58143.2023.10151606.

[16] Tariq, M.I., 2019. Agent Based Information Security Framework for Hybrid Cloud Computing. KSII Transactions on Internet & Information Systems, 13(1). pp.14-19

[17] Tavbulatova, Z. K., K. Zhigalov, S. Yu Kuznetsova, and A. M. Patrusova, (2020). "Types of cloud deployment." In Journal of Physics: Conference Series, 1582(1), p. 012085. IOP Publishing.

[18] Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., &Jagtap, S. (2022). A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. International Journal of Intelligent Networks 2(5), pp.20-34