Journal of Theoretical and Applied Information Technology
31st May 2023. Vol.101. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COOPERATIVE TRUST FRAMEWORK BASED ON HY-IDS, FIREWALLS, AND MOBILE AGENTS TO ENHANCE SECURITY IN A CLOUD ENVIRONMENT

HICHAM TOUMI[1], FATIMA ZAHRA FAGROUD[2], KHADIJA ACHTAICH[3], FATIMA LAKRAMI[4], MOHAMED TALEA[5]

[1]Higher School of Technology-Sidi Bennour, Chouaïb Doukkali University, El Jadida, Moroccom.

[2] Faculty of Sciences Ben M'sik, Hassan II University of Casablanca, Casablanca, Morocco.

[4]STIC Laboratory, Chouaib Doukkali University, El-Jadida, Morocco.

[5]Information Processing Laboratory, Faculty of Sciences Ben M'sik, University Hassan II Casablanca, Morocco.

E-mail: [1]toumi.doc@gmail.com, [2]fagroudfatimazahra0512@gmail.com.com, [3]k.achtaich@gmail.com, [4]fatima.lakrami@gmail.com, [5]taleamohamed@yahoo.fr

ABSTRACT

Cloud computing has indeed become a popular method for hosting and delivering internet-based services due to its efficiency and scalability. However, as with any technology, there are inherent security risks associated with it. Organizations must carefully evaluate the security measures provided by their chosen cloud provider and implement additional security measures as needed to protect their data and applications from potential attacks. Security is a crucial concern in cloud computing, and ensuring client satisfaction requires transparency, reliability, and increased security measures. Preventing and mitigating the impact of potential intrusions is a top priority, given the dynamic nature of cloud computing environments. In addition, effective resource protection and recovery must be in place to ensure business continuity without relying on external intervention. addressing the self-healing of cloud security requires the utilization of fundamental aspects of autonomic computing in the cloud. The strong alignment between autonomic computing systems and multi-agent systems allows for the creation of an intelligent cloud architecture that can effectively support autonomic aspects. Therefore, a cooperative Hybrid Intrusion Detection System (Hy-IDS), Mobile Agents, and Firewalls framework have been proposed to counter security attacks in this environment. Our solution offers an extra layer of preventative and protective security measures that not only detects known intrusions but also detects variations of multiple known attacks and previously unknown attacks.

Keywords: *Cloud Computing, Virtualization, Security, Firewalls, IDS*

1. INTRODUCTION

The technology and concept of cloud computing have become increasingly popular as the industry has matured [1, 2]. In addition, more and more service providers are recognizing the significant advantages of using cloud computing for information processing and usage. As a new business service model, cloud computing has developed rapidly. Virtualization is the cornerstone of the cloud computing model, with hypervisors serving as crucial software components responsible for presenting a virtualized view of the hardware to virtual machines and ensuring the successful functioning of the cloud infrastructure. While virtualization technology is a key component of cloud computing, it has also given rise to security concerns as it has become more widely used. In fact, the potential harm caused by security breaches in a virtualized environment is far greater than in traditional stand-alone environments, which has had a serious impact on the development of the cloud computing industry [3, 2]. Protecting the security of virtualization in cloud computing is therefore an essential measure for promoting safe and orderly development in this industry. Recent developments have shown that the virtual infrastructure is particularly vulnerable to targeted attacks, which can compromise the entire computing infrastructure or result in massive information theft of user data. As cloud computing technology continues to grow at a rapid pace, it introduces even more vulnerabilities. Therefore, security is considered one of the most

critical aspects in a cloud computing environment, given the sensitivity of the data being stored [4].

The security of data and intrusion detection in the Cloud are significant concerns due to the presence of various vulnerabilities. The confidentiality, availability, and integrity of cloud resources and services are all impacted. Protecting against various network attacks is the most important security issue in cloud computing. To defend against these attacks, technologies such as message encryption and firewall can be used as a first line of defense [5]. Intrusion detection systems (IDS) are software or hardware systems that automate the procedure of monitoring the events occurring in a computer system or network and examining them for malicious activities. IDS are often deployed in advantageous positions and play a crucial role in safeguarding the network against attacks.

In order to secure critical IT infrastructures, IDS is widely deployed and can monitor user actions, network traffic, configurations, and logs to detect malicious activity. However, most IDS solutions work independently and their detection results cannot be used advantageously. To address this limitation, we propose a new security policy that enables the detection of distributed attacks, such as Denial of Service (DoS), which traditional security solutions like firewalls are unable to detect [2]. Moreover, complex attacks like insider attacks or DDoS attacks cannot be detected by traditional security solutions [6]. Therefore, to effectively mitigate the impact of such attacks, a smart and efficient Hybrid Intrusion Detection System (Hy-IDS) must be integrated into the cloud infrastructure [4],[7,8].

In this paper, we will deepen the development of our framework, which uses a Hybrid Intrusion Detection System (Hy-IDS), firewalls, and mobile agents, our framework can detect and prevent intrusion attempts in a cloud computing environment. The first objective of the framework is to detect intrusion in a virtual environment using mobile agents to collect malicious data. The second objective is to generate new signatures from the malicious data collected in the first phase. Finally, the third objective is to dynamically deploy updates between clusters in cloud computing using the newest signatures previously created. This framework seems to have the potential to effectively detect and prevent intrusion attempts in a cloud computing environment, providing an additional layer of security to protect against attacks.

The rest of this paper is organized as follows: Section II presents the theoretical background that discusses vulnerabilities, threats, and attacks relevant to Cloud. Section III, which forms the core of this paper, explains and describes in detail our approach. The proposed framework is discussed in section IV. Finally, we conclude with perspectives and references in section V.

2. THEORETICAL BACKGROUND AND RELATED WORK

2.1 Cloud Security Issues and Challenges

The security of data and systems in the cloud is a significant concern due to the presence of various vulnerabilities that can be exploited by malicious actors [9] [10]. Some of the major security challenges in the cloud include data breaches, unauthorized access, insecure interfaces and APIs, insider threats, and attacks targeting the underlying infrastructure. In addition, the shared nature of cloud computing means that there is a risk of data leakage or loss, especially if cloud service providers do not implement adequate security measures. Furthermore, compliance with regulatory requirements and data protection laws is a critical issue for cloud users, as they are responsible for ensuring that their data is stored and processed in accordance with legal and ethical guidelines [11] [12].

Cloud computing offers many benefits such as scalability, flexibility, and cost-effectiveness, but it also poses several security challenges. Here are some of the common cloud security issues and challenges [13] [14]:

- Data breaches: One of the most significant security risks in cloud computing is data breaches. If the cloud provider's security is compromised, attackers can gain unauthorized access to sensitive data, including financial records, customer data, and intellectual property.
- Malware attacks: Cloud infrastructure is also susceptible to malware attacks. Attackers can introduce malware into the cloud environment through malicious emails or infected software.
- Insider threats: Insider threats, including both intentional and unintentional threats, can pose a significant risk to cloud security. This can include employees with malicious intent, as well as employees who accidentally expose sensitive data.

- Lack of visibility and control: Cloud computing often involves a shared responsibility model, which means that the cloud provider and the customer share responsibility for security. However, customers may lack visibility and control over the security measures implemented by the cloud provider.
- Compliance and regulatory issues: Companies that handle sensitive data may need to comply with various regulatory requirements, such as HIPAA or GDPR. However, cloud computing can make it challenging to ensure compliance, as data may be stored in multiple locations and jurisdictions.
- Data loss: Data loss can occur due to various reasons, such as hardware failure, software bugs, or accidental deletion. In a cloud environment, data loss can occur due to factors beyond the customer's control, such as a cloud provider's system failure.
- Identity and access management: Cloud environments can involve multiple users and devices, making it challenging to manage identity and access control. Ensuring that only authorized personnel can access data is crucial for cloud security.

To address these challenges, cloud providers and users can adopt a range of security measures, such as encryption, access control, authentication, monitoring and logging, intrusion detection and prevention, and backup and recovery. However, these measures can be complex to implement, and the responsibility for security is often shared between the cloud provider and the user. In addition, emerging technologies such as artificial intelligence and the Internet of Things (IoT) are introducing new security challenges that need to be addressed. Overall, the security of data and systems in the cloud is an ongoing concern, and requires a proactive and multi-layered approach to mitigate risks and ensure the safety and integrity of cloud-based systems [15].

2.2 A cloud-based Intrusion Detection System

A cloud-based IDS (Intrusion Detection System) is a security technology that is provided as a managed service by cloud providers or third-party vendors. It can monitor network traffic and system activity across multiple cloud environments [16].

Cloud-based IDS solutions typically use machine learning and advanced analytics to detect and analyze security events and anomalies in real-time. One of the main benefits of a cloud-based IDS is that it can help simplify security management and reduce costs for organizations with complex cloud environments. They can provide scalability, as they can be easily configured to handle changes in network traffic and infrastructure, and can be deployed quickly and easily across multiple cloud environments. However, it is important to carefully evaluate cloud-based IDS solutions to ensure they meet specific security and compliance requirements. Factors to consider include the types of security events and anomalies that the IDS can detect, the level of customization and integration with other security technologies, and the scalability and performance of the solution [17].

2.3 Security Challenges of SDN and Cloud

Software-defined networking (SDN) can be used to provide security over the cloud in several ways, such as follows:

- Network Segmentation: With SDN, you can segment your network to isolate different types of traffic, such as web traffic, application traffic, and database traffic. This helps to prevent the spread of threats and malware across your network.
- Access Control: SDN can be used to create and enforce access policies for different types of users, devices, and applications. For example, you can use SDN to create a virtual private network (VPN) to securely connect remote users to your cloud infrastructure.
- Network Monitoring: SDN can provide real-time network monitoring and analysis to detect potential security threats. You can use SDN to monitor network traffic and identify any unusual patterns or behaviors that could indicate a security breach.
- Centralized Management: SDN provides centralized management and control of your network, which can help to improve security by ensuring that all devices and applications are up-to-date and configured properly.
- Automated Response: SDN can be used to automate responses to security incidents, such as isolating infected devices or blocking suspicious traffic. This can help to reduce the time it takes to respond to a security incident, minimizing the impact of a potential breach.

Overall, SDN can provide a more agile, flexible, and secure cloud environment by providing centralized management and control, network

segmentation, access control, and automated response.

2.4 Mobile Agent-Based IDS

A mobile agent-based IDS (Intrusion Detection System) is a security solution that uses mobile software agents to monitor and detect security threats in a distributed environment, such as a cloud or a network. Mobile agents are autonomous software programs that can move from one location to another and execute tasks on behalf of the user or system. The mobile agents are deployed to different virtual machines or instances within the cloud or network to collect data and perform analysis locally. A mobile agent-based IDS can reduce network traffic and latency, as data collection and analysis can be performed locally by the mobile agents. Mobile agents can be easily deployed and configured to monitor different types of cloud resources, providing a scalable and flexible solution. Factors to consider include the mobility and communication capabilities of the agents, the security of the agents and the overall system, and the scalability and flexibility of the solution [18] [19].

Overall, a mobile agent-based IDS can be an effective solution for securing a distributed environment [20]. It can detect specific types of security threats or anomalies, resulting in faster detection and response times [21] [22]. The solution provides a more scalable and flexible approach compared to traditional IDS solutions [23].

2.5 Security Threats to Virtualization in Cloud Computing

There are several security threats to virtualization in cloud computing, some of which include [24]:

- Hypervisor vulnerabilities: A hypervisor is a virtual machine monitor that creates and manages virtual machines. If the hypervisor is compromised, it can allow attackers to access and control virtual machines and the data they contain.
- VM escape: This is when an attacker gains unauthorized access to a virtual machine and then breaks out of the virtual environment to access the host system or other virtual machines.
- Data breaches: Virtual machines and their data are vulnerable to data breaches, especially if the virtual machines are not properly secured. Attackers can gain access to sensitive data, such as credit card numbers and personal information.
- Denial-of-service (DoS) attacks: DoS attacks can overwhelm virtual machines or the virtual infrastructure, causing it to become unavailable or slow [25].
- Insider threats: Employees or contractors with access to the virtual environment can intentionally or unintentionally cause damage to the virtual machines or access sensitive data [26].
- Malware attacks: Malware can infect virtual machines, compromising their security and allowing attackers to gain access to the virtual environment [27].

To mitigate these threats, cloud providers and users should implement best practices for virtual machine security, such as regularly patching and updating software, implementing strong authentication and access controls, using encryption to protect sensitive data, and monitoring the virtual environment for unusual activity.

2.6 Firewalling

A firewall is responsible for monitoring and evaluating network traffic both coming in and going out of a network based on predetermined security protocols. The firewall only allows authorized traffic to enter the network, while denying all other traffic that may pose a threat. Firewalls can be deployed as software on individual hosts or as hardware on the network. They use specific criteria, such as the source or destination of packets, protocol, and service to filter traffic, and rely on filtering mechanisms defined by a set of rules to protect a system from flooding attacks [28]. The Virtual Firewall System is a service that provides network traffic filtering for virtual instances, allowing for the inspection of flow packets and the use of pre-defined security policies to prevent unwanted communication resulting from attacks like DoS attacks. Virtual firewalls offer a high degree of flexibility, as they can be easily adapted to the changing policies of virtual networks [29].

2.7 Related Works

In recent years, cloud computing has emerged as a significant topic of discussion in the realm of corporate information technology. Researchers have focused on evaluating the impact of cloud network security on the services offered to users. In [30], the author characterizes the impact of virtual infrastructure on the network performance of Amazon EC2 cloud. They observed instability in throughput and abnormal delays, even when the data center network was underutilized. However, this issue can be mitigated by designing cloud network

Journal of Theoretical and Applied Information Technology
31st May 2023. Vol.101. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

measurements with care, ensuring the use of virtual instances that can fully utilize at least one CPU core [31].

The authors of the study suggest a universal system that can provide support for information-centric Internet of Things (IoT) services, complementing global cloud and Information-Centric Networking (ICN) technologies [31,32]. They developed a multi-layer, content and service-centric approach to managing IoT data. However, the study finds that the system has only loosely integrated techniques from ICN. Nonetheless, this approach enables flexible control over data networking and routing across federated clouds, without affecting the actual physical infrastructure.

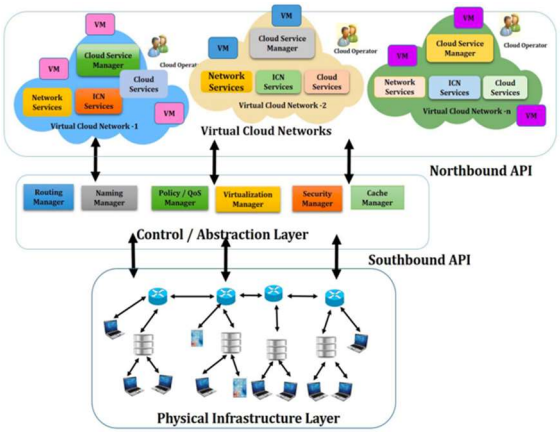

Figure .1. The SDN based Information Centric Cloud Framework

In [31], the author introduces an information-centric cloud framework based on Software Defined Networking (SDN), which can allocate network resources to support elastic cloud applications depending on Service Level Agreement (SLA) requirements. This framework computes paths that ensure both network security and performance. To detect malicious activities within the network infrastructure, the authors use an efficient detection system for malicious switches in the SDN data plan, which can divert data traffic and degrade network performance, as shown in Figure 1 [33]. Additionally, they propose the use of a Trusted Authority for Edge Computing (TA-Edge), which ensures the trustworthiness of edge devices for data forwarding. In this setup, the edge device acts as a certificate authority for a specified trusted domain [33].

Cloud computing, Software-Defined Networking (SDN), and Network Functions Virtualization (NFV) technologies, along with their associated software-defined infrastructures, all utilize virtualization technology to provision virtual resources and offer them as services to users. However, with these new technologies and infrastructures come traditional vulnerabilities, as well as new technology-specific security risks [34].

3. OUR COLLABORATIVE TRUST FRAMEWORK BASED ON HY-IDS, MOBILES AGENTS AND FIREWALLS

In previous works, we introduced an approach that aimed to enhance collaboration among the Hybrid Intrusion Detection System (Hy-IDS), Response Generation Algorithms (RGA), Mobile Agents (MA), and firewalls. After developing attack detection concepts, we shifted our focus to response strategies for attacks and the deployment of response actions in neighboring clusters. In this section, we begin by presenting the objectives of the proposed framework and its overall architecture, which consists of four main layers and functions to address attack responses. We also detail the role of each component within the architecture and how they will react in case of an attack, building upon our previous work [4, 7].

3.1. The Objectives of the collaborative Framework

Our proposed framework has the potential to mitigate the impact of various types of attacks. To accomplish this, the objectives of the framework are organized into five main points as outlined below:

- Intrusion detection: Utilizing an Intrusion Detection System (IDS) and mobile agents to detect and collect malicious data.
- Signature generation: Generating new signatures from the collected malicious data using Signature Generation Algorithm (SGA).
- Dynamic update deployment: Dynamically deploying updates between clusters in Cloud Computing with the latest generated signatures.
- Remote response actions: Dynamically deploying remote response actions using a combination of virtual firewall (VF) and hardware firewall (HF).
- Dynamic response update deployment: Dynamically deploying appropriate response actions between clusters in Cloud Computing with the latest updates.

3.2. Collaborative Framework Architecture

In this section, we propose a logical control architecture to satisfy the structural requirement. Therefore, we could improve the strategy for exchanging sensitive data between and within Cloud Computing clusters, such as detection rules and response actions.

3.2.1 Structuring into domains

In our contribution, the cloud is segmented into domains such as Cloud Computing Administrative Domain (CCAD), Cluster Controllers Domain (CCD), Nodes Controllers Domain (NCD), and Protected Nodes Domain (PND) as shown in Figure 2.

- **Cloud Computing Administrative Domain (CCAD):** our Cloud Computing administrative domain is generally named Front-end Cloud. It is managed by Active Controllers Cloud (ACC). therefore, active controllers are responsible for security management within the cluster control domain. it allows monitoring, detecting, and responding to network attacks.
- **Cluster Controllers Domain (CCD)**: it is an intermediary between the Front-end Cloud and Back-end Cluster. It is presented by the Front-end Cluster and administered by a set of Active Control Nodes (ACNs). therefore, they are responsible for managing security within a cluster control domain. in our contribution, they generate new signatures and global response actions to an attack. in addition, they allow the dynamic deployment of responses to the control node closest to the attacker.

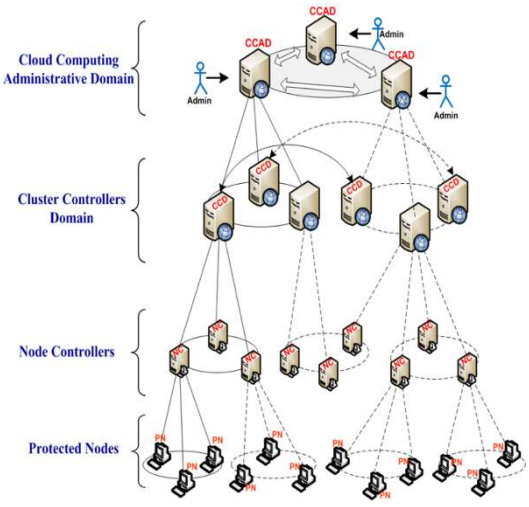

Figure. 2. Cloud Architecture Domain Structure

- **Node Controllers Domain**: It allows the detection of attacks at the server and data center level in a cluster. It hosts virtual machine instances and manages virtual network endpoints. In addition, theoretically, there is no limit to the number of nodes per controller cluster.
- **Domain of Protected Nodes**: it represents any physical or virtual, that will be protected.

3.2.2 Structuring in plans

in order to have compatibility with traditional networks, active nodes such as active control nodes and active administration nodes which will be deployed only in a few specific points of the network. we will manage a network with two main planes: an active plane and a non-active plane (conventional nodes). In our approach, we will detect attacks, respond appropriately to network attacks, dynamically share security rules and manage updates between neighboring clusters in cloud computing. Therefore, we divide each plane into two new planes as shown in Figure 3.

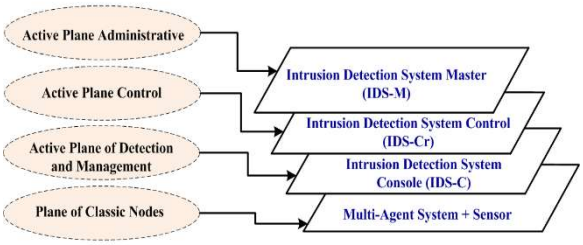

Figure. 3. Cloud Architecture Plans Structure

- **Active Plane Administrative**: it groups the active nodes of administration (IDS-M). The active node of cloud administration is responsible for configuring and administering several active nodes of cluster control. It communicates and cooperates with other administration nodes to have a global view of Cloud Computing and supported services.
- **Active Plane Control**: it groups the Active Nodes of Cluster Control (IDS-Cr). An active node of cluster control is responsible for generating security response actions and deploying them dynamically in the network. These nodes communicate with the administration node.
- **Active Plane of Detection and Management**: it represents physical nodes. The role of the nodes is to host KVM, as well as the hypervisor for the virtual machines that are deployed. It is

used to load and verify the life cycle of instances running on the node.

- **Plane of Classic Nodes**: it represents the virtual machines, operating systems, platform and services presented by Cloud Computing providers.

3.3. Components of our framework

In figure 4, we illustrate our proposed collaborative framework, which utilizes a Hybrid Intrusion Detection System (Hy-IDS), Multi-Agent System, and Firewalls. The Hy-IDS comprises three types of IDS, namely Intrusion Detection System Control (IDS-C), Intrusion Detection System Center (IDS-Cr), and Intrusion Detection System Master (IDS-M), which are strategically implemented in security points throughout the cloud.

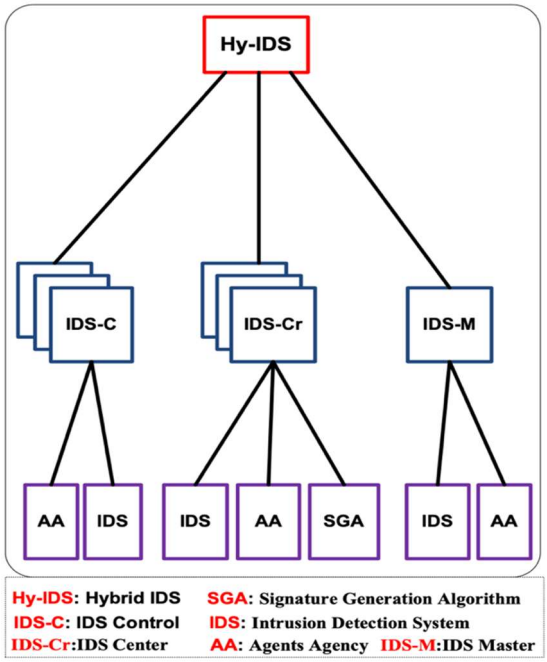

Figure. 4. Components of our Hy-IDS

- **IDS-C**:The proposed framework utilizes the collaboration between IDS and mobile agents, which are implemented in Agents Agency (AA). The IDS components are placed at the node level to monitor the virtual machines, providing an added layer of trust to the VMs. Specifically, the IDS-C runs at the VMM level.

- **IDS-Cr**: To enhance the trust in virtual machines (VMs), our framework employs a collaboration of the Intrusion Detection System (IDS) and the mobile agents in Agents Agency (AA). The IDS component is placed at the node level (physical server) to monitor the VMs, and it is also integrated into the Virtual Machine Monitor (VMM) to provide an additional layer of trust. The IDS-C component is installed in the front-end cluster to monitor the nodes and generate new signatures using the collaboration of the IDS and the Responses Generation Algorithm (RGA) with the multi-agent system.

- **IDS-M**: the IDS-M is placed in the front-end cloud to monitor the cloud and manage response actions. It also facilitates the deployment of updates between neighboring clusters. The IDS-M is based on the collaboration of an Intrusion Detection System (IDS) and the Living Environment of Mobile Agents called Agents Agency (AA). This approach ensures a high level of trust in the virtual machines and allows for effective response action management. Research studies [8] [10] have demonstrated the effectiveness of this approach.

3.4. Proposed framework over cloud computing

In Figure. 5, the Cloud Architecture is divided into a front-end and back-end. The front-end is responsible for connecting external and internal networks and is represented by the Cloud layer.

To manage the cloud, we use a Cloud Controller (CLC) in the Front-End, which provides EC2-compatible interfaces and a web interface to the outside world. The CLC serves as the administrative interface for cloud management and performs high-level resource scheduling. It is important to note that only one CLC can exist per cloud and it handles authentication, accounting, and reporting.

The Back-End of the cloud architecture is responsible for delivering services and processing user queries to access VM instances. It comprises computer hardware and software and is represented in Figure 5 by the Cluster-Layer, Node-Layer, and VM-Layer. The Cluster Controller (CC) acts as the Front-End for a cluster within a cloud computing environment and communicates with the Cloud Controller and Node Controller. The CC is responsible for managing virtual machine instances and Service Level Agreements (SLAs) per cluster. The Node Controller (NC) is located at the physical server level and hosts virtual machine instances, managing the virtual network endpoints.

In the previous section, we presented the components of our Hy-IDS and the proposed cloud model. In Figure 5, we superimposed our Hy-IDS with the cloud computing model. Specifically, IDS-

Journal of Theoretical and Applied Information Technology
31st May 2023. Vol.101. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

C is placed at the level of nodes (physical server) to monitor virtual machines for intrusion detection and malicious data aggregation using mobile agents. IDS-Cr is placed in the front-end Cluster to monitor nodes and generate new signatures. IDS-M is located in the front-end Cloud to monitor clusters and manage updates [7, 8, 10].

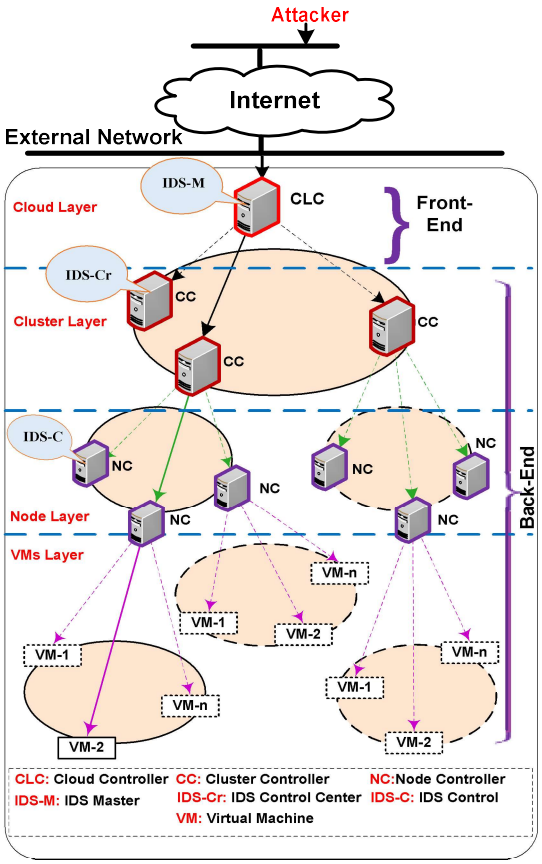

Figure. 5. Our Cloud Computing Architecture

3.5. Analyzing the Functioning of Our Framework over Cloud Computing

3.5.1 Security monitoring and attack detection using IDS-C

To detect an incident, it is essential to have the means to monitor and supervise the infrastructure, both at the level of the network and of the services operated. Monitoring makes it possible in particular to follow the evolution of the consumption of resources, such as network bandwidth, CPU and memory resources, and disk space. Significant variations observed in these resources may indicate an operational problem, and possibly a denial of service. However, an in-depth analysis of network traffic and events is triggered. Currently, there are a lot of protocols that make it possible to obtain information on network exchanges, such as the source or destination IP addresses, the transport protocol used, the source or destination ports, as well as other characteristic elements of the traffic. attack detection consists of analyzing the reports sent by the monitoring systems. After identifying an attack, the detector passes the specification of this attack (Source address, Source port, Type of attack…) to the response generator to generate the appropriate response actions, which will be transmitted on to the deployment manager. Finally, the detector can have the state of the system to be protected and its activity.

In Figure 6, the primary stage of attack detection is carried out within the VMs layer and Node layer. The detection process is built on four key components, namely IDS-Control (IDS-C), Agent Agency, Static Agents Detection (SA), and Investigative Mobile Agents (IMA). The Static Agent (SA) is responsible for detecting any suspicious activity and generating an alert. It records these events in a log file and sends the ID-event (represented as ID-Event in Figure 7) to the Agent Analyzer in IDS-C. The Agent Analyzer utilizes a database for Event-ID analysis, after which it stores the type of attack and IP address in the Victim Host List (VHL).

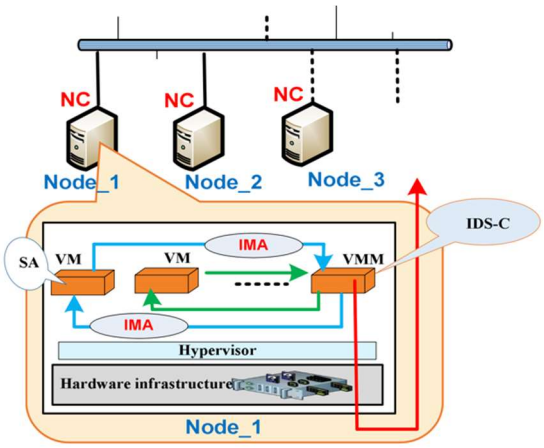

Figure .6. SA And IDS-C Over The Nodes

To describe the type of attack, the system sends a profile to the Agent Generator (AG), which then obtains the IP address of the infected host from VHL. Afterward, the generator agent requests the Mobile Agent Dispatcher (MA-D) to generate Investigation Mobile Agent (IMA). These IMAs are assigned specific tasks and sent to virtual machines (VMs) that sent similar alerts. The IMAs investigate all VMs by collecting attack information from their log files. The collected information is then sent to the Alerting Agent for advanced analysis, as illustrated in Figure 7. VMs that are eventually discovered to be compromised will be blacklisted in their cluster. Then, IDS-C changes the trust level of infected

Journal of Theoretical and Applied Information Technology
31st May 2023. Vol.101. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

machines to limit their communication with normal machines. thus, when a new VM appears in the blacklist, the administrator takes the necessary measures. These measures are very different from actions against the infection of physical machines. Virtual machines can be easily cloned and moved between physical servers, which makes them dynamic but also increases the speed at which vulnerabilities can spread. In the event of an attack, the IDS-C aggregates malicious data and stores them in a temporary database. Subsequently, the IDS-C generates Transfer Mobile Agents (TMA) to notify the IDS-Cr units located in the cluster layer.

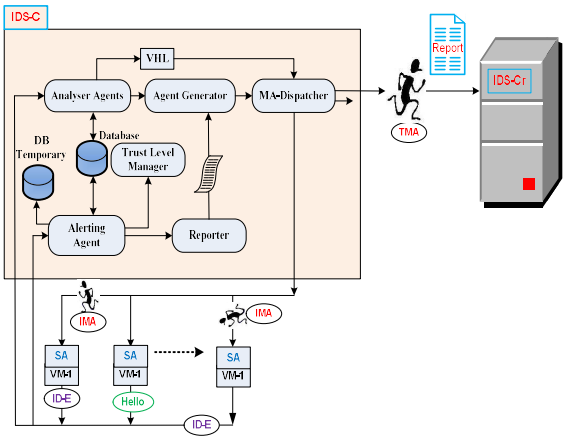

Figure. 7. Attack Detection Using Mobile Agents And IDS-C

3.5.2 Generation of response actions using IDS-Cr

When treating an attack, it is important to note that some attackers seem to use denial of service as a diversion: a DDoS attack can seek to cover an intrusion attempt or a data extraction. therefore, It is necessary to ensure that the information system is not the target of another attack and to carry out global control of the entity's information system once the attack is over.

The Intrusion Detection System Center (IDS-Cr) is part of our Hy-IDS Framework. It is placed at the Front-End Cluster and mainly consists of three components namely, Signature Generation Algorithm (SGA), Agent Agency (agent runtime environment) and NIDS. In our framework, the Intrusion Detection System Center (IDS-Cr) is used to analyze attack specifications and generate appropriate response actions. Therefore, the detection of network intrusions and the generation of new signatures ("response actions") are ensured by the combination of NIDS with the Signature Generation Algorithm as shown in Figure 8.

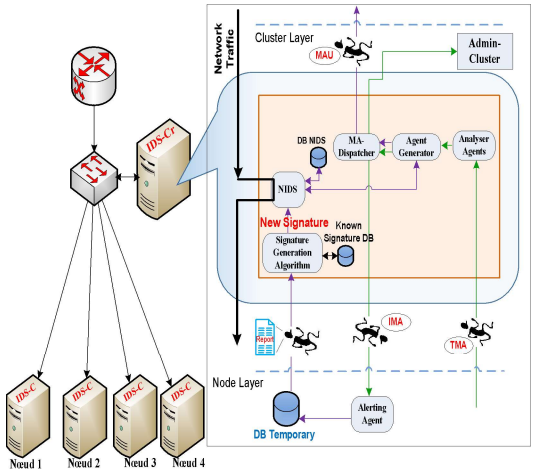

Figure .8. Generation Of Response Actions

The production of these actions is done in two phases, Figure 9: the first phase consists of producing an initial response applied locally by IDS-C to protect the virtual machines (IDS-C placed at the level of Virtual Machine Manager (VMM)). The second phase consists of producing a global and optimal response to the attack. It contains network response actions that must be deployed and applied in the network. However, the global response actions generated by the IDS-Cr are executed at the Front-End cloud level using the IDS-M if it is an external attack. Finally, the IDS-M sends them to the IDS-Cr and IDS-C of neighboring clusters. then, these response actions will be executed in the protection element closest to the attacker.

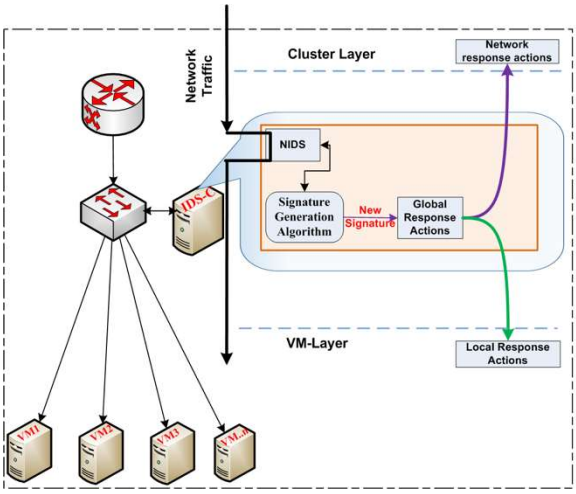

Figure .9. different types of response actions

3.5.3 Dynamic deployment of response actions

In Figure 10, the deployment of the response actions is presented by a complex process which includes a set of activities. it is launched at the end

Journal of Theoretical and Applied Information Technology
31st May 2023. Vol.101. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of the intrusion detection management process and response action generation.

- The provision: This activity is also called the broadcast of global response actions, it is the interface between the generation process and the deployment process.
- Installing the software: An activity that allows the rules to be inserted (response action) in the deployment target sites. It is considered the most complex and important activity in the deployment life cycle.

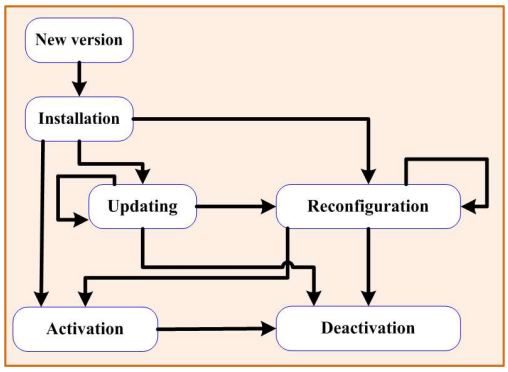

Figure .10. Process Of Dynamic Deployment Of Response Actions

- Activation: This activity allowed the execution of the new rules recently added. It can be reduced to simply invoking a method in its simplest form. On the other hand, in its most complex form, it may be necessary to activate elements of the target environment such as software or server dependencies before the new rule can be activated.
- Deactivation: An activity typically used before an update, uninstall, or reconfigure activity. It consists of interrupting the execution of a response action that has already been deployed.
- Updating: an activity that consists of modifying an already installed rule, for example by installing a new version. The update can be static or dynamic.
- Reconfiguration: this activity makes it possible to modify a rule already installed by selecting a different configuration (not similar) to the existing configuration. It can be, for example, the addition or deletion of a new IP or simply the change of configuration parameters (access allowed or denied).

The IDS-Cr allows the generation of local and global response actions, Figure 11. The first is deployed and executed locally by the IDS-C. Global response actions are deployed and executed by the IDS-M in order to deploy them to neighboring clusters.

A. Management of Local Response Actions

Locally, the IDS-C receives the response actions generated by the IDS-Cr, which will be deployed and executed in the virtual cloud environment. The virtual firewall is a network security system, which controls the incoming and outgoing network traffic based on a set of rules, as shown in Figure 11.

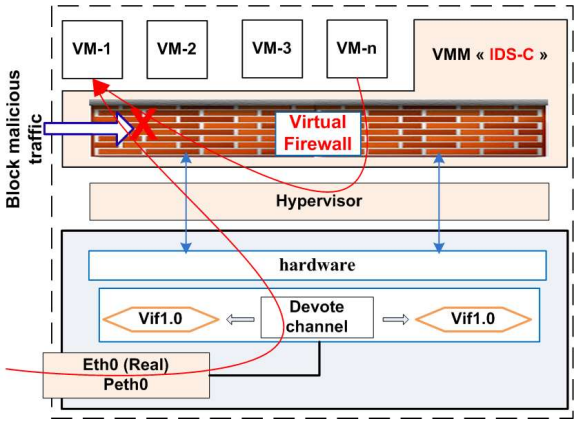

Figure .11. Virtual Firewall To Execute Response Actions

Although firewalls can be utilized to regulate access between virtual machines and the Internet, it can be challenging to secure and monitor virtual traffic between two virtual machines that never leaves the physical host hardware. Traditional physical firewalls are ineffective in such scenarios. Finally, local response actions are deployed and executed at the virtual firewall. it makes it possible to block and limit malicious traffic, which comes either from the outside or from a neighboring virtual machine.

B. Management of Global Response Actions

whether the attack is launched from an external network or from a neighboring cluster, the IDS-Master deals with the deployment and execution of active response services corresponding to global response actions. However, for externally initiated attacks, the IDS-Master executes the response actions in the Front-End Cloud, otherwise, it deploys the response actions to the DS-Cr or IDS-C closest to the attack source. Finally, the dynamic deployment process of response actions from an IDS-M to an IDS-Cr or IDS-C, is presented as follows:

- firstly, source IDS-M sends active packets to target IDSC-Cr/IDS-C, with information indicating the identification of response actions to be performed.
- When an active packet arrives at the target active node (IDS-Cr or IDS-C). Based on a thorough analysis, if the response action is available locally, the service execution process starts. Otherwise, the controller requests a response action download from the active source control node (IDS-M).
- When IDS-M receives the response action download request, it loads the code and sends it to the active target control node (IDS-Cr or IDS-C).
- Once the active code is downloaded to the target active node (IDS-Cr or IDS-C), the execution process starts.

3.5.4 dynamic update management between different cloud clusters.

As shown in Figure 12, if a new attack is detected in a cluster, the IDS-Cr generates new signatures to protect neighboring nodes and clusters. Subsequently, the IDS-M retrieves the new signature using a Mobile Agent Update (MAU) to update its database (DBM) and deploy its own MAUs to update its clusters (except for the one that reported the new signature).

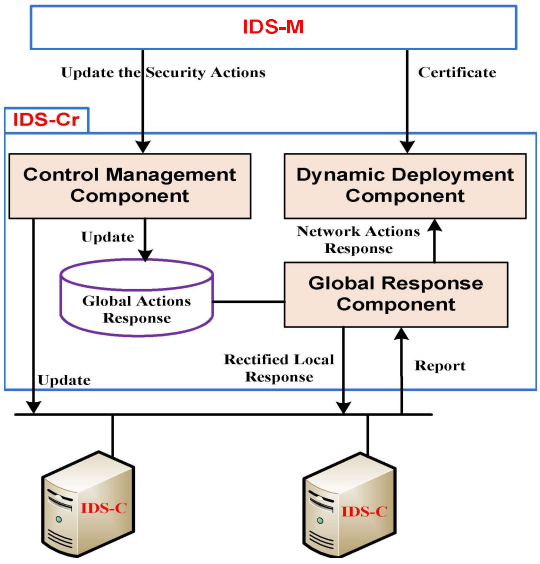

Figure .12. Dynamic Update Management

3.6. Global collaborative framework to improve security in the cloud

In this work, we propose a flexible security architecture against network attacks. This architecture is based on mobile agents and aims to achieve two main objectives:

- detect and respond to network attacks: The responses are executed in two phases: respond locally by taking the initial countermeasures then respond in the network by pushing the global countermeasures very close to the source of the attack.
- dynamically update and distribute security information regarding attacks (detection and response rules).

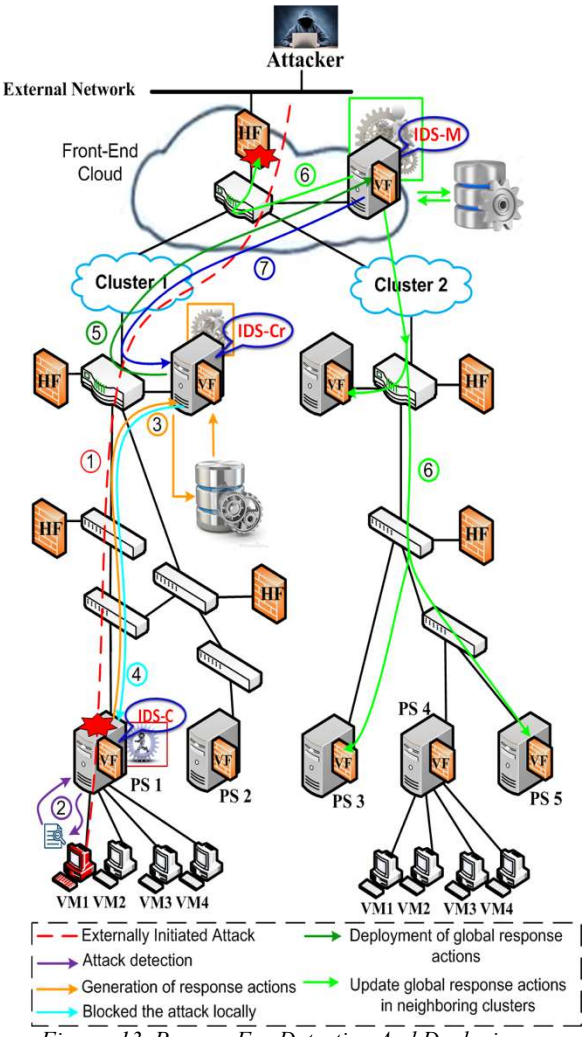

Figure .13. Process For Detecting And Deploying Response Actions

Our framework is based on mobile agents in order to make security responses automatic and dynamic. the execution of countermeasures is pushed closer to the source of the attack where they can produce better results as illustrated in Figure 13. Stopping attacks close to their sources is one of the main objectives of our proposal. however, pushing

responses to the source of the attack allowed us to avoid congestion and minimize legitimate request damage. stopping attacks close to their sources is one of the main objectives of our proposal. however, pushing responses to the source of the attack allowed us to avoid congestion and minimize legitimate request damage.

As shown in Figure 13, in order to present the operating principle of our framework, we start our scenario by initiating an attack from an external network (step 1). However, for the detection of this attack, the IDS-C performs advanced analyzes of the targeted machine (step 2). Then, the IDS-C generates the descriptive report which contains the specification of the detected attack (Source address, Source port, Destination address, Destination port, Start date of attack, Type of attack, etc.). This report is sent to the nearest central control node (Intrusion Detection System Center (IDS-Cr)). using this descriptive report, the active control node generates the attack response, which consists of two parts (step 3).

The first part represents the initial actions and countermeasures taken locally at the IDS-C node (step 4). The second part represents the global response actions that are exploited by Intrusion Detection System Master (IDS-M), step 5. However, these response actions will be deployed dynamically using mobile agents, very close to the attack source, in the active control node closest to the attacker. Therefore, in the event of an external attack, it will be blocked by a physical firewall placed at the Front-end Cloud. In the event of an internal attack, it will be blocked either by Physical Firewall (PF) or Virtual Firewall (VF) of its cluster (step 6). After applying the remote response actions, the IDS-M sends notifications to the IDS-Cr and the IDS-C to deactivate the local response actions.

4. DISCUSSION

Cloud computing is a constantly developing concept that combines numerous existing technologies and computing approaches to create something new. However, the transformative nature of the cloud is also linked to significant security and privacy risks. Intrusion detection and other malicious activities at the network level are significant security issues in the Cloud. Nevertheless, traditional security techniques like firewalls, host-based antivirus software, and intrusion detection systems do not provide adequate security in virtualized systems due to the rapid spread of threats via virtualized environments. Therefore, to ensure a high level of trust in cloud computing, we propose a new framework that utilizes a cooperative approach of Hy-IDS and mobile agents in combination with physical and virtual firewalls. This new architecture is aligned with the organization's objectives and able to support "business" processes. Indeed, the presentation of the functional architecture leads in particular to highlight the information repositories, to locate the "business services" in the architecture and to identify the interfaces between functional subsets. Our architecture based on mobile agents includes the following functionalities.

- Observation of the system activity to be protected (collection and presentation of network traffic activity in the form of observations that are used to identify an attack).
- Detection of attacks based on the observations.
- Generation of appropriate response actions (local and remote).
- Dynamic deployment of remote response actions.
- Dynamic updating of security features (detection rules and response rules).

These features represent the functional behavior of our architecture. They describe two processes: the first process represents the attack detection cycle, the generation of response actions and the deployment of these response actions. The second process presents the management of the update of the security functions (detection rules and response rules).

Using mobile agents allowed us to adopt a scalable framework. Indeed, a scalable framework can cope with hypergrowth without having to significantly increase spending on recruitment, hardware and IT resources. adaptation to growing infrastructures is better controlled by our framework. it is able to detect intrusions in VMs, even in case of migration, using mobile agents. Favored by investors and cloud providers, attracted by optimal profitability and the prospect of achieving economies of scale. Therefore, this is the strength of our framework, which gives the Firewalls, IDS and NIDS great scalability and flexibility. Therefore, we have met almost all the mentioned challenges in our framework.

5. CONCLUSIONS AND FUTURE WORKS

Cloud computing is a technology that allows customers and service providers to benefit from unlimited processing capacities, with very

competitive usage and deployment costs. However, this paradigm also brings many new challenges for data security and access control. There is a massive need to bring Security, Transparency and Reliability in the Cloud model. However, with the aim of proposing a framework that offers a more flexible solution to the problem of cloud computing security management, we have designed a model for detecting and responding to attacks based on mobile agents. Hence, one of the questions being asked during this research is how to reduce the impact of any type of intrusion in the cloud environment. To overcome these kinds of attacks, we proposed a collaborative framework based on the Hybrid Intrusion Detection System (Hy-IDS), Firewalls and Mobile Agents. As mentioned previously, mobile agents are used to investigate virtual machines, to transfer malicious data, and deploy update between different clusters in cloud. Our contribution has three primary objectives. The first objective is to detect intrusions in virtual environments using mobile agents that collect and transfer malicious data. The second objective is to generate new signatures from this data. The third objective is to dynamically deploy updates between clusters in cloud computing by utilizing the latest response actions. Further research can be undertaken to improve the work presented.

The immediate extension of this work would be the definition of a contract management policy in order to integrate it into the final selection process. As a future directive, we plan to integrate software-defined networking (SDN) in our framework in order to improving agility, increasing performance and optimizing costs. SDN offers a wide choice of automation and programmability functions for data centers, clusters, LANs and WANs. Therefore, the implementation of SDN in our solution permit to add more advantages to our framework.

however, provision, manage and program faster our networks using SDN technology. In this centralized network management approach, the underlying network infrastructure is completely decoupled from the applications. In the next work, we aim to automate the dynamic deployment of response actions and security feature updates using SDN. Finally, remember that the issues of trust and security in an open and heterogeneous environment such as cloud computing still remain open issues, so many avenues remain to be explored.

REFERENCES:

[1] Sharma, S., Soni, S., Sengar, S., (2012) Security in cloud computing National Conf. on Security Issues in Network Technologies, 1-6.

[2] Chen, Lei, et al. "Research on virtualization security in cloud computing." IOP conference series: materials science and engineering. Vol. 806. No. 1. IOP Publishing, 2020.

[3] Sen, J., (2013) Security and privacy issues in cloud computing Retrieved from arxiv.org/pdf/1303.4814.

[4] Lata, S., & Singh, D. (2022). Intrusion detection system in cloud environment: Literature survey & future research directions. International Journal of Information Management Data Insights, 2(2), 100134.

[5] Albalawi, A. M., & Almaiah, M. A. (2022). Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. J. Theor. Appl. Inf. Technol, 100, 2988-3011.

[6] Sohal, Amandeep Singh, et al. "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments." Computers & Security 74 (2018): 340-354.

[7] Toumi, Hicham, et al. "Implementing Hy-IDS, mobiles agents and virtual firewall to enhance the security in IaaS Cloud." Procedia Computer Science 160 (2019): 819-824.

[8] Toumi, Hicham, et al. "Use trust management framework to achieve effective security mechanisms in cloud environment." (2017).

[9] ALOUFFI, Bader, HASNAIN, Muhammad, ALHARBI, Abdullah, et al. A systematic literature review on cloud computing security: threats and mitigation strategies. IEEE Access, 2021, vol. 9, p. 57792-57807.

[10] TOUMI, Hicham, TALEA, Amal, MARZAK, Bouchra, et al. Cooperative trust framework for cloud computing based on mobile agents. International Journal of Communication Networks and Information Security, 2015, vol. 7, no 2, p. 106.

[11] Almorsy, Mohemed, John Grundy, and Amani S. Ibrahim. "Collaboration-based cloud computing security management framework." 2011 IEEE 4th International Conference on Cloud Computing. IEEE, 2011.

[12] Imran, Faisal, Yin Yunfei, and Mohammad Ikram. "CLOUD COMPUTING SECURITY ISSUES AND THREATS IN BUSINESS ENVIRONMENT." GSJ 7.7 (2019).

[13] Zenker, Eric, and Maryam Shahpasand. "A review of testing cloud security." International Journal of Internet Technology and Secured Transactions 8.3 (2018): 374-397.

[14] HYUN, Sangwon, KIM, Jinyong, KIM, Hyoungshick, et al. Interface to network security functions for cloud-based security services. IEEE Communications Magazine, 2018, vol. 56, no 1.

[15] E. Messmer, "Gartner: Cloud-Based Security as a Service Set to Take Off," Network World, Oct. 2013; https://www. networkworld.com/article/2171424/data-breach/gart- ner--cloud-based-security-as-a-service-set-to-take-off.html, accessed Oct. 14, 2017.

[16]Aldwairi, M., Mardini, W., & Alhowaide, A. (2018). Anomaly payload signature generation system based on efficient tokenization methodology. International Journal on Communications Antenna and Propagation (IRECAP), 8(5).

[17] Shurman, M. M., Al-Jarrah, O. M., Esoh, S. B., & Alnabelsi, S. H. (2017). An Enhanced Cross-Layer Approach Based on Fuzzy-Logic for Securing Wireless Ad-Hoc Networks from Black Hole Attacks.

[18] Sharma, Pinki, Jyotsna Sengupta, and P. K. Suri. "Survey of intrusion detection techniques and architectures in cloud computing." International Journal of High Performance Computing and Networking 13.2 (2019): 184-198.

[19] Okikiola, Folasade Mercy, et al. "A new framework for detecting insider attacks in cloud-based E-Health care system." 2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS). IEEE, 2020.

[20] Meng, Weizhi, et al. "Detecting insider attacks in medical cyber–physical networks based on behavioral profiling." Future Generation Computer Systems 108 (2020): 1258-1266.

[21] Narayana, K. E., and K. Jayashree. "Survey on cross virtual machine side channel attack detection and properties of cloud computing as sustainable material." Materials Today: Proceedings 45 (2021): 6465-6470.

[22] Mahipal, S., and V. Ceronmani Sharmila. "Virtual machine security problems and countermeasures for improving quality of service in cloud computing." 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS). IEEE, 2021.

[23] Imrana, Yakubu, et al. "A bidirectional LSTM deep learning approach for intrusion detection." Expert Systems with Applications 185 (2021).

[24] Kilincer, Ilhan Firat, Fatih Ertam, and Abdulkadir Sengur. "Machine learning methods for cyber security intrusion detection: Datasets and comparative study." Computer Networks 188 (2021): 107840.

[25] Seyedi, B., & Fotohi, R. (2020). NIASHPT: a novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. The Journal of Supercomputing, 76(9), 6917-6940.

[26] De la Prieta, F., Rodríguez-González, S., Chamoso, P., Corchado, J. M., & Bajo, J. (2019). Survey of agent-based cloud computing applications. Future generation computer systems, 100, 223-236.

[27] Uddin, M., Memon, J., Alsaqour, R., Shah, A., & Rozan, M. Z. A. (2015). Mobile agent based multi-layer security framework for cloud data centers. Indian Journal of Science and Technology, 8(12), 1.

[28] Alabady, S. A., Al-Turjman, F., & Din, S. (2020). A novel security model for cooperative virtual networks in the IoT era. International Journal of Parallel Programming, 48(2), 280-295.

[29] Mishra, P., Biswal, A., Garg, S., Lu, R., Tiwary, M., & Puthal, D. (2020). Software defined internet of things security: properties, state of the art, and future research. IEEE Wireless Communications, 27(3), 10-16.

[30] G. Wang and T. S. E. Ng, "The impact of virtualization on network per- formance of amazon ec2 data center," in Proceedings of the INFOCOM, (Piscataway, NJ, USA), IEEE Press, 2010.

[31] Ghosh, U., Chatterjee, P., Tosh, D., Shetty, S., Xiong, K., & Kamhoua, C. (2017, June). An SDN based framework for guaranteeing security and performance in information-centric cloud networks. In 2017 IEEE 10th International Conference on Cloud Computing (CLOUD) (pp. 749-752). IEEE.

[32] E. Borgia, R. Bruno, M. Conti, D. Mascitti, and A. Passarella, "Mobile edge clouds for information-centric iot services," in ISCC, IEEE, 2016.

[33] Qureshi, K. N., Jeon, G., & Piccialli, F. (2021). Anomaly detection and trust authority in artificial intelligence and cloud computing. Computer Networks, 184, 107647.

[34] Farahmandian, S., & Hoang, D. B. (2016, December). Security for software-defined (cloud, SDN and NFV) infrastructures–issues and challenges. In Eight international conference on network and communications security.