RESEARCH & INNOVATION DIVISION
IJIST

Artificial Intelligence-Augmented Intrusion Detection Systems for Advanced Threat Taxonomy in Cloud Computing Environments

Farhan Nisar[1] Arshad Farhad[2], Baseer Ali Rehman[3], Shum Yee Chan[4,] Muhammad Nauman Khan[5], Muhammad Touseef Irshad [6]

[1] Department of Physical and Numerical Sciences, Qurtaba University, Peshawar
[2]Department of Computer Science, Bahria University, E-8 Islamabad
[3]Department of Applied Social Sciences, University of Peshawar
[4]Department of Applied Social Sciences, Hong Kong Polytechnic University
[5]Department of Computer Science, Agriculture University, Peshawar
[6] Department of Computer Science, National University of Modern Languages, Peshawar

***Correspondence**: farhansnisar@yahoo.com, arshadfarhad.buic@bahria.edu.pk, baseerali0007@gmail.com, csyeecoding@gmail.com,nauman.marwat94@gmail.com, touseef.irshad@numl.edu.pk

Citation: Nisar. F, Farhad. A, Rehman. B. A, Chan. S. Y, Khan. M. N, Irshad. T. M. "Artificial Intelligence-Augmented Intrusion Detection Systems for Advanced Threat Taxonomy in Cloud Computing Environments" IJIST, Vol. 07, Issue. 04 pp 2263-2278, October 2025

Received| August 22, 2025 **Revised|** September 29, 2025 **Accepted|** October 01, 2025 **Published|** October 03, 2025.

Over the past few decades, cyber-attacks have emerged as a grave form of criminal activity and a subject of intense scholarly and policy debate. The rapid proliferation of cloud computing services— particularly Software as a Service (SaaS)—has further motivated research to classify security threats and their corresponding countermeasures. Scholars have increasingly focused on the risks, vulnerabilities, and malicious intrusions inherent in such environments, with particular emphasis on *MITM (MITM) attacks* and their mitigation and detection mechanisms. Host-based virtual software has demonstrated considerable efficacy in detecting malware within localized environments. Building on this foundation, the present study classifies Man-in-the-Middle (MITM) attacks in SaaS platforms through the deployment of Cloud-based Intrusion Detection Systems (CIDS). Our investigation concentrates specifically on attacks that target cloud hosts deployed within SaaS infrastructures. The proposed methodology incorporates the roles of the source cloud, destination cloud, and directional flow of the attack vector. In this context, the cloud ecosystem is understood as a dynamic environment where any participating entity, equipped with sufficient technical expertise, may both launch and be subjected to sophisticated intrusions. Accordingly, adaptive CIDS monitoring architectures are essential to safeguard communication between cloud actors. Moreover, CIDS frameworks furnish modular components capable of aggregating alerts, conducting analysis, and notifying administrators of potential breaches. To further illustrate the threat landscape, we present a statistical analysis of vulnerabilities most frequently exploited in MITM scenarios. This classification not only highlights the evolving tactics of adversaries but also equips readers with a structured understanding of MITM attacks, thereby fostering greater familiarity with contemporary cloud security challenges.

Keywords: SaaS, Malware, CIDS, Classification

Introduction:

Service-oriented web application is the key enabler for such a computing infrastructure. The SaaS providers reduce the resources and maintenance costs by sharing servers and their applications with their clients. A Man-in-the-Middle (MITM) attack is a security breach in which an adversary covertly intercepts and manipulates communication between two legitimate parties. This type of attack compromises the confidentiality, integrity, and authenticity of transmitted data. In subsequent sections of this paper, references to MITM attacks are made with respect to this definition to ensure consistency and avoid redundancy. Besides, software-based applications are the techniques that allow for the inspection of CIDS from outside the client Operating system and analysis of the running application inside it. Thus, the fundamental challenge is to protect her data and identify malicious users in SaaS. The isolation ensures both higher integrity of the diagnosis and encourages practitioners to bring Cloud-based IDS to a SaaS cloud provider [1].

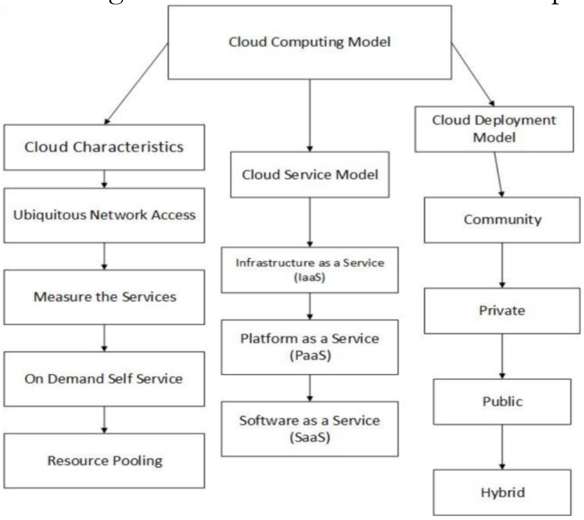

Figure 1. Cloud Computing Models

Objectives of the Study:

To classify MITM (MitM) attacks in the SaaS cloud by examining their origins among different actors within the SaaS environment.

To provide an overview of how MitM attacks enable one actor to potentially harm other entities in the SaaS ecosystem.

To highlight the absence of automatic detection solutions for these attacks, especially those arising from network security issues, such as deficient patching and a lack of monitoring.

To emphasize the need for knowledge of existing attacks to design software-oriented Cloud Intrusion Detection Systems (CIDS) that effectively address such threats.

To focus specifically on MitM attacks that directly target SaaS architectures, thereby laying the foundation for improved analysis, monitoring, and detection mechanisms.

The framework gives SaaS providers an authentic approach to detect malicious users where multiple user simultaneously accesses a single database. We presented our classification method in the "Threat model in SaaS" section and details of each class in "Attacks outside on SaaS cloud"," SaaS as target of attacks", and "SaaS architecture as attack source" sections. The evaluation section presents the identified focus of related work. The "Conclusion" section presents our summary work.

Relevant Work:

SaaS is multi-tenant when several tenants share one or more application database instances and lease a specific domain and pay for the product services (i.e., professional or enterprise) and the number of user accounts. Arshad et al [2] include different discussions from IT experts on the most substantial threats in the IT industrial sectors and from academic researchers. In the business sector, SaaS is implemented on the presentation layer, where web pages request HTTP for the application, and the business layer manages different business rules and helps communication between the presentation and data access layers.

Nisar et al [3] discuss service delivery models as Infrastructure as a Service IaaS, Platform as a Service PaaS, and Software as a Service SaaS and the deployment Models (Public, Private, Hybrid, Community, Virtual private cloud).

Baseer et al [4] discuss the survey of security issues in SaaS cloud. The author presents a comparison between the IT and business sectors on how the business sector deals with SaaS cloud, and researchers consider solutions for the SaaS network and software resources. The author classifies two different attacks identified: threats from clients and threats from malicious cloud service providers.

Modi et al [5] outline different IDS proposed that detect attacks among Virtual machines in the IaaS layer. The threats discuss the confidentiality and availability of cloud resources, with their effects and mitigation solutions. Finally, they discuss the different levels in cloud infrastructure in cloud models.

Naveed et al [1] identify different security issues arising in cloud environments and categorize in into five groups: i.e., security standards, network, access control, data, and cloud infrastructure. Nine known attack groups have been defined, such as Denial of Service, Cross-VM side channel, and Cloud malware injection. The countermeasures have been discussed and evaluated with limited factors. Additionally, the authors provide an overview of previous research in the field of Cloud Network Security.

Their classification considers [6] security properties, availability, authenticity, and privacy. The author also discusses the security assurance for embracing a methodology for collecting evidence that supports the security properties. They discussed security assurance techniques in survey publications and have been tested, monitoring certification, compliance, and different service level agreements. The disadvantage of the said system is that when the host system is tampered with, like a rootkit, it is not reliable to return the right diagnosis.

The IDS analyzes [7] machine states and events through SaaS Virtual Machine monitoring, by which it can isolate, interpose, and inspect properties of VMM. Beak et al. have developed a SaaS cloud environment bringing SaaS VM functionality for the cloud users. Cloud VM is wrapping the Remote Procedure Calls of the inspection library LibVMI.

The literature on cloud security highlights multiple forms of cyberattacks, which can be systematically classified into distinct taxonomies. To enhance clarity, the discussion is organized into subsections that address common attack categories: Man-in-the-Middle (MITM), SQL Injection (SQLi), Denial of Service (DoS), Privilege Escalation, and Spoofing. Each subsection presents a concise definition, significant prior studies, and open research gaps. A comparative summary table is provided at the end of the section to synthesize key findings.

The CIDS [8] helps to protect the components from different threats and can control a task in the SaaS VM that can modify the CIDs component. It collects events and audits from VMs so that be correlator and detector components can analyze them. CIDs can detect masqueraders that access the SaaS from different hosts in clouds and network-based attacks by which they could threaten other actors of clouds, and an adequate CIDs-based detection mechanism.

Threat Model:

We n SaaS cloud environments, multiple actors interact across a shared infrastructure, which increases the potential attack surface.[9] A threat model defines who the attackers are, what resources they target, and how they exploit vulnerabilities. In the context of MITM (MitM) attacks, the following elements are considered:

Actors (Potential Adversaries):
Malicious insiders within the cloud provider.
Compromised users or tenants sharing the SaaS environment.
External attackers exploit weak or unpatched network protocols.

Assets at Risk:
Confidential data in transit between clients and servers.
Authentication tokens, credentials, and session keys.
Inter-service communications within the SaaS environment.

Attack Vectors:
Exploiting insecure communication channels (e.g., weak encryption, misconfigured SSL/TLS).
Leveraging deficient patching or a lack of real-time monitoring.
Injecting malicious proxies or sniffing traffic between cloud users and services.

Impact:
Data theft, session hijacking, and service disruption.
Loss of trust in the SaaS provider.
Escalation of attacks across multiple tenants due to shared infrastructure vulnerabilities.

Cloud nodes: They contain the resources that can be accessed through cloud middleware. It is the set of policies and support service-oriented environment.

Logs and Audit Collector: It acts as a sensor for the CIDS detector and logs, a sequence of user and collects data and commands.

Cloud Provider: The application is accessible through client infrastructure, such as a web server, and it can be physically accessed. Provider's tasks include system maintenance and SaaS VMs deployment. Guest task: It is the sequence of commands and actions submitted through the client to an instance of VM.

External Entity: It can be a customer or client and manages the VMs allocated by the cloud provider according to the terms of the service level agreement.

Virtual Machine: VM deployment is a contacted agreement between the cloud provider and the customer. The detection mechanism is implemented outside the VM, i.e., out of reach of intruders. It provides the customer's application and services.

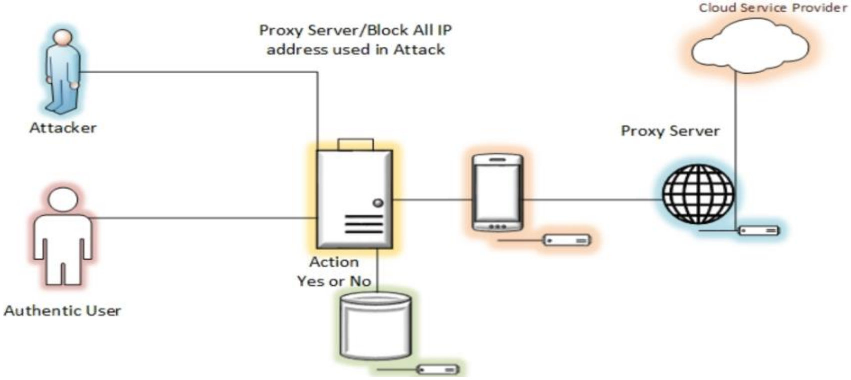

Figure 2. Cloud Security Model

The audit system: It has three main functions. First of all, it monitors message exchange among nodes and clouds. Then it monitors the middleware logging system in the cloud node itself. CIDs collect all audit data, including login and logout. The third function is to store events and logs from the VM system.

Several reasons put the SaaS VMs under the focus of our classification and analysis:

In the SaaS cloud, the reasons behind migration and adoption for cloud users mainly include on-demand and unlimited computation capabilities of SaaS VMs.

However, SaaS Host users are calculating software for critical services. This makes SaaS VMs a critical component in that service model. The security of SaaS VMs is addressed by different research works in virtualization by monitoring mechanisms at the application and software levels.

The use of CIDs mechanisms for security monitoring of SaaS of VMs is a promising approach that motivated research work in finding the best fit users and bringing its capabilities as a service in SaaS cloud, the security monitoring of SaaS based techniques, such as isolation of the monitoring agent.

Figure 1 sketches our classification between users and entities. Figure.1 shows that the attacks between the cloud provider and SaaS application user (dashed line) do not involve SaaS VMs.

Attack classes:

We describe the following classes of attacks: The classical attacks are performed by a user against the data of different users using the same application. These attacks can occur when the application and database are completely On-premises in their own infrastructure. One-to-one: These attacks are performed by a SaaS user from the domain of its application (App1) to access the rows of another application (App2). A best example is when App1 is modified or updated through the App-ID parameter to generate the following run-time SQL query: Select* from Orders where App-ID = 2. The App1 can be modified by App-ID in web sessions, since they are created by the client and server side to allow the application to identify the session and applications. One-to-many: These attacks are similar to previous ones; the difference is that Application (App2) accesses the rows of several Applications (App1 and App3) using its domain (www.App2.SaaS.com). When a malicious user attacks and injects 2=2 in the input field of a web session. In order to generate the query, Select * from Orders where AppID=2 or 2=2, it allows App1 to read the orders of other applications without injecting special characters.[10] We detail each class of attacks and provide the categories. An attack can be applied for both client and server within the cloud when distinction is necessary.

Attacks in Classical Mode:

In these attacks, the malicious user activities that he never originated through SaaS VM nor aimed to infect a VM with malware injection. A unique characteristic of cloud attacks is that detected by mechanisms through monitoring SaaS applications, machines,s, and CIDs monitoring VMs.

Access Management as a source of Attacks:

In this section, different attack origins through malicious activities due to the presence of sensitive data and targeting the cloud providers are discussed. We differentiate [11] between malicious users and non-malicious users in the SaaS cloud. However, different attacks can be realized when a malicious user accesses resources and applications only available and registered Users.

Misconfiguration of Cloud Customer:

A SaaS cloud adds more layers in its system, increasing the chance of misconfiguration arising; even a small configuration can affect the availability of cloud infrastructure.[12] Customers degrade the service quality of different clients in the same cloud and prevent others from accessing their critical resources. A report case describes a malicious customer creating loops in one content delivery network and multiple content delivery networks (CDNs). Such loops cause one request to be processed indefinitely, resulting in desired potential and consumption resource MITM attacks.

Access Management Authorize customers or non-customers:

According to the report, different agreements of access and management through different dedicated APIs, software, networks, storage, and usage of register accounts are attractive for attackers. [13] Different engineering also handles and needs to protect their data, as it helps attackers collect valuable information from [12], triggering them from users to manipulate their software services by alarming false information.

Attacks targeting the cloud provider did not directly harm the SaaS application machine, but first, they tampered with the functionality of the Cloud system. The design flaws in supportive stacks can help an external attacker about the virtual environment, execute unauthorized commands at cloud management, or perform a middle attack, for instance, exploiting vulnerabilities described in shown in Figure 2.

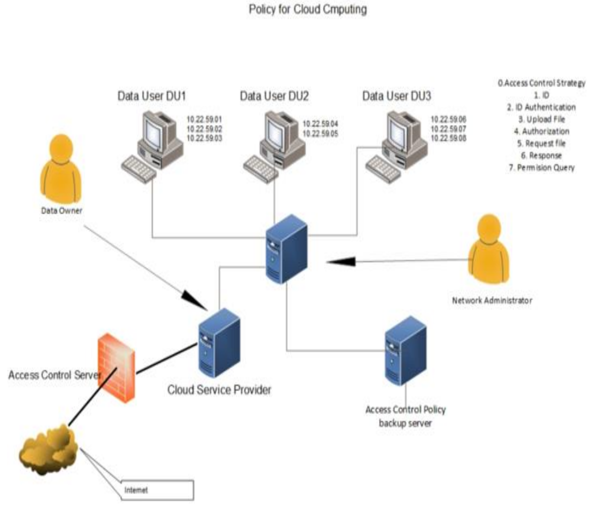

Figure 3a. Cloud Access Control policy

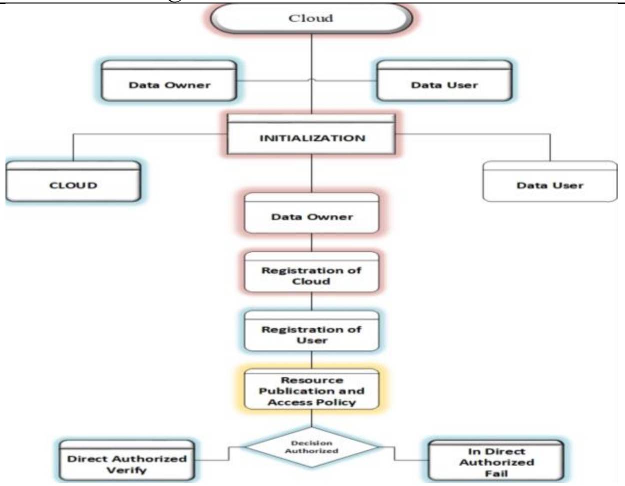

Figure 3b. Cloud Access Control Policy Algorithm

Table 1. [14] Attacks taking on Virtual Machine in SaaS

Effects and Risks	**Impact on SaaS Model** [4]
Data Breach: It is an incident in which sensitive and confidential data is stolen and used by an unauthorized person.	**'Confidentiality of Data Storage"** Solution: A Cryptographic Mechanism provides data storage and backup mechanisms.
In sufficient Identity, Credential, and Access Management: Users should be identified uniquely with federated authentication like SAML.	**"Authentication and Access Control"** Use a strong and multi-tier password for the authentication process.
Shared Technology: Sharing of resources and services among multiple users. They increase dependence on logical segmentation and control so that one tenant cannot interfere with other tenants.	**"Virtualization Availability'** Isolation of data and copies must be ensured. Strong Authentication mechanism to prevent the issue.
Denial of Service: They target the cloud models in a finite system resource, such as disk space, memory, and power consumption.	**"Data Privacy and Availability"** Encryption Homomorphism techniques are used for data storage and backup mechanisms.
Data loss: Data ownership, operational failure, data deletion, and availability challenges in cloud computing.	**"Intrusion detection":** It is based on traffic control on the network, understands the changing threat, and manages end-to-end encryption.

Different Cloud Provider as a source of attack:

The CERT (Computer Emergency Response Team) describes an insider attacker as an employee, business partner, or contractor who has access to an organization's network system and intentionally misuses resources in a manner that creates a negative effect on the availability, confidentiality, and integrity of an organization or information system. According to the survey in 2018 [12], 18% cases are reported as illegitimate modification, data breaches, and theft in private clouds were the result of organization employee insider conduct by malicious administrators who directly access client data. If cloud services use data encryption, a malicious user must have access to the private key when they are stored at the provider's storage components.

The outsider cloud provider attacked both customers and the external opponent.

SaaS application One to One as a target of attack

The activities attempted by the current SaaS application machine morph it to behave in an unauthorized manner towards its owner and environment.

From external opponent Compromised Retention Repositories:

The infected application, containing malware, unintentionally allows users who upload misconfiguration image templates. Only registered customers have the right to upload SaaS application templates.

Location-based Authentication:

Weaknesses of SaaS application machine placement algorithms and the lack of location privacy in cloud computing to verify and gain location. Software distribution Unit (SDU) [15] is a common software in data centers to monitor the software storage and consumption by using SNMP (Simple Network Management Protocol) to access the SDU The attacker introduces varying targets and loads to identify the server on the target machine.

Algorithm 1 Security-Based Trust

Input: The number of candidate Cloud Service Providers, CSP 'a and Security metrics, 'b'

Data Collection and Pre-processing DCP: It defines the security metrics 'b' according to some security issue of the cloud service template. A Candidate CSPs fill out the Security Metrics template and submits it as a security control delivery to SCDs. Integration and normalization of the SCDs as the Dataset N.

Security controls Deliverables: CSP, the content of Dataset N. (for example: security metrics) is quantified as dataset P according to security metrics.

Security Level Evaluation: Construct a normalized decision of metrics Q with quantitative SCD R by using the Formula

$$Rm \times n = \frac{Pij}{\sqrt{\sum m}} \; a \times b$$

It determined the SCDs as positive and negative ideal solutions for security metrics.

Attacks on migration of SaaS Virtual Machine:

One of the main features is live migration, in which a running SaaS VM is moved from one server to another server with the least possible interruption. It also improves the operating cost (like energy, power) by using a SaaS application machine. These attacks must be passive and active attacks that perform IP spoofing on the SaaS Virtual machine and extract sensitive data, such as keys and passwords. Different migration data and passwords can be sniffed if transmission is done without any encryption techniques, and the confidentiality of the SaaS infrastructure VM can be compromised.

Data Security-based Attack on Client Application:

These [16] attacks are one of the most common application-level attacks that hacked the SaaS web application of the client. Hackers use IP spoofing in web applications today. MITM-attack is an attack on the privacy of the client and a particular site, which can lead total breach of cloud security when customer data is manipulated or stolen. MITM attacks involve three parties: the attacker, the client, and the website. It steals client cookies and sensitive information, which identify the client with the SaaS website application. With the token of a legitimate user, the attacker can proceed with their interaction with the SaaS web application—specifically, to protect the user. There are two ways to become infected by XSS attacks.[17] An attacker's goal is to temper the application and hinder the SaaS application from properly delivering its cloud services.

Access Control from Cloud Provider:

Moreover, known attacks are buffer overflow, browser attacks [18], and cross-site scripting. However, if owning the cloud services is not the final objective, it is necessary to have enough capabilities to prevent further damaging attacks.

These attack scenarios have:

Buffer overflow is exactly what it sounds like: a target of a SaaS application to find a clear password using a specific command and extract a private key using third-party tools.

Accessing the sensitive and confidential information from its active logical databases.[19]

Exploiting vulnerability flaws in the integrity-protection mechanism of the hypervisor to divert a SaaS application to a web browser under his control using basic relocation functionality.

Using CIDs techniques and inspection techniques to illegally extract any information from the target SaaS application machine.

Privilege Escalation in SaaS Cloud:

There are two kinds of privilege in SaaS cloud: vertical and horizontal. Vertical Escalation in SaaS cloud requires granting himself higher privileges. It can be achieved by performing Kernel-level operations that allow the attacker to run unauthorized code [20] in the SaaS cloud.

SaaS application theft:

However, an attacker manipulates the control panel of the website that manages live migration of the server from one place to another, to gain unauthorized migration access to the website to his own cloud infrastructure.

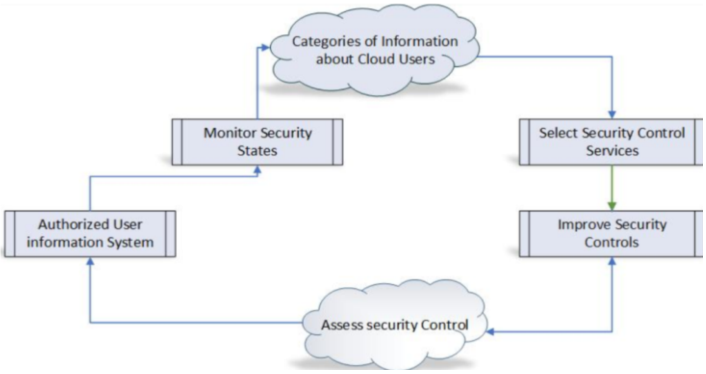
Categories of Information about Cloud Users
Monitor Security States
Select Security Control Services
Authorized User information System
Improve Security Controls
Assess security Control

Figure 4. CloudSecurity Control Policy

Table 2. Attacks taking on a Virtual Machine outside in SaaS

Outside User/ External Entity	Bad repositories and an attack on application Location Attacks on migrated virtual machines
Cloud Provider Services	Key theft and Password Disk Partition access Virtual-Based Intruder VBI-based attacks Virtual Machine theft

Table 3. [21] Attacks taking on a Virtual machine originated in SaaS

Source	Target	Virtual Machine	Cloud Provider
Originated Virtual Machine	Anti-VMI machine Anti-VM attack	Exploiting live migration	Dos attacks
Application Security	Session management & broken Authentication	SQL injection attacks	Modification of data rest and session hijacking
Physical level security issues	Loss of powerand	Phishing Attacks Malware Malware-Injected Attacks Attacks	Limited access to centers, Hardware modification, and theft
Originated Virtual Machine	Anti-VMI machine Anti-VM attack	Exploiting live migration	Dos attacks

Algorithm for Parsing and Summarization of MITM Attack in Cloud

```
Begin
Built table T with rows n
Define
dest-ip=1, sign-ip=2; i=1;
Aler-dscrp-strct = T (1)(signature-name, signature-class-id, priority, score-ip, ipprotocol, source-port, destination-port)
While (Length T 1 and I < length T)
    For j=i+1 to Length T do
        If (T(I, alter-dscrp-ip) = T(j, alert-descrp-strct))
            Add the I record in the table summarized T
            Delete i and j records from Table T, set i=1
        Else
            Merge i and j records of table T and add the resultant merge record in table T. Set i=1;
        End if
        End if
    End for
    i=i+1
End while
Add table T to table summarized T
End IF
Return summarized-T
```

Exploiting live Migration in SaaS:

Cloud Management is forcing the system to create many cloud migrations, leading to MITM attacks on SaaS applications and involving clients. Fake migration is injected SQL malware through a malicious SaaS web session into the host to perform SaaS application escape or MITM attacks against the client and different SaaS application Virtual Machines.

Attacks on the SaaS Hypervisor machine:

MITM Attacks:

It is the attacks against SaaS applications, where the attacker perhaps changes and transfers the corresponding information between the source and destination, who trust that they are directly communicating with one another. The IT culprit positions himself in a discussion between the application and its clients, for example, login certifications, account details, and ID card information. SaaS business, web-support exchange, and different sites where logging is required. The table shows the MITM types of attacks, including SSL decryption, CA decryption, IP spoofing, DHCP, and DNS spoofing are examples of MITM attacks.

Table 4. shows the MITMA attacks on different communication

Man-in-the-Middle Types	Layers of SaaS	Type of layer
ARP Spoofing	Datalink layers	OSI layer
CA Decryption and SSL Decryption	Presentation layers	OSI layer
IP Spoofing	Networking & Transport Layer	OSI layer
DHCP and DNS Spoofing	Application	OSI layer
FBS types	GSM	Cellular Network
FBS types	UTMS	Cellular Network

This attack exploitation by which malware in the SaaS applications: a) Local area Network tracking web application, b) Remote Network Tracking web application, c) Remote Network tracking SaaS application. It can manage to decode the unknown traffic between two parties.

Spoofing MITM SaaS Applications:

The same method is applied in modern cryptography spoofing in SaaS applications, where an attacker intercepts the personal and confidential information between the source and controls the sensitive data, while the source is not aware of the web session. When a source wants to communicate with other parties in a SaaS web application, then if the Network application is the same as an unknown MAC address, the main Cloud server broadcasts an ARP (Address Resolution Protocol) request to all clients for a similar Network application. Moreover, when the Address Resolution Protocol cache is managed in a dynamic or static mode, each application can be easily compromised by unauthorized forged Address Resolution Protocol messages. A proper authentication mechanism for log-in and log-out for SaaS web applications is missing. The medium saves IP to Mac entry in its local cache, and avoiding broadcasts and communication can speed up.

Using that security weakness for perfect MITM attack, Suppose, we have network: the attacker 'A' (IP =10.0.x.x3, Mac= EE: FF:GG: HH: A3), Malicious 'X' (IP= 10.0.x.x3, MAC = XX: XX: XX: XX: XX: XX: X1), victim 'B' (IP = 10.0.x.x2, Mac= CC: CC: CC: CC: CC: X3). Perfect based on the Address Resolution Protocol is shown:

'A' sends an ARP reply text message to X, which sends that IP: 10.0.x.x3 has Mac Address: EE: FF: GG: HH: A3. The message will update 'X's ARP table.

'A' also sends an ARP reply with 'Y', which sends that IP: 10.0.x.x3 has Mac address: EE: FF: GG: HH: II: JJ:x3. This message updates the 'Y' ARP table.

When 'X' wants to message to Y, it goes for 'A' Mac address EE: FF:GG: HH: II: X3, instead of "C" s CC:CC:CC:CC:CC: A2.

'Y' wants to send a message to X. It will go to A.

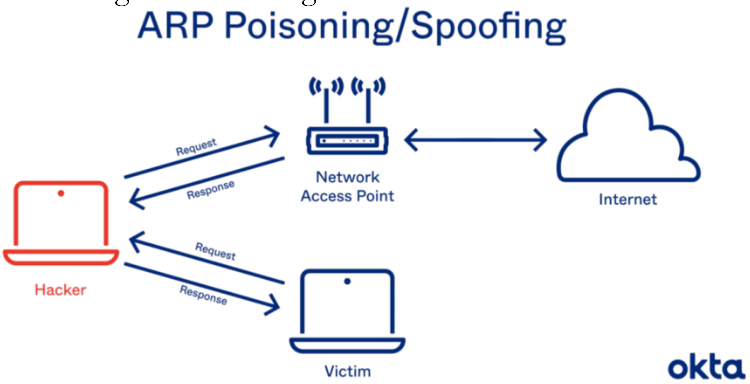

Figure 5. Cloud Computing ARP Model

Table 5 below shows a typical comparison between spoofing prevention techniques:

Table 5. Comparison of various spoofing prevention technologies

Medium of communication	Protocol	Concerns
Server-Based Commu Cloud	Address-Resolution Protocol	Cannot work for wireless communications in an IaaS cloud.
Server & Client-Based Cloud	DHCP, ARP	Compatible for Man of Middle Attack and Denial of Service, DHCP in PaaS cloud, but has a single point of failure in the IaaS cloud.
Client-Based Cloud	ARP	The level of importance of each client cloud is very difficult to decide for cloud computing.
Server-Based Cloud	ARP	Works only in Link Cloud. Dynamic IP does not support.
Cryptographic client-based	UDP/ARP	Authentication and UDP.
Symmetric & Private Cryptography Technique	DHCP	Client registers in advance, and the message flow, hard to large number of hosts.
Router-Based Cloud	ARP, IP	Filtering the on-path method can't secure communication between the Cloud Environment.
Router Host Cloud	DHCP, IP	Highest securedcommunication, but not a friendly user.

Algorithm: The analysis algorithm for Model C

```
Begin
Input: test audit data during the current login session
Use CIDs to compute SaaS by aligning against in same machine
If SAS $< \Phi$ sasThen
For each cloud node (C _node) that contains user I, do
Use CIDs to compute SaS, for the ith user in C _ node
If SaS $> \Phi$sas
Not-Masq-flag = True
Exit the loop
End if
End for
End if
If Not-Masq-flag = flag or HIDs instance is fired, then
Run step 2 of model A for each user CIDS instance firing
End if
End
```

Hyper call Attacks at SaaS:

These attacks consist of intrusion by a malicious guest SaaS application to another SaaS application using hyper call exploiting and interfaces malware vulnerabilities in the SaaS application VMMs hyper call handler. Attacks lead to an updated and modified 'host crash', between the execution of malicious code with SaaS application privileges. Xen memory enables different attacks, which are detailed in CVE-2015-4164 and the records.

Anti-SaaS application Attack:

SaaS application VMI is a powerful technique that specifically targets aspects of the Guest client whose execution is from outside. In SaaS architecture, the SaaS application machine allows a user to run a cloud Intrusion Detection System that monitors and secures the running Virtual Machine properties. The mechanism of monitoring and data in SaaS applications keeps the data secure and running properly. If any malware is detected, then in the web session and subvert an inspection tool for analysis, if it succeeds, then manipulate the kernel data by removing and adding the field of data structure, and both simultaneously, and changing its semantics.

Another method for Anti-SaaS application attacks is MITM personality malware, by which malware analyzes the web session environment, it only runs harmless code, and behaves as escaping detection.

Evaluation of attacks involving VMs

In this section, several aspects of SaaS malware attacks that involve SaaS applications are discussed. Our objective is to help the users of SaaS clients to have different types of standing for relevant security purposes and aspects about the attacks threatening their cloud environments, so a CIDs-based mitigation mechanisms can be designed.

First, we have classified and summarized different attacks in terms of security impact, attack complexity, and proposed defense mechanisms in the literature review. However, we analyze different types of attacks and vulnerabilities exploited by the attacks, reported in databases, and highlight the evaluation of the SaaS in the course of time. Finally, we present the economic impact of attacks on business processes as well.

Attack characteristics. In the Table, we summarized the SaaS attacks by presenting their characteristics, which are described as follows:

Table 6. Characteristics of different Attacks from SaaS Virtual Machines

Attacks	Counter Measures	Detectability	Complexity
Anti-SaaS VM Attack	Difficult Attack-specific	Unresolved issue	Medium
SaaS Virtual Machine Attack	Quality of Service Management	E-Monitoring System	Low
Dos channels Attack	Patching, Software Engineering, and formal verification	RTSC per heuristic and code	High
MITM Attack hypervisor	Attack specific	Un-resolved problem	Low

Complexity: It defines the difficulties faced by the attacker when performing the attacks, ranging from low, high, and medium.

Detectability: It defines the SaaS attack difficulties to detect an attack, ranging from easy to medium, and medium to difficult, and their deployment mechanism.

Countermeasures: It ensures the existing techniques to mitigate the SaaS attacks in cloud environments.

The table describes the different attacks that are addressed in the literature. Major countermeasures that deal with vulnerabilities and their mechanisms in the design of a virtualization component as a SaaS hypervisor. In the coming section "Vulnerability and SaaS Attacks report for clouds", we present a statistical analysis of the vulnerabilities of the SaaS cloud popular hypervisors.

Vulnerability & SaaS Attack Reports

This study adopts a statistical analysis approach to classify MITM (MitM) attacks in the SaaS cloud, where such attacks may act as a single point of failure due to the central role of the hypervisor and virtual machines (VMs). In particular, we consider popular hypervisor vulnerabilities affecting SaaS cloud infrastructures, such as Xen and KVM, commonly deployed in data centers and OpenStack-based virtualization environments.

The Methodology Follows These Directives:

The methodology of this study is presented under a distinct section to ensure clarity and transparency. It outlines the research framework, including data sources, classification procedures, and detection mechanisms. The approach integrates CVE dataset analysis with conceptual modeling of attack behaviors in SaaS environments, while also specifying detection strategies such as rule-based filtering for SQLi and anomaly detection for MITM. This structured methodology enhances reproducibility and provides a clear foundation for the subsequent results and discussion.

The classification of attacks in this study is primarily based on CVE (Common Vulnerabilities and Exposures) dataset analysis, which provides a comprehensive record of disclosed vulnerabilities. This empirical foundation ensures that our taxonomy is aligned with real-world threats. To complement the dataset-driven classification, we also incorporate conceptual modeling, which illustrates how identified vulnerabilities propagate within SaaS cloud environments. Although simulations were not conducted in the present work, they are identified as a future extension for empirical validation and performance benchmarking.

Data Source Selection:

Vulnerability data is collected from CVE Details (www.cvedetails.com), which provides comprehensive information on Common Vulnerabilities and Exposures (CVE). Each SaaS attack vulnerability is identified through its unique CIDs (CVE IDs) to ensure consistent tracking and reporting.

Data Preprocessing:

Duplicate entries within the vulnerability reports are eliminated to ensure accuracy and avoid statistical bias. Only entries explicitly describing vulnerabilities in SaaS applications that can be exploited by MitM or related attacks are retained for analysis. Classification of Vulnerabilities Vulnerabilities are classified based on their attack vector (e.g., network, virtualization layer, authentication process). Each vulnerability is mapped to its impact on SaaS security dimensions, including confidentiality, integrity, availability, and trust. Analysis and Interpretation Statistical summaries (frequency counts, distribution by hypervisor type, attack surface) are generated to highlight patterns of exploitation in SaaS environments. The classified vulnerabilities form the foundation for understanding MITM threats in SaaS and for suggesting CIDS (Cloud Intrusion Detection System) mechanisms to mitigate such attacks.

Business and Economic Perspective:

SaaS cloud is offering the possibilities of optimization and cost-saving applications for the cloud, different third parties, and contract agreements signed between the cloud provider and business client, and the user pays for resources that can be consumed by their deployed SaaS application. In cloud computing, clients can pay for using the cloud services and consume by data centers deployed SaaS VMs. Moreover, the security threat from attacks involving SaaS VMs can impact both the cloud client and cloud provider financially and economically. MITM-attack and Denial of Service are the most common and largest attacks, and a common threat. According to a survey [21] of different attacks, the cost to medium to larger organizations averages $63000 per incident, while $55000 for medium enterprises for SaaS cloud environments. Cloud provider is penalized with clients, which can due when QoS (Quality of service) specified in the SLAs is not fulfilled.

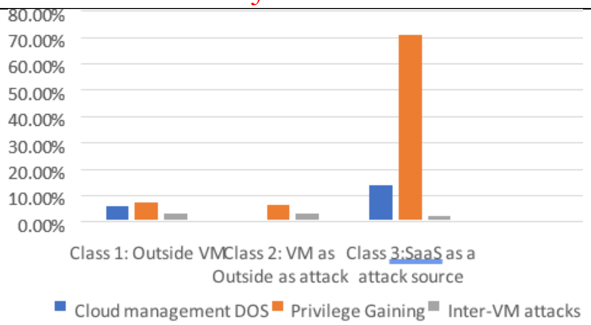

Figure 6. Cloud Computing SaaS Attacks

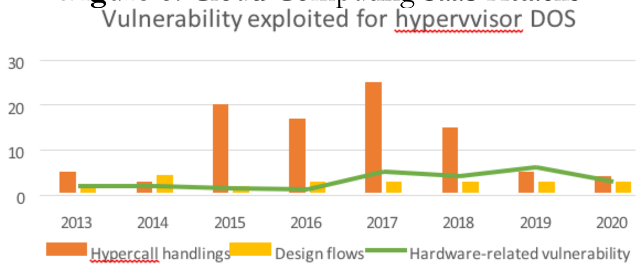

Figure 7. Cloud computing vulnerability exploited by DoS attacks

The cloud user sent a request that simultaneously uses bandwidth and results in billing for the cloud provider/owner.

Both cloud client and cloud provider should implement effective solutions that reduce the risk of SaaS security breaches. Cloud computing providers invest in security measures, including software, hardware, antivirus, and different IT Security employees to prevent different security threats. In case of MITMA (Man in the Middle Attack), financial damages for the cloud provider include the cost of working hours for disinfection, analysis, and revenue, repairing of system, and losses in productivity of the cloud service. Moreover, the long-term damage to the provider's reputation needs to be considered: if the breach is privately announced and it can be restrictive for future clients.

Our detection framework employs a hybrid strategy tailored to different attack types. SQL Injection (SQLi) attacks are identified through rule-based mechanisms, which match incoming queries against predefined malicious patterns. In contrast, Man-in-the-Middle (MITM) attacks are detected using anomaly detection methods, which monitor irregularities in network traffic flows. While these techniques provide robust initial detection, we also recognize the potential of machine learning (ML)driven models for adaptive recognition, which we outline as part of future work.

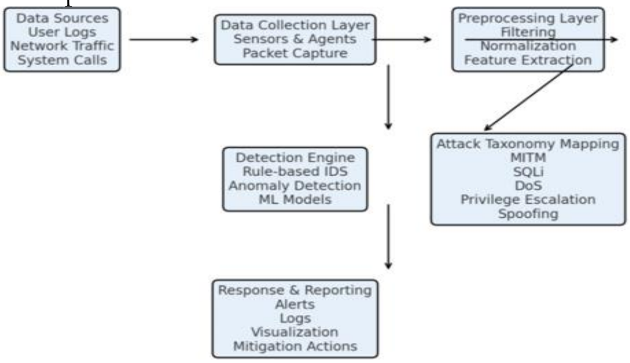

Figure 8. Proposed Cloud Intrusion Detection System (CIDS) Architecture

Conclusion:

In this paper, we present the classification of MITMA in the SaaS cloud. We define it in different scenarios, in which internal and external attacks, SaaS VMs, and cloud providers can be the source and destination of attacks. Our approach takes into account and targets

SaaS attacks that take place outside of the SaaS application and discusses different classes: attacks that take place inside from SaaS application, attacks that target the SaaS application, and attacks originating from the SaaS application. A common characteristic of attacks that have been addressed using CID-based techniques. However, we focus on attacks that directly involve SaaS for both the source and target of attacks. Our study supports at early stage of design of CIDs-based mitigation mechanisms by identifying the SaaS attacks that threaten their SaaS Virtual Machine by which can harm co-located SaaS VMs.

A statistical analysis of CVE reports on SaaS virtualization products how most vulnerabilities allow attackers to exploit flaws in the product design, especially to achieve MITM attacks from business and economics perspectives, most damaging attacks and more expensive losses for the cloud provider.

Reference:

[1] F. Nisar, M. Amin, M. Touseef Irshad, H. Hadi, N. Ahmad, and M. Ladan,"Machine learning-based spreading factor optimization in LoRaWAN networks," *Front. Comput. Sci*, vol. 7, 2025, doi: https://doi.org/10.3389/fcomp.2025.1666262.

[2] G. Idex, "Cisco Global Cloud Index-Forecast and Methodology-2016-2021," *Cisco, San Jose, Ca, USA, white Pap.*, 2018, [Online]. Available: https://www.scribd.com/document/370618138/Cisco-Global-Cloud-Index-Forecast-and-Methodology-2016-2021

[3] T. S. and G. Byrd, "The Internet of Everything," *Computer (Long. Beach. Calif).*, 2014, [Online]. Available: https://www.researchgate.net/publication/264231862_The_Internet_of_Everything

[4] D. E. Culler, "THE ONCE AND FUTURE INTERNET OF EVERYTHING," *GetMobile Mob. Comput. Commun.*, vol. 20, no. 3, pp. 5–11, Jan. 2017, doi: 10.1145/3036699.3036701.

[5] W. Shi and S. Dustdar, "The Promise of Edge Computing," *Computer (Long. Beach. Calif).*, vol. 49, no. 5, pp. 78–81, May 2016, doi: 10.1109/MC.2016.145.

[6] F. Nisar, M. Amin, M. Touseef Irshad, H. Hadi, N. Ahmad, and M. Ladan, "XGBoost-Driven Adaptive Spreading Factor Allocation for Energy-Efficient LoRaWAN Networks," *Front. Commun. Networks*, vol. 6, p. 1665262, doi: 10.3389/FRCMN.2025.1665262.

[7] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *https://doi.org/10.1137/S0097539701398521*, vol. 32, no. 3, pp. 586–615, Feb. 2012, doi: 10.1137/S0097539701398521.

[8] K. Upreti, B. K. Vargis, R. Jain, and M. Upadhyaya, "Analytical study on performance of cloud computing with respect to data security," *Proc. - 5th Int. Conf. Intell. Comput. Control Syst. ICICCS 2021*, pp. 96–101, May 2021, doi: 10.1109/ICICCS51141.2021.9432268.

[9] G. A. Shiraz M, "Mobile Cloud Computing: Critical Analysis of Application Deployment in Virtual Machines," *Int. Conf. Comput. Netw. (ICICN 2012)*, 2012, [Online]. Available: https://www.researchgate.net/publication/264888478_Mobile_Cloud_Computing_Critical_Analysis_of_Application_Deployment_in_Virtual_Machines

[10] Q. S. and D. L.-J. M. R. Baharon, "A New Lightweight Homomorphic Encryption Scheme for Mobile Cloud Computing," *2015 IEEE Int. Conf. Comput. Inf. Technol.*, pp. 618–625, 2015, doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.88.

[11] C. Wang, W. Li, Y. Li, and X. Xu, "A Ciphertext-Policy Attribute-Based Encryption Scheme Supporting Keyword Search Function," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8300 LNCS, pp. 377–386, 2013, doi: 10.1007/978-3-319-03584-0_28.

[12] J. K. L. Xu Yang, Xinyi Huang a, "Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing," *Futur. Gener. Comput. Syst.*, vol. 62, pp. 190–195, 2016, doi: https://doi.org/10.1016/j.future.2015.09.028.

[13] K. Zhang, "Energy-Efficient Offloading for Mobile Edge Computing in 5G Heterogeneous Networks," *IEEE Access*, vol. 4, pp. 5896–5907, 2016, doi: 10.1109/ACCESS.2016.2597169.

[14] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, pp. 47–53, 2000, [Online]. Available: https://link.springer.com/chapter/10.1007/3-540-39568-7_5

[15] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, 2011, doi: https://doi.org/10.1007/978-3-642-19379-8_4.

[16] A. Lewko, A. Sanais, and B. Waters, "Revocation systems with very small private keys," *Proc. - IEEE Symp. Secur. Priv.*, pp. 273–285, 2010, doi: 10.1109/SP.2010.23.

[17] G. B. & M. S. Matt Blaze, "Divertible protocols and atomic proxy cryptography," *Adv. Cryptol. — EUROCRYPT'98*, pp. 127–144, 2006, doi: https://doi.org/10.1007/BFb0054122.

[18] Y. D. Anca Ivan, "Proxy Cryptography Revisited," *Netw. Distrib. Syst. Secur. Sympt SanDaiego CA*, 2003, [Online]. Available: https://www.ndss-symposium.org/wp-content/uploads/2017/09/Proxy-Cryptography-Revisited-Anca-Ivan.pdf

[19] J. Weng, R. H. Deng, X. Ding, C. K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," *Proc. 4th Int. Symp. ACM Symp. Information, Comput. Commun. Secur. ASIACCS'09*, pp. 322–332, 2009, doi: 10.1145/1533057.1533100.

[20] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *Lect. Notes Comput. Sci.*, 1985, doi: https://doi.org/10.1007/3-540-39568-7_2.

[21] J. A. González-Martínez, E. G.-S. , Miguel L. Bote-Lorenzo, and R. Cano-Parra, "Cloud computing and education: A state-of-the-art survey," *Comput. Educ.*, vol. 80, pp. 132–151, 2015, doi: https://doi.org/10.1016/j.compedu.2014.08.017.