Acadlore Transactions on AI and Machine Learning
https://www.acadlore.com/journals/ATAIML

Characterization and Risk Assessment of Cybersecurity Threats in Cloud Computing: A Comparative Evaluation of Mitigation Techniques

Oludele Awodele[1], Chibueze Ogbonna[1], Emmanuel O. Ogu[1], Johnson O. Hinmikaiye[1], Jide E. T. Akinsola[2*]

[1] Department of Computer Science, Babcock University, 121003 Ilisan-Remo, Nigeria
[2] Department of Computer Sciences, First Technical University, 200255 Ibadan, Nigeria

* Correspondence: Jide E. T. Akinsola (akinsolajet@gmail.com)

Received: 03-11-2024 **Revised:** 05-02-2024 **Accepted:** 05-10-2024

Citation: O. Awodele, C. Ogbonna, E. O. Ogu, J. O. Hinmikaiye, and J. E. T. Akinsola, "Characterization and risk assessment of cybersecurity threats in cloud computing: A comparative evaluation of mitigation techniques," *Acadlore Trans. Mach. Learn.*, vol. 3, no. 2, pp. 106–118, 2024. https://doi.org/10.56578/ataiml030204.

Abstract: Advancements in information technology have significantly enhanced productivity and efficiency through the adoption of cloud computing, yet this adoption has also introduced a spectrum of security threats. Effective cybersecurity mitigation strategies are imperative to minimize the impact on cloud infrastructure and ensure reliability. This study seeks to categorize and assess the risk levels of cybersecurity threats in cloud computing environments, providing a comprehensive characterization based on eleven major causes, including natural disasters, loss of encryption keys, unauthorized login access, and others. Using fuzzy set theory to analyze uncertainties and model threats, threats were identified, prioritized, and categorized according to their impact on cloud infrastructure. A high level of data loss was revealed in five key features, such as encryption key compromise and unauthorized login access, while a lower impact was observed in unknown cloud storage and exposure to sensitive data. Seven threat features, including encryption key loss and operating system failure, were found to significantly contribute to data breaches. In contrast, others like virtual machine sharing and impersonation, exhibited lower risk levels. A comparative analysis of threat mitigation techniques determined Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege (STRIDE) as the most effective methodology with a score of 59, followed by Quality Threat Modeling Methodology (QTMM) (57), Common Vulnerability Scoring System (CVSS) (51), Process for Attack Simulation and Threat Analysis (PASTA) (50), and Persona non-Grata (PnG) (47). Attack Tree and Hierarchical Threat Modeling Methodology (HTMM) each achieved 46, while Linkability, Identifiablility, Nonrepudiation, Detectability, Disclosure of Information, Unawareness and Noncompliance (LINDDUN) scored 45. These findings underscore the value of fuzzy set theory in tandem with threat modeling to categorize and assess cybersecurity risks in cloud computing. STRIDE is recommended as an effective modeling technique for cloud environments. This comprehensive analysis provides critical insights for organizations and security experts, empowering them to proactively address recurring threats and minimize disruptions to daily operations.

Keywords: Cloud computing; Cybersecurity; Fuzzy set theory; Information security; Threat modeling

1 Introduction

Information and Communication Technology (ICT) has expanded dramatically with the advent of cloud computing and the tremendous benefits it offers to business organizations [1]. However, the transition from the traditional era of doing business to this new paradigm may be hampered by cloud tenants' different security and privacy concerns and a lack of underlying infrastructure transparency [2]. Due to a lack of transparency in the underlying cloud infrastructure, security policymakers have been emphasizing the need to protect cloud infrastructure, ICT systems and applications against cyberattacks [3]. Cloud infrastructure can be described as the fundamental cloud telecommunication systems connected and classified as instruments utilized in ICT activities. These infrastructures are deployed and made available through the cloud system to decrease procurement and physical space management costs [4]. As a software as well as hardware element collection that is important to allow cloud computing, cloud infrastructure may also be referred to as cloud computing infrastructure [5]. The present state of cybersecurity in cloud computing indicates an increasing reliance on cloud services, with a noticeable move toward hybrid cloud systems and the implementation of

Zero Trust Architecture (ZTA) [6]. To handle increasing threats and regulatory problems, organizations are turning to cloud-native security solutions [7].

Fuzzy set theory is a mathematical paradigm for dealing with ambiguity and vagueness in data. Unlike classical set theory, which assumes that an element either belongs or does not belong to a set, fuzzy set theory enables partial membership, which means that an element might belong to a set to some extent [8]. Fuzzy set theory is ideal for cybersecurity research as it can deal with ambiguous data and the complexities of risk evaluation and threat analysis. It enables a more detailed knowledge of potential hazards and weaknesses, particularly in evolving and complicated cyberspaces [9]. Threat modeling is a methodical way to detect and address potential security threats and vulnerabilities in software or systems. It involves exploring the system's architecture, detecting potential dangers, and devising tactics to combat them. Threat modeling is ideal for cybersecurity research given that it provides an organized and complete approach to analyzing and mitigating security concerns [10]. Organizations can improve their general level of security by proactively discovering possible vulnerabilities early in the creation or implementation process [11]. In addition to the economic benefits of cloud computing, cloud infrastructure poses a security threat. Cybersecurity is the practice of protecting cloud infrastructure and its surroundings from cyberattacks [5]. Cybersecurity refers to the use of procedures, technology, and controls to defend against cyberattacks on infrastructure, networks, devices, programs, systems, and data. Its goals are to reduce the risk of cyberattacks as well as defend against the illegal use of technology, networks, and systems.

Information technology is becoming much more prominent. It promotes security events to grow exponentially in many forms, such as denial of service (DoS), unauthorized access, malware assaults, data breaches, social engineering or phishing attacks on the Internet. As one of the cloud service delivery methods, Infrastructure as a Service (IaaS) provides on-demand computing resources that present the environment of cloud computing with significant risks, among other things [12]. These security incidents are referred to as cybersecurity risk, which is defined as the potential loss caused by an organization's technological infrastructure [13, 14]. According to Guide 73:2009 of the International Organization for Standardization (ISO) on risk management, cybersecurity risks are associated with the loss of confidentiality, integrity, information, data, and control systems, and they reflect the potential negative impacts on assets, organizational operations, other organizations, the nation as well as individuals [15].

Documentation through the Anurag Visual, Agile and Simple Threat (AVAST) statistics shows about 50 million executable malwares. This statistic doubled to about 100 million in 2012, and it was about 900 million in 2019 [16]. According to AVAST figures, the year 2022 has seen a record-breaking number of malware—over 1.2 billion—in existence [11]. Organizational activities were affected financially by this, which caused major financial losses for both firms and individuals. The cost of a data breach is USD 8.19 million worldwide and USD 3.9 million in the United States on average. In addition, the cost of global economic cybercrime is USD 400 billion each year [3, 17–19]. This is really provocative and should compel every organization to look for preventative measures. To this end, this study explored various cybersecurity threats, such as loss of encryption keys, and illegal access to login within the cloud computing environment, aiming to provide ways to mitigate their effects and reduce the danger of cyberattacks.

2 Literature Review

Cybersecurity is the process of preventing cyberattacks, cyber threats and illegal access to company applications, data, programs, networks, and systems [20]. Whereas cyber threats or security attacks are defined as hostile acts aiming to steal or harm data or disrupt an enterprise's digital welfare and stability [21]. Cybersecurity may help with risk management, the prevention of cyberattacks, data breaches, and identity theft [22]. It responds to threats if a company knows network security and operative occurrence response plans, such as safeguarding data and protecting it against theft and loss as well as scanning computers for malevolent software [23].

Cloud computing is a continually advancing technology that allows appealing and quantitative services, which enables businesses to commercialize their operations, increase efficiency and make profit while lowering expenses [24, 25]. It has the potential to become a market leader while providing secure, virtual, and cost-effective solutions [26, 27]. Cloud computing has several advantages including flexibility, efficiency, scalability, integration, capital savings, and shared resources [28]. It also provides a sophisticated virtual environment for business applications and operations [29]. Riding on its highlighted importance, cloud computing has the potential to redefine how businesses manage information technology while changing the economics of hardware and software [30]. Cloud computing comes with its downsides. To understand cloud computing security dangers [31], it is essential to understand the dependence and connection between cloud computing models [32]. According to the National Institute of Standards and Technology (NIST), cloud computing has critical features, which are four cloud deployment models and three cloud service models [33]. Figure 1 shows the visual model of cloud computing.

Joshi et al. [12] presented an overview of the dangers and weaknesses of cloud computing. It was discovered that threats and vulnerabilities, such as data loss, vulnerable systems, malicious insiders, data breaches, DoS, Application Programming Interfaces (APIs), account hijacking, shared technology vulnerabilities, weak authentication and identity management as well as the associated vulnerabilities, are still evolving. Cloud computing is a new sort of computing

model. Many firms are attempting to use it owing to its inherent benefits. According to the survey, cloud computing security is still developing, with new threats and vulnerabilities being discovered.

Amara et al. [24] conducted a study on threat modeling for cloud infrastructure using several methods, such as attack trees, surfaces and graphs, as well as security metrics. Attack trees and graphs are all examples of attack surfaces. The research demonstrated how to apply a hardening strategy based on threat models and security metrics. A clearer picture of possible hazards and prevention was offered, not only benefiting cloud providers but also instilling more trust in cloud tenants.

To approach the important concern of integrity and privacy issues in IaaS, Joshi et al. [12] detailed many sorts of security vulnerabilities in the IaaS layer and ways for resolving them to enhance performance and maintain the greatest degree of IaaS security. The study identified two types of risks: component-based and service-based threats. However, the mechanism used in classifying these threats was not analyzed. The outcome of the study by Naseer et al. [24] emphasizes architectural concepts, essential security needs, security risks and attacks on cloud computing as well as mitigating solutions. The research focuses on the dangers defined as components by Joshi et al. [12]. The study summarized many security attacks and threats, the techniques of mitigating and classifying them according to the affected cloud services and their location on the network layers. Nevertheless, it has limitations with respect to the execution of the presented mitigation techniques. Akinsola et al. [34] developed a threat-hunting model using machine learning paradigms with great applications in the cloud environment.

Alhebaishi et al. [35] and Urias et al. [21] conducted thorough threat modeling experiments based on two sample cloud infrastructures using many prominent approaches such as attack trees, graphs and surfaces as well as graph security metrics accordingly. The findings suggest that potential cloud tenants might be more confident in adopting cloud infrastructure services if a clearer image of potential hazards in cloud infrastructure and appropriate remedies are provided. However, the study does not include any methods, which can be used by cloud data centers to obtain actionable knowledge from threat modeling and measurement findings [36]. In addition, the study does not clearly identify cybersecurity threats with their corresponding threat levels, which has been addressed in this study. This is particularly related to the impact of cyberthreat features on related mitigation techniques and the impact of the causes with the corresponding risk level on those cyberthreat features.

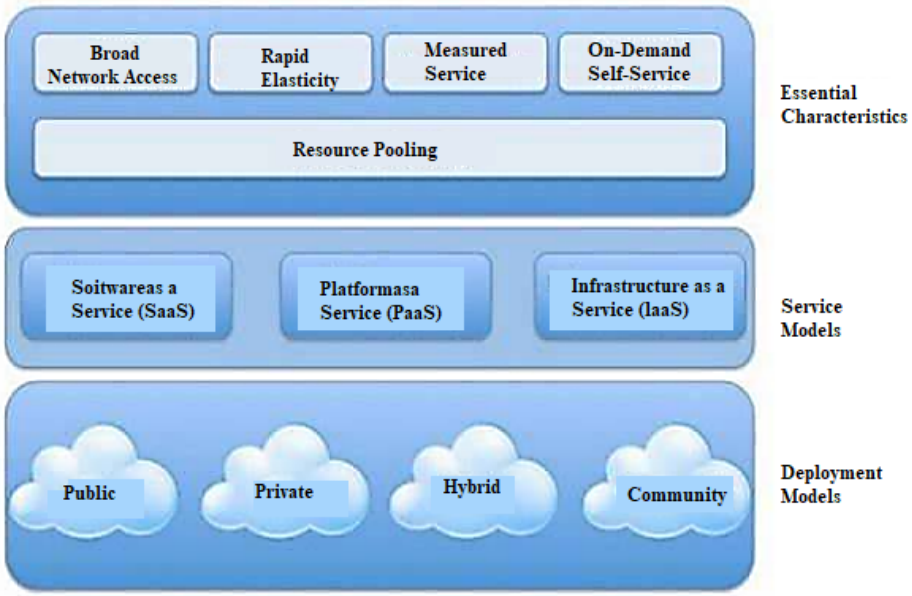

Figure 1. A visual model of cloud computing [34]

The asset-centric threat modeling methodologies have proven to be beneficial for asset protection, analysis, and business risk control. The most widely used methodologies are Damage, Reproducibility, Exploitability, Affected Users and Discoverability (DREAD), Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), PASTA and Threat and Risk Intelligence Knowledge-base (Trike). Meta-attacking language has been identified as a good tool for threat modeling and attack simulations.

By considering cyberthreats such as data loss and breaches, account hijacking, insecure interfaces and APIs, malicious insiders, insufficient due diligence, abusive use of cloud services, shared technology issues, identity theft, changes in business model, and lock-in in the IaaS in a cloud environment, this study aims to determine

their risk levels and find out the best cyberthreat mitigation techniques suitable for the IaaS in a cloud computing environment. Therefore, works of literature were analyzed and synthesized using the Preview, Question, Read and Summarize method (PQRS). Thereafter, empirical analysis was conducted using fuzzy set theory in the determination of cyberthreat risk levels. The outcome of this study contributes to the cloud computing field and helps cybersecurity experts develop a cyberthreat mitigation model adaptable to the cloud environment.

3 Methodology

This study employed desk-based research and empirical work. It comprises the examination of existing literature on review methodologies, which helps situate the study within the context of existing evidence by employing a semi-experimental research methodological approach. This study focuses on providing a secured cloud platform by identifying critical assets and infrastructure from threat agents. The research aim was achieved by characterizing existing cybersecurity risk mitigation models and then determining the risk level using a threat modeling approach.

Previous studies were extensively assessed using the PQRS for various security threats attacking cloud computing infrastructure as well as the different methods available for tackling these security issues. The features generated from the PQRS were characterized into assets, threat actors, and attack vectors for effective threat matrix formulation.

The threat features obtained were used to develop the security threat taxonomy. The threat taxonomy was created using matrix formulation by considering the categories of threats, artifacts/actors, cybersecurity threats and attacks for the threat modeling techniques. The fuzzy set theory was implemented to measure the risk level of various cybersecurity threats discovered, and various threat modeling techniques such as STRIDE, PASTA, LINDDUN, CVSS, Attack Tree, PnG, Security Cards, HTMM, QTMM, Trike, Visual, Agile and Simple Threat (VAST) Modelling, and OCTAVE were adopted for solving the identified threats. However, cyber risk mitigation in relation to Platform as a Service (PaaS) and Software as a Service (SaaS) was not considered in this study.

3.1 Characterization of Cybersecurity Threats and Determination of Risk Levels

The study extensively assessed previous literature concerning various security threats attacking cloud computing infrastructure and the different methods available for tackling these security issues. These studies were analyzed and synthesized using the PQRS. The PQRS was selected because it gives a direct flow on how related works can be obtained for benchmark purposes. In addition, it helps quickly identify the risk factors that may affect the adoption of cloud infrastructure services. This study characterizes cyber threats based on eleven features such as data loss and breaches, account hijacking, and so on, as well as some causes such as natural disaster, loss of encryption key, illegal access to login details, undeserved operations conducted by users, unknown cloud storage, exposure of sensitive information, unlawful acts of users, usage of the same virtual machine (VM) by multiple users, impersonation, operating system failure, following internal security measures. Linguistic characterization and fuzzy approaches were utilized for risk level determination.

These features were then characterized into assets, threat actors, and attack vectors for effective threat matrix formulation.

3.1.1 Cybersecurity threats and risk level determination

A comparative analysis of cybersecurity threats was conducted using eleven major causes based on how dangerous the cybersecurity threats are. In addition, it helps detect the threats that need to be eradicated. The risk level was determined using this approach.

The input defined in Eq. (1) and reported in Table 1 together make up the fuzzy input for the classification of cybersecurity threats. The defined membership of the fuzzy input shows the degree of their presence in the set between 0 and 1 inclusive.

$$A = \begin{cases} \text{data loss, data breaches, account hijacking, insecure interfaces and APIs,} \\ \text{malicious insiders, insufficient due diligence, abusive use of cloud services,} \\ \text{shared technology issues, identity theft, changes in business model, lock-in} \end{cases} \tag{1}$$

According to Eq. (2), the membership variables represent the level of membership for the specified membership set A. It is employed to demonstrate the level of categorization for a specific class attribute value. The grades specified in Eq. (2) can be assumed for the input and output variables.

$$mA(x) = \text{low, medium, high, very high} \tag{2}$$

Eq. (3) is given as the Triangular Membership Function (TMF). The lower boundary a_1, the upper boundary a_3 and the value a_2 describe the TMF of A, where a_1 is less than a_2, and a_2 is less than a_3 such that x is the average value of A and a_1, a_2 and a_3 are real numbers, as shown in Eq. (3).

Since the membership variables consist of four variables, the TMF as given in Eq. (3) was adopted. The extreme values were calibrated using the TMF. Figure 2 shows the triangular fuzzy number (TFN) used in Table 1, indicating the fuzzy range of values for the fuzzification procedure.

$$\mu_{(A)}(x) = \begin{cases} 0, & x < a_1 \\ \frac{x-a_1}{a_2-a_1}, & a_1 \leq x \leq a_2 \\ \frac{a_3-x}{a_3-a_2}, & a_2 \leq x \leq a_3 \\ 0, & x > a_3 \end{cases} \tag{3}$$

where, x in Eq. (3) represents the x-coordinate of real values, and a_1, a_2 and a_3 represent the y-coordinate between 0 and 1.

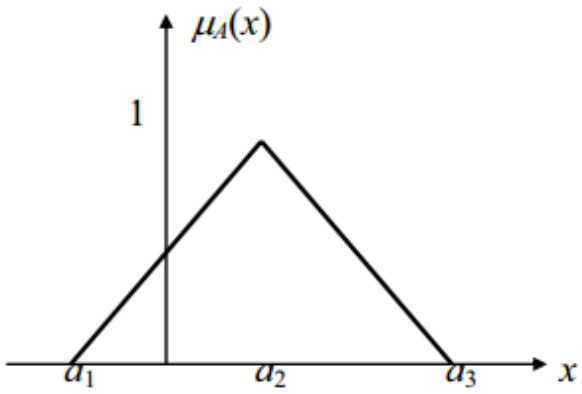

Figure 2. TFN (a_1, a_2 and a_3)

Intervals are used in Table 1 because there are four linguistic variables and the adapted membership function is triangular. Therefore, the value interval can be assumed using $x_i / \sum n$, where x_i = 1 to 4 and n = 4. In other words, x_i is the individual linguistic variable l = low, 2 = medium, 3 = high, 4 = very high and $x_i / \sum n$ is the total number of linguistic variables, with n = 4.

For instance, low is 1/4 = 0.25; medium is 2/4 = 0.5; high is 3/4 = 0.75 and very high is 4/4 = 1. Table 1 shows the range of intervals.

Table 1. Fuzzy value range

Membership Variable	Value Range
Low	$0.1 \leq x < 0.3$
Medium	$0.3 \leq x < 0.6$
High	$0.6 \leq x < 0.8$
Very high	$0.8 \leq x \leq 1.0$

3.2 Creation of Taxonomy for Cybersecurity Threats in a Cloud Computing Environment

The procedures utilized in characterizing and determining risk levels are elucidated accordingly. The taxonomy presents a summary of all the security threats affecting cloud computing infrastructure. The affected cloud infrastructure is also listed accordingly, such as the attack methods, and mitigation techniques for these threats are also included in the taxonomy.

3.3 Comparative Analysis of Threat Mitigation Techniques

The study comparatively analyzed the identified threat mitigation techniques such as STRIDE, PASTA, LINDDUN, CVSS, Attack Tree, PnG, Security Cards, HTMM, QTMM, Trike, VAST Modelling, and OCTAVE. These mitigation techniques help ensure the proper security of cloud computing. Comparative analysis was performed on 12 mitigation techniques based on 14 features namely, documentation, technical threat identification, time consumption, usage, model maturity, training or usage requirements, business impact, security properties, threat classification, stakeholders' input or collaboration, threat prioritization, and reliability. This helps identify the most suitable technique to mitigate the effect of cyberthreats on cloud infrastructure.

4 Results

This section discusses the results of the study using the methodology in Section 3, such as the characterization of cyberthreats, the creation of a taxonomy of cloud computing security threats, and the assessment of cybersecurity risk levels for effective mitigation.

Table 2. Analysis of cybersecurity threats using risk level parameters

		Cybersecurity Threat Features										
S/N	**Causes**	**Data Loss**	**Data Breaches**	**Account Hijacking**	**Insecure Interfaces and APIs**	**Malicious Insiders**	**Insufficient Due Diligence**	**Abusive Use of Cloud Services**	**Shared Technology Issues**	**Identity Theft**	**Changes in Business Model**	**Lock -in**
1	Natural disaster	High	Low	Low	Low	Low	Low	Low	Low	Low	High	Low
2	Loss of encryption key	High	High	Medium	High	Low	Low	Low	Low	Low	Low	Low
3	Illegal access to login details	Low	High	High	Low	Low	Low	Low	Low	High	Low	Low
4	Undeserved operations conducted by users	High	High	High	Low	High	Low	Low	Low	Low	Low	Low
5	Unknown cloud storage	Low	High	Low	Low	High	High	Low	Low	Low	Low	High
6	Exposure to sensitive information	Low	High	Low	Low	High	Low	Low	Low	Low	Low	Low
7	Unlawful acts of users	High	High	Low	Low	High	Low	High	Low	Low	Low	Low
8	Usage of the same VM by multiple users	Low	Medium	Medium	Low	Low	Low	Medium	High	Medium	Low	Low
9	Impersonation	Low	Low	Medium	Low	Low	Low	Low	Medium	High	Low	Low
10	Operating system failure	High	High	Medium	Low	Low	Low	Low	Low	Low	Medium	Low
11	Following internal security measures	Medium	High	Medium	Low	Low	Medium	Low	Low	Low	Low	Low

Table 3. Analysis of cybersecurity threats using fuzzy set analysis

		Cybersecurity Threat Features										
S/N	**Causes**	**Data Loss**	**Data Breaches**	**Account Hijacking**	**Insecure Interfaces and APIs**	**Malicious Insiders**	**Insufficient Due Diligence**	**Abusive Use of Cloud Services**	**Shared Technology Issues**	**Identity Theft**	**Changes in Business Model**	**Lock -in**
1	Natural disaster	0.75	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.75	0.25
2	Loss of encryption key	0.75	0.75	0.50	0.75	0.25	0.25	0.25	0.25	0.25	0.25	0.25
3	Illegal access to login details	0.25	0.75	0.75	0.25	0.25	0.25	0.25	0.25	0.75	0.25	0.25
4	Undeserved operations conducted by users	0.75	0.75	0.75	0.25	0.75	0.25	0.25	0.25	0.25	0.25	0.25
5	Unknown cloud storage	0.25	0.75	0.25	0.25	0.75	0.75	0.25	0.25	0.25	0.25	0.75
6	Exposure to sensitive information	0.25	0.75	0.25	0.25	0.75	0.25	0.25	0.25	0.25	0.25	0.25
7	Unlawful acts of users	0.75	0.75	0.25	0.25	0.75	0.25	0.75	0.25	0.25	0.25	0.25
8	Usage of the same VM by multiple users	0.25	0.25	0.75	0.25	0.25	0.25	0.75	0.75	0.75	0.25	0.25
9	Impersonation	0.25	0.25	0.75	0.25	0.25	0.25	0.25	0.75	0.75	0.25	0.25
10	Operating system failure	0.75	0.75	0.75	0.25	0.25	0.25	0.25	0.25	0.25	0.75	0.25
11	Following internal security measures	0.75	0.75	0.75	0.25	0.25	0.75	0.25	0.25	0.25	0.25	0.25
12	**Total**	**11.5**	**13.5**	**12**	**6.5**	**9.5**	**4.5**	**7.5**	**4**	**4.5**	**4**	**3.5**

4.1 Characterization of Cyberthreats

The characterization results of cyberthreats are based on features such as data loss and breaches, account hijacking, malicious insiders, shared technologies, insecure interfaces, abusive use of the cloud, insufficient due diligence, and identity theft. Also, causes such as loss of encryption, illegal access to login, undeserved operations conducted by

users, unknown cloud storage, and exposure of sensitive information are presented accordingly. The results show that there is high data loss in five features and low data loss in six features. Seven features are affected by data breaches, medium for one feature and low for two features. Table 2 and Table 3 show the characterization summary of security threats using risk level parameters and a fuzzy approach, respectively.

4.2 Creation of a Taxonomy for Cloud Computing Security Threats

This study created a taxonomy for cloud computing security threats, elucidating security threats, affected cloud infrastructure, attack methods and mitigation techniques. Figure 3 shows the diagram for the taxonomy.

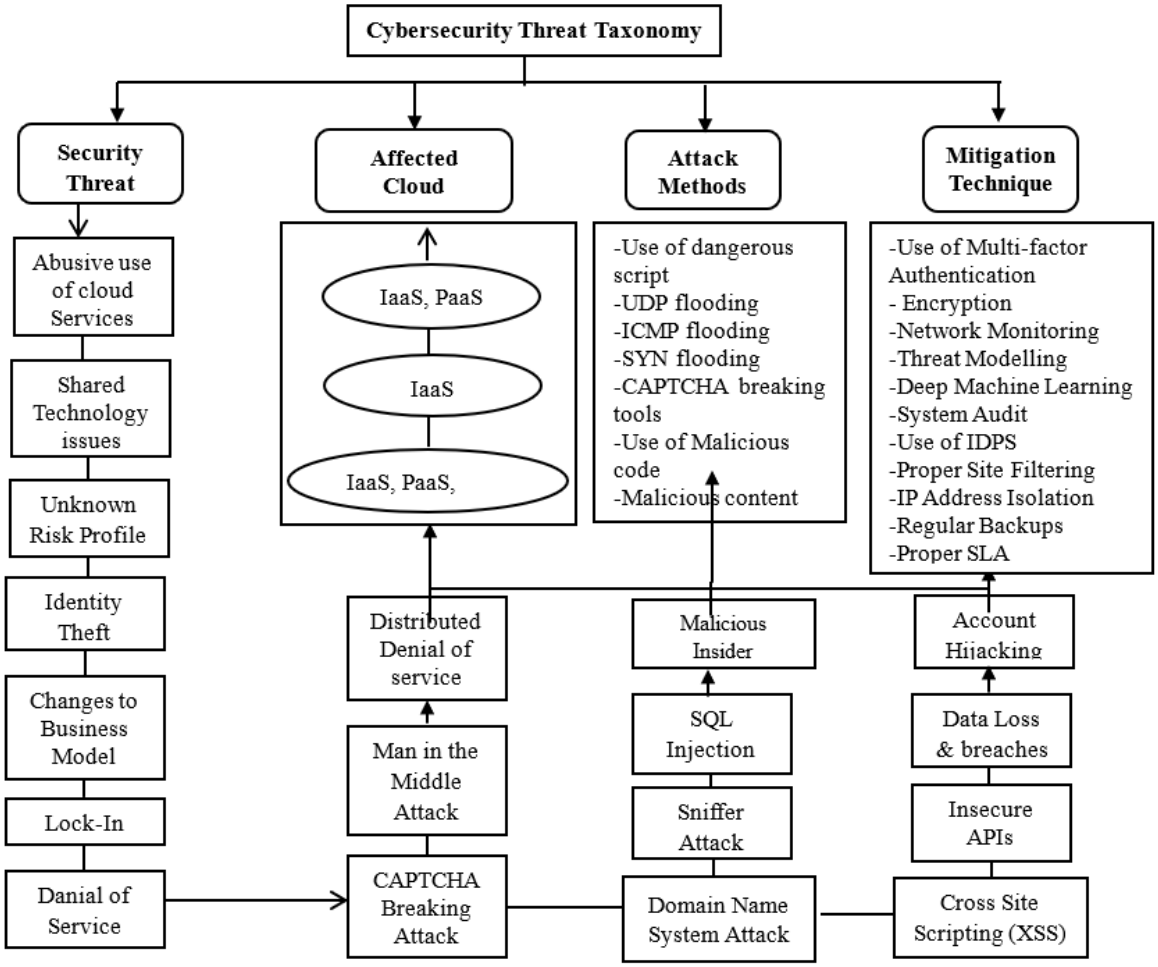

Figure 3. Taxonomy for cloud computing security threats

4.3 Available Threat Mitigation Techniques for Securing Cloud Computing Infrastructure

A comparative analysis was conducted on threat mitigation techniques such as STRIDE, PASTA, LINDDUN and others for securing cloud computing, aiming to find out the best techniques to eradicate the cybersecurity threat discovered in Section 4.1. Table 4 and Table 5 show the comparative analyses of threat mitigation techniques on 14 features using linguistic and numerical methods, respectively.

4.4 Comparative Analysis of Threat Modeling Techniques

The results of the comparative analysis of threat mitigation techniques are detailed in Table 4 and Table 5, which assess 14 features for rating the attributes of these approaches. STRIDE demonstrated high performance across 12 features, medium performance in one feature, and low performance in one feature. PASTA displayed high performance in 11 features, medium performance in one feature, and low performance in two features. LINDDUN provided high results in eight features, medium in four features, and low in two features. CVSS showed high results in seven features, medium in four, and low in three. Attack Tree achieved high results in five features, medium in six, and low in three. PnG demonstrated high performance in eight features, medium in four, and low in two. Security Cards provided

high results in eight features, medium in two features, and low in four. HTMM exhibited high results in five features, medium in four, and low in five features. QTMM presented high results in nine features, medium in three, and low in two features. Trike showed high results in six features, medium in six, and low in two features. VAST Modelling achieved high results in nine features, medium in three features, and low in two features, while OCTAVE exhibited high results in five features, medium in four, and low in five features. Therefore, STRIDE is the best technique for mitigating threats in cybersecurity, with a value of 59, followed by QTMM (57), CVSS (51), PASTA (50) and PnG (47). However, Attack Tree and HTMM have the same value of 46, followed by LINDDUN (45), OCTAVE (44) and Trike (43). Security Cards and VAST Modeling have the lowest value of 42. Numerical analysis was conducted using the data from Table 5 to determine the most effective threat mitigation techniques. Table 4 provides a detailed explanation of each feature for the respective threat mitigation technique, with each value represented across the rows in Table 5. Figure 4, Figure 5, Figure 6, Figure 7 and Figure 8 show the visual representation of some features against the mitigation techniques.

Table 4. Comparative analysis of threat mitigation techniques

		Threat Mitigation Techniques											
S/N	**Features**	**STRIDE**	**PASTA**	**LINDDUS**	**CVSS**	**Attack Tree**	**PnG**	**Security Cards**	**HTMM**	**QTMM**	**Trike**	**VAST Modelling**	**OCTAVE**
1	Documentation	EHD	HD	HD	LD	LD	LD	LD	LD	LD	LD	HD	LD
2	Technical threat identification	HS	HS	MS	LD	LD	LD	LD	S	LD	S	S	MS
3	Non-technical threat identification	HS	S	S	HS	HS	S	S	MS	HS	MS	MS	MS
4	General threat identification	VE	VE	ME	VE	VE	E	E	VE	VE	ME	E	E
5	Time consumption	C	ETC	HC	TC	TC	LTC	TC	HC	TC	ETC	HC	LTC
6	Usage	VEtU	DtU	EtU	MEtU	MEtU	VEtU	EtU	EtU	MEtU	EtU	VEtU	MEtU
7	Model maturity	HM	MM	MM	MM	MM	MM	LM	MM	HM	MM	MM	MM
8	Training/usage requirements	RLT	RMT	RMT	RMoT	RMoT	RMT	RMoT	RMoT	RMoT	RMoT	RMT	RMT
9	Business impact	L	EH	L	M	M	M	M	L	M	M	H	H
10	Security properties	EH	VH	VH	H	VH	H	H	VH	EH	VH	H	VH
11	Threat classification	VE	E	E	HE	E	E	HE	E	HE	E	E	NE
12	Stakeholders' input/collaboration	VHC	EHC	HC	NC	NC	HC	EHC	NC	VHC	HC	HC	LC
13	Threat prioritization	MP and ME	EHP and HE	HP and ME	EHP and HF	MP and ME	HP and ME	HP and ME	MP and ME	EHP and HE	MP and ME	MP and ME	LP and NE
14	Reliability	HR	HR	MR	HR	MR	MR	ELR	LR	HR	HR	HR	HR

Note: EHD = Extremely High Documentation, HD = High Documentation, LD = Less Documentation, HS = Highly Suitable, S = Suitable, MS = Moderately Suitable, VE and HE = Very Efficient and Highly Efficient, E = Efficient, ME = Moderately Efficient, NE = Not Efficient, HTC = High Time Consuming, ETC = Extremely Time Consuming, TC = Time Consuming, LTC = Less Time Consuming, VEtU = Very Easy to use, EtU = Easy to Use, MEtU = Moderately easy to use, DtU = Difficult to use, M = High Maturity, MM = Medium Maturity, LM = Low Maturity, EH = Extremely High, VH = Very High, H = High, EHC = Extremely High Collaboration, VHC = Very High Collaboration, HC = High Collaboration, NC = No Collaboration, EHP and HE = Extremely High Prioritization and Highly Efficient, HP and ME = High Prioritization and More Efficient, MP and ME = Medium Prioritization and Moderately Efficient, LP and NE = Low Prioritization and Not Efficient, HR = Highly Reliable, MR = Moderately Reliable, LR = Low Reliability, ELR = Extremely Low Reliability.

Table 5. Comparative analysis of threat mitigation techniques based on fuzzy set analysis in Table 2

		Threat Mitigation Techniques											
S/N	**Features**	**STRIDE**	**PASTA**	**LINDDUS**	**CVSS**	**Attack Tree**	**PnG**	**Security Cards**	**HTMM**	**QTMM**	**Trike**	**VAST Modelling**	**OCTAVE**
1	Documentation	5	4	4	2	2	2	1	4	1	2	4	2
2	Technical threat identification	5	5	3	5	5	5	5	2	5	2	2	3
3	Non-technical threat identification	5	3	3	5	5	3	3	4	5	4	4	4
4	General threat identification	5	5	4	5	5	3	3	5	5	4	3	3
5	Time consumption	2	1	2	3	3	4	3	4	3	1	1	4
6	Usage	5	1	3	4	4	5	3	3	4	3	5	4
7	Model maturity	5	3	4	3	3	3	2	4	5	3	3	4
8	Training/usage requirements	5	2	3	4	4	3	4	4	4	4	3	3
9	Business impact	1	5	2	3	1	3	1	2	3	3	4	4
10	Security properties	5	4	4	3	4	3	3	5	5	4	3	4
11	Threat classification	5	3	3	4	3	3	4	3	4	3	3	1
12	Stakeholders' input/collaboration	4	5	3	1	1	3	5	1	4	3	3	2
13	Threat prioritization	3	5	4	5	3	4	4	3	5	3	3	2
14	Reliability	4	4	3	4	3	3	1	2	4	4	4	4
15	**Total**	**59**	**50**	**45**	**51**	**46**	**47**	**42**	**46**	**57**	**43**	**42**	**44**

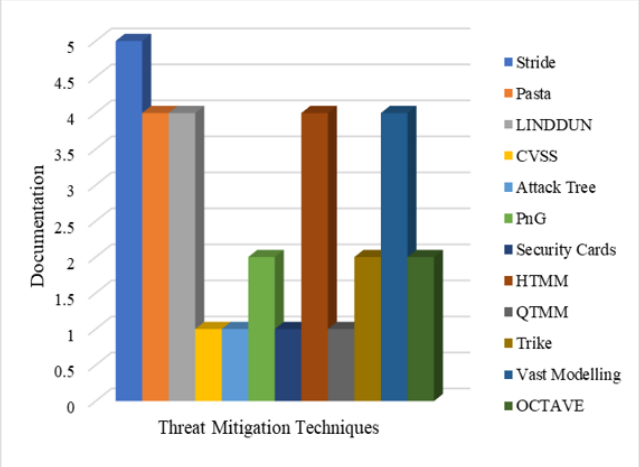

Figure 4. Comparative analysis of documentation

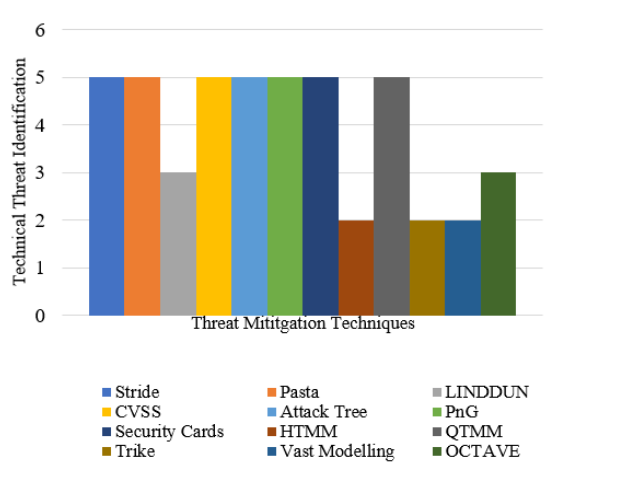

Figure 5. Comparative analysis of technical threat identification

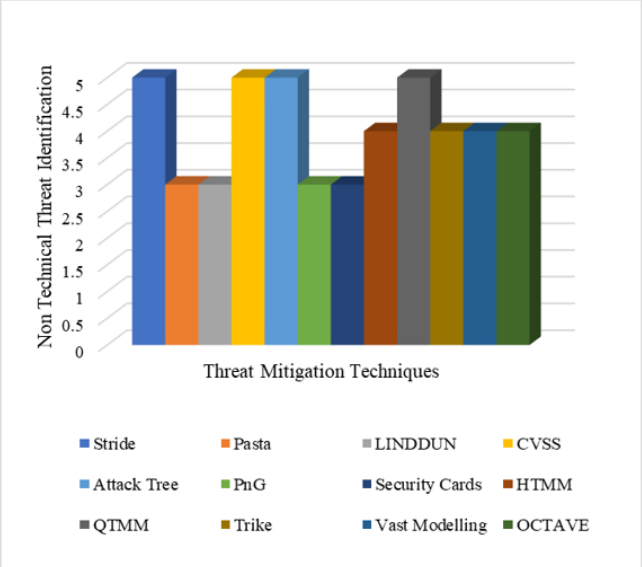

Figure 6. Comparative analysis of non-technical threat identification

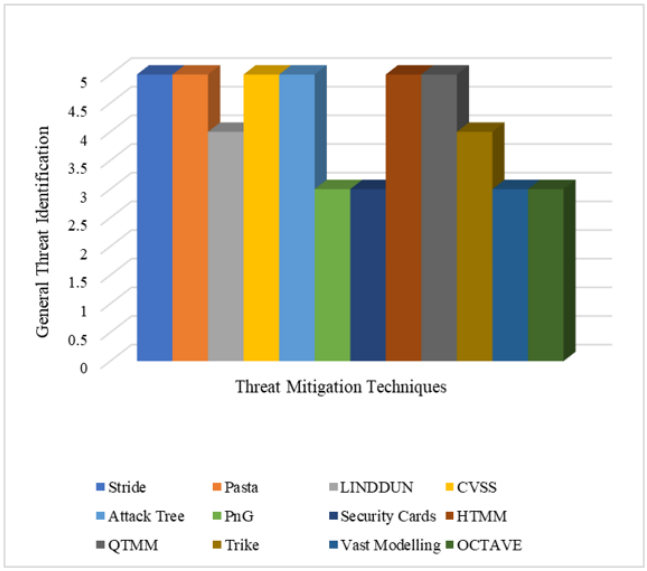

Figure 7. Comparative analysis of general threat identification

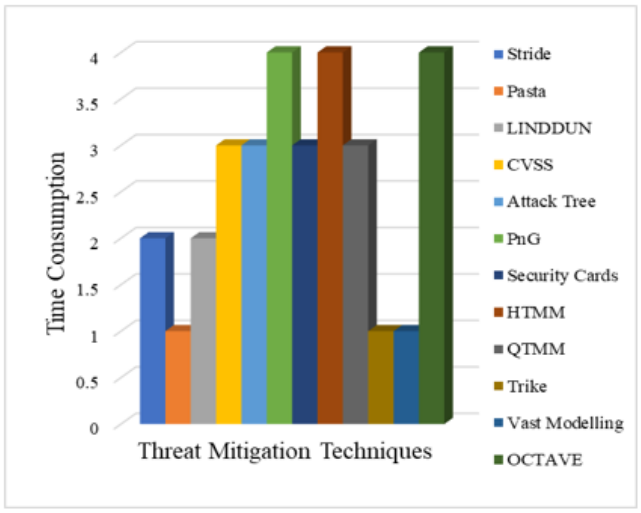

Figure 8. Comparative analysis of time consumption

5 Discussion

Organizations can now rent cloud infrastructure and computing capabilities from third-party providers rather than building on-premises IT infrastructure or leasing data center space. However, the transition to this new paradigm may be hampered by cloud tenants with different security and privacy concerns and the lack of underlying cloud infrastructure transparency. Therefore, security policymakers have been emphasizing the need to protect the cloud infrastructure, ICT systems and applications against cyberattacks.

According to the comparison results of threat mitigating techniques in cybersecurity using 14 features, considering the 12 threat modeling techniques, STRIDE has the highest value based on fuzzy set analysis, as shown in Table 5.

It is noteworthy that the major causes of cybersecurity threats are undeserved operations conducted by users, unknown cloud storage, unlawful acts of users, usage of the same VM by multiple users, operating system failure and following internal security measures, with each having the highest value of 4.75 among the causes of cybersecurity threats. The least common causes are natural disasters and exposure to sensitive information with a value of 3.75. This implies that natural disasters should not be given much concern for IaaS in the cloud environment. However, the most prominent feature to consider in threat mitigation techniques is general threat identification because it has the highest value of 50 among the threat mitigation features. The least prominent feature of cyberthreat mitigation is time consumption, with a value of 31, indicating that time consumption should not be considered an important feature in threat mitigation techniques.

The STRIDE is the best technique for mitigating threats in cybersecurity, with a value of 59, followed by QTMM (57), CVSS (51), PASTA (50) and PnG (47). This corroborates the findings by Yeng et al. [37], which show that STRIDE gathers high-level security requirements for cloud computing. However, Attack Tree and HTMM have the same value of 46, followed by LINDDUN (45), OCTAVE (44) and Trike (43). Security Cards and VAST modeling have the lowest value of 42.

5.1 Limitations of the Study

Instead of considering risk mitigation concerning PaaS and SaaS, this study only considers cloud risk mitigation in IaaS. Considerations could be given to other ranking methods such as the Preference Ranking Organization Method for Enrichment Evaluation (PROMETHEE), Elimination Et Choice Translating Reality (ELECTRE) and VIKOR to avoid subjectivity in selecting the best cyberthreat mitigation techniques.

6 Conclusions

With the rise of cloud computing, users, practitioners, and providers have become concerned about cloud security. Cloud platforms have become popular as a result of advancements in machine learning, deep learning techniques and cloud computing power. More and more third-party cloud services are being adopted, such as IaaS, SaaS and PaaS, bringing about security challenges in cloud computing that require efficient mitigation.

According to existing studies, organizations and cloud service providers have established numerous controls to assure data security and protection. However, such procedures entail numerous constraints that most cloud service providers are hesitant to impose, since they are likely to reduce the efficiency of cloud access.

This study utilized fuzzy set theory and threat modeling techniques to categorize cybersecurity threats within the cloud computing environment. It was concluded that STRIDE is the best for mitigating cybersecurity threats. The limitation of the study can be addressed by considering other forms of cloud computing, such as PaaS, and SaaS within the context of cybersecurity mitigation techniques.

The outcome of this study helps business organizations and cyber security experts take into account the frequently occurring threats and see how to mitigate them before they hamper the business's day-to-day operations. Apart from fuzzy set theory and numerical analysis, other ranking analysis methods regarding risk such as PROMETHEE, ELECTRE and VIKOR, and other threat mitigation methods such as Threat Modeling in Pervasive computing (TMP) and Practical Threat Analysis (PTA) could be considered for further studies.

Author Contributions

This research is the result of collaborative efforts by all the authors. "Conceptualization, Awodele, Ogbonna, Hinmikaiye and Akinsola; methodology, Ogu, Hinmikaiye and Akinsola; software, Ogu and Hinmikaiye; validation, Akinsola; formal analysis, Awodele and Ogbonna; investigation, Ogu and Hinmikaiye; resources, Awodele and Ogbonna; data curation, Ogu, Hinmikaiye and Akinsola.; writing—original draft preparation, Hinmikaiye and Akinsola; writing—review and editing, Awodele, Ogu, Hinmikaiye and Akinsola; visualization, Ogu and Akinsola.; supervision, Awodele, Ogbonna and Ogu; project administration, Hinmikaiye and Akinsola. All authors have read and agreed to the published version of the manuscript."

Data Availability

The data used to support the research findings are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] H. Azam, M. A. Tajwar, S. Mayhialagan, A. J. Davis, C. J. Yik, D. Ali, and S. R. Sindiramutty, "Innovations in security: A study of cloud computing and IoT," *Int. J. Emerg. Multidiscip. Comput. Sci. Artif. Intell.*, vol. 2, no. 1, 2023. https://doi.org/10.54938/ijemdcsai.2023.02.1.252

[2] A. Ethan and K. Khan, "Security challenges in cloud computing: A comprehensive overview," Ph.D. dissertation, University of California, USA, 2023.

[3] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity threats and their mitigation approaches using machine learning—A review," *J. Cybersecur. Priv.*, vol. 2, no. 3, pp. 527–555, 2022. https://doi.org/10.3390/jcp2030027

[4] S. Achar, "An overview of environmental scalability and security in hybrid cloud infrastructure designs," *Asia Pac. J. Energy Environ.*, vol. 8, no. 2, pp. 39–46, 2021. https://doi.org/10.18034/apjee.v8i2.650

[5] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," *Futur. Gener. Comput. Syst.*, vol. 79, pp. 849–861, 2018. https://doi.org/10.1016/j.future.2017.09.020

[6] S. Ahmadi, "Zero trust architecture in cloud networks: Application, challenges and future opportunities," *J. Eng. Res. Rep.*, vol. 26, no. 2, pp. 215–228, 2024. https://doi.org/10.9734/jerr/2024/v26i21083

[7] H. Moneer, M. Molik, and K. Khan, "Identity and access management in cloud environments: Security challenges and solutions," 2013. https://www.researchgate.net/publication/372448430

[8] M. Faheem, U. Akram, I. Khan, S. Naqeeb, A. Shahzad, and A. Ullah, "Cloud computing environment and security challenges: A review," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 10, 2017. https://doi.org/10.14569/ijacsa.2017.081025

[9] R. Ansari, P. Dehghani, M. Mahdikhani, and J. Jeong, "A novel safety risk assessment based on fuzzy set theory and decision methods in high-rise buildings," *Buildings*, vol. 12, no. 12, p. 2126, 2022. https://doi.org/10.3390/buildings12122126

[10] T. Theodoropoulos, L. Rosa, C. Benzaid, P. Gray, E. Marin, A. Makris, L. Cordeiro, F. Diego, P. Sorokin, M. D. Girolamo, P. Barone, T. Taleb, and K. Tserpes, "Security in cloud-native services: A survey," *J. Cybersecur. Priv.*, vol. 3, no. 4, pp. 758–793, 2023. https://doi.org/10.3390/jcp3040034

[11] "Threat modeling resources from shostack associates," *Shostack*, 2023. https://shostack.org/resources/whitepapers

[12] B. K. Joshi, M. K. Shrivastava, and B. Joshi, "Security threats and their mitigation in infrastructure as a service," *Perspect. Sci.*, vol. 8, pp. 462–464, 2016.

[13] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *J. Manuf. Syst.*, vol. 47, pp. 93–106, 2018.

[14] M. E. Paté-Cornell, M. Kuypers, M. Smith, and P. Keller, "Cyber risk management for critical infrastructure: A risk analysis model and three case studies," *Risk Manag.*, vol. 38, pp. 226–241, 2017.

[15] R. Ivanova, "ISO 31000 - Prerequisite for strategic risk management in the activities of organizations," *Izvestia J. Union Sci. Varna*, vol. 10, no. 1, pp. 55–62, 2021.

[16] H. Alawneh, "Android malware detection using data mining techniques on process control block information," Ph.D. dissertation, Auburn University, 2020. https://etd.auburn.edu/xmlui/handle/10415/7390

[17] "Malware & PUA," *AV-ATLAS*, 2024. https://portal.av-atlas.org/malware

[18] F. M. K. Quimba, M. A. A. Barral, and J. C. T. Carlos, "Analysis of the fintech landscape in the philippines," 2021. https://www.pids.gov.ph/publication/research-paper-series/analysis-of-the-fintech-landscape-in-the-philippines

[19] M. K. Ahsan, "Increasing the predictive potential of machine learning models for enhancing cybersecurity," *NDSU Repository*, 2020. https://hdl.handle.net/10365/32291

[20] R. Buch, D. Ganda, P. Kalola, and N. Borad, "World of cyber security and cybercrime," *Recent Trends Program. Lang.*, vol. 4, no. 2, pp. 18–23, 2017.

[21] V. E. Urias, B. Van Leeuwen, W. M. Stout, and H. Lin, "Applying a threat model to cloud computing," in *2018 International Carnahan Conference on Security Technology*, Montreal, Canada, 2018, pp. 1–5.

[22] T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information security risk assessment methods in cloud computing: Comprehensive review," *J. Comput. Inf. Syst.*, pp. 1–28, 2024.

[23] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29 775–29 818, 2021.

[24] N. Amara, H. Zhiqui, and A. Ali, "Cloud computing security threats and attacks with their mitigation techniques," in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Nanjing, China, 2017, pp. 244–251.

[25] T. Diaby and B. B. Rad, "Cloud computing: A review of the concepts and deployment models," *Int. J. Inf. Technol. Comput. Sci.*, vol. 9, no. 6, pp. 50–58, 2017.

[26] R. Sharma and R. Arya, "Secure transmission technique for data in IoT edge computing infrastructure," *Complex Intell. Syst.*, vol. 8, pp. 3817–3832, 2022.

[27] C. Chandgude and G. Gadekar, "Core of cloud computing," *Int. J. Eng. Res. Appl.*, vol. 7, no. 4, pp. 76–81, 2017.

[28] K. E. Akinola and A. A. Odumosu, "Threat handling and security issues in cloud computing," *Int. J. Sci. Eng. Res.*, vol. 6, no. 11, pp. 1371–1385, 2015.

[29] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Comput. Secur.*, vol. 49, pp. 70–94, 2015.

[30] H. Saini, A. Upadhyaya, and M. K. Khandelwal, "Benefits of cloud computing for business enterprises: A review," in *Proceedings of International Conference on Advancements in Computing & Management*, Jaipur, India, 2019, pp. 1003–1007.

[31] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," in *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance*, Auckland, New Zealand, 2018, pp. 1–6. https://doi.org/10.1109/AVSS.2018.8639152

[32] M. Dawood, S. S. Tu, C. B. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, "Cyberattacks and security of cloud computing: A complete guideline," *Symmetry*, vol. 15, no. 11, pp. 1–33, 2023. https://doi.org/10.3390/sym15111981

[33] J. Moura and H. David, "Review and analysis of networking challenges in cloud computing," *J. Netw. Comput. Appl.*, vol. 60, pp. 113–129, 2016. https://doi.org/10.1016/j.jnca.2015.11.015

[34] J. E. T. Akinsola, E. A. Olajubu, and G. A. Aderounmu, "Development of threat hunting model using machine learning algorithms for cyber attacks mitigation," in *2022 International Conference on Computational Science and Computational Intelligence*, Las Vegas, USA, 2022, pp. 1011–1016. https://doi.org/10.1109/CSCI58124.2022.00242

[35] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal, "Threat modeling for cloud data center infrastructures," in *Foundations and Practice of Security. FPS 2016. Lecture Notes in Computer Science*. Springer, 2017. https://doi.org/10.1007/978-3-319-51966-1_20

[36] J. W. Rittinghouse and J. F. Ransome, *Cloud Computing - Implementation, Management, and Security*. CRC Press, Taylor Francis Group, 2019.

[37] P. K. Yeng, S. D. Wulthusen, and B. Yang, "Comparative analysis of threat modeling methods for cloud computing towards healthcare security practice," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 11, pp. 772–784, 2020. https://doi.org/10.14569/IJACSA.2020.0111194