



## Potential Security Issues in Implementing IaaS and PaaS Cloud Service Models

Wishnu Kusumo Agung Erlangga\*, Muhammad Rheza Ramadhan\*\*

\*University of Glasgow, United Kingdom

\*\*Australia National University, Australia

\*Corresponding Email: wishnukaerlangga@gmail.com

### ABSTRACTS

As the digital world evolves, so does potential problem that computer users encounter. Cybersecurity threats are still evolving and expanding. Unfortunately, most computer users do not understand this properly. The cloud models offered by various public cloud providers remain concentrated on infrastructure resources, application platforms, and software services despite the recent increase in the popularity of cloud computing. The first step in this study will be a literature review to get an understanding of accessible cloud service models. The papers chosen for the study spans 2010 to 2020. All data was gathered from pertinent and related literature on cyber security and cloud computing. The following tenets serve as the foundation for this architecture. First, in the described architecture, the perimeter scanner serves as the first entry point for external cyberattacks. Firewall and other security layers become next barriers if the attack can get past first layer. On the other side, the machine learning system will detect every successful assault that gets past the security layers. As a result, there are numerous viewpoints and categorization systems for diverse attacks. It is possible to advance cyber security research in the context of cloud technology by merging the results of existing studies and developing international guiding standards.

### ARTICLE INFO

**Article History:**

Received 18 Dec 2022

Revised 20 Dec 2022

Accepted 25 Dec 2022

Available online 26 Dec 2022

**Keywords:**

Cloud computing,  
Cloud service model,  
Cyber security,  
Cyber-crime,  
Cloud security framework,  
Machine Learning,  
MITM, MITB,  
Microsoft Azure

## 1. BACKGROUND

Despite the recent explosion in popularity of cloud computing, the cloud models provided by different public cloud providers continue to be focused on three service tiers: infrastructure resources, application platforms, and software services. Even though, according to Coppolino et al. (2017), Jang-Jaccard & Nepal (2014), cyber security dangers are developing and changing. Unfortunately, computer users typically do not follow this up with proper comprehension. Modest businesses are still often believed to be immune to cracker assaults because of their small size and lack of important data. In the United States, up to 56% of small business owners said they were unconcerned about falling prey to hacking (CNBC, 2021). According to a survey conducted by Proofpoint (2019) over millions of tracked cloud user accounts, 72% of cloud users have been the target of villains, which at least one incident had been experienced by 40% of them. In fact, during the same time period, 43% of firms experienced ten or more breaches.

According to a poll of 400 IT decision-makers from small and medium-sized enterprises, 74% of workers find it difficult to follow adequate security practises when working remotely (Help Net Security, 2021).

Unfortunately, researchers have started to see cloud security systems as a cohesive entity comprising the perspectives of cloud vendors and cloud clients, which has attracted them inadequate attention. The private IaaS and PaaS cloud environment are the subject of this project's research. In this study, we tried to answer two questions.

First, what effects do the adoption of IaaS or PaaS cloud service models have on cyber security? Second, how do researchers learn about IaaS and PaaS security vulnerabilities and threats?

To better understand the relationship between cloud service models and cyber security, this study examined those two cloud service models and looked into the consequences of those models' implementation.

## 2. STUDY CONTEXT AND LITERATURE SURVEY

Virtual machines (VMs) are used in cloud computing (Microsoft, 2021a) as the virtual equivalent of desktop or laptop. The ability to create many VMs connected by a separate Virtual Network is made possible by cloud computing (VN). According to Kaelin (2019; Microsoft, 2021b), VN is an isolated and private environment to connect and execute VMs, including database applications. It is used to create communication channels between cloud resources, including the on-premises machines of tenants.

This study examines two cyberattacks: Man-In-The-Middle (MITM) and Man-In-The-Browser (MITB). A MITM cyberattack involves an outsider who unwittingly lies to two parties in order to learn or even alter the information shared between them (Mallik et al., 2019). Based on (OWASP, n.d.), MITB employs a similar strategy but adds a Trojan Horse to learn about and alter the connection between two parties using the target's browser.

The following system is used to conduct various experiments linked to this

research in order to demonstrate some of the critiques that can be made of this paper:

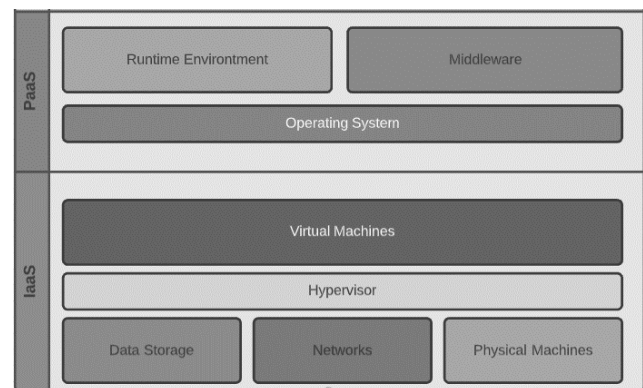
- 1) MITM assault: ARP Poisoning as the method, Kali Linux as the operating system, and Ettercap version 0.8.3.1 was the application;
- 2) MITB assault: XSS Hooking and Javascript Injection method, Kali Linux was the operating system as well and the application used was BeEF version 0.5.3.0.

## 2.1. Cloud Service Models

Cloud servers have virtual data centres as one of their features. The same idea governs how cloud computing services work: they offer users on-demand online computing based on their needs. IaaS is a cloud model that gives users the ability to create their own computer systems using the resources that have been made available. IaaS solutions give businesses the ability to create and maintain computing infrastructure, such as servers, networks, and data storage. This paradigm handles computing resources like memory, data centres, and network storage as a provisioning service (Subashini & Kavitha, 2011). Scalability and infrastructure provision are provided by IaaS.

PaaS is a cloud service model that enables users to execute development and deployment utilising any resources made available by the cloud provider. It can be said that IaaS is the most basic form of cloud while PaaS adds runtime environment and an operating system to it. Therefore, everything that is controlled by the IaaS directly underneath PaaS will always be included. The availability of middleware is another essential

requirement for PaaS. Middleware acts as a bridge between the operating system and the programmes it runs. Similar to a water pipe connecting two areas to guarantee that water flows smoothly to its destination, it links one platform to another platform. The conceptual alignment between the IaaS and PaaS cloud models is shown in Fig. 1. Layers of IaaS and PaaS.



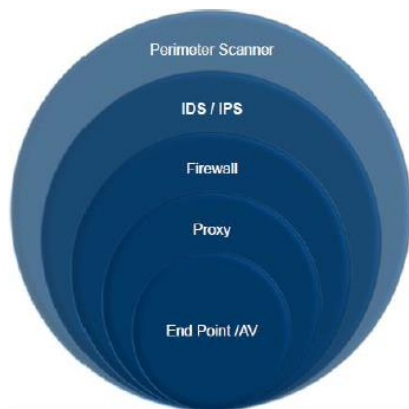
**Fig. 1. Layers of IaaS and PaaS**

During the COVID-19 pandemic, as online services become increasingly dependable as a means of communication, many cybercrimes target consumers. The emergence of SECaaS is related to the rising popularity of cloud computing. It provides security in a separate way for cloud operations, data, and applications. Additionally, it encourages the use of new security architectures with adaptable and affordable protection measures (Hawedi et al., 2018).

## 2.2. Cloud Security

Three components make up a well-known cyber security model: confidentiality, integrity, and availability (CIA). NIST's definitions of confidentiality state that maintaining authorised constraints on information access and disclosure, as well as

safeguards for individual privacy and privileged information, constitutes sustaining confidentiality. Integrity encompasses safeguarding against unauthorised data change or loss as well as ensuring the veracity and non-repudiation of data. The last attribute is availability, which denotes the capability of authorised individuals to access (and modify) data whenever necessary. Evangelopoulou provided one illustration of a tiered security system (2021). Because it includes a failsafe, layered cyber security makes this method look like an onion. As seen in Fig. 2. Cybersecurity Defense Mechanism with Layers, the mechanism being discussed may encompass several forms of defence as can be seen below.



**Fig. 2. Cybersecurity Defense Mechanism with Layers**

However, De Donno et al. (2019) put the operating system to IaaS while PaaS and SaaS were integrated in one layer. They see the network layer as a part of the physical layer rather than a separate entity.

According to (Campfield, 2021), major cloud service providers like Microsoft Azure, Google Cloud Platform, and Amazon Web Service (AWS) are responsible for protecting the cloud infrastructure, while cloud users are responsible for protecting their own data. While tenants are in charge of maintaining security "in the cloud," they are responsible for protecting users "at the cloud."

### 2.3. Risks to Cloud Security

A number of risks serve as security gaps (Almorsy et al., 2010). Security issues for cloud models, according to Tchifilionova (2010) are not limited to viruses or trojans types. The two researchers' assertion appears to be supported by the numerous types of attacks that take place. Table 1 lists cyber security dangers and assaults that have been incorporated into IaaS and PaaS service models from 2010 to 2020 in accordance with the study's purview. The codes started with JA stands for Journal Articles.

**Table 1. Attacks/Threats in Cloud from Journal Articles**

Codes	Journal Title and Authors	Types of Attacks/Threats
JA1	An Analysis of The Cloud Computing Security Problem (Almorsy et al., 2010)	DoS
		MITM
		Injection Attack

		Dictionary Attack
		XML-Related Attack
		Replay Attack
		Malware/Viruses
		DDoS
		Hypervisor Security Breach
		Virtual Network Attack
		Virtual Machine Attack
JA2	Cloud Computing Security Considerations (A. Tripathi & A. Mishra, 2011)	Hypervisor Security Breach
		Phishing, Fraud, & Software Vulnerabilities
JA3	A survey on security issues in service delivery models of cloud computing (Subashini & Kavitha, 2011)	DoS
JA4	Security Issues and Solutions in Cloud Computing (You et al., 2012)	Data Breach
		Data Lock-in
		Data Remanence
		Virtual Machine Attack
		DoS
JA5	Cloud-based DDoS Attacks and Defenses (M. Darwish et al., 2013)	DoS
		DDoS
JA6	Cloud Computing: Security and Reliability Issues (Ahamed et al., 2013)	DoS
		DDoS
		Side Channel Attack
		Malware/Viruses
		Virtualisation Leakage
		Insider Attack
JA7	A survey of security issues for cloud computing (Khan, 2016)	Port Scanning
		Data Scavenging
		Spoofing
		Virtual Machine Attack
JA8	Web Services Attacks and Security- A Systematic Literature Review (Mouli & Jevitha, 2016)	DoS
		Spoofing
		XML Injection
JA9	A survey on cloud computing security: Issues, threats, and solutions (Singh et al., 2016)	DoS
		Data Loss
		Data Leakage
		Data Manipulation
JA10	Analisis Teknik-Teknik Keamanan Pada CloudComputing dan NEBULA (Future Cloud): Survey Paper (Nugraha, 2016)	Snooping Attack
		DoS
		MITM
JA11		Data Loss
		Data Leakage

	Data Security is the Major Issue in Cloud Computing - A Review (Monika & Y., 2016)	Virtual Machine Attack
		MITM
		DoS
		DDoS
		Malware
JA12	On cloud security attacks: A taxonomy and intrusion detection and prevention as a service (Iqbal et al., 2016)	Side Channel Attack
		Virtual Machine Attack
		Phishing
		MITM
		Cloud Malware Injection Attack
JA13	Identity and access management in cloud environment: Mechanisms and challenges (Indu et al., 2018)	Brute Force Attack
		Virus/Malware
		Virtual Machine Attack
		MITM
		Replay attack
		Session/cookie hijacking
		DoS
		DDoS
JA14	Identifying the Top Threats in Cloud Computing and Its Suggested Solutions: A Survey (Kofahi & Al-Rabadi, 2018)	Data Loss
		Data Breaches
		Account or Service Hijacking
		DoS
JA15	Recent security challenges in cloud computing (Subramanian & Jeyaraj, 2018)	Snooping Attack
		Address Spoofing
		Hypervisor Security Breach
		Side Channel Attack
		Virtual Machine Attack
JA16	Security In Cloud Computing: A Survey (Alhenaki et al., 2019)	Phishing
		Port-Scanning Attack
		MITM
		Metadata Spoofing Attack
		Virtual Machine Attack
JA17	Security concerns and countermeasures in cloud computing: a qualitative analysis (Anjana & Singh, 2019)	Virtual Machine Attack
		Shared Resources
		Virtual Networks
		Hypervisor
JA18	Cyber-Storms Come from Clouds: Security of Cloud Computing in the IoT Era (De Donno et al., 2019)	Multi Tenancy
		Virtual Machine Attack
		MITM
		DDoS
		Injection flaws
		MITB
		XML Signature Element Wrapping
		Metadata Spoofing

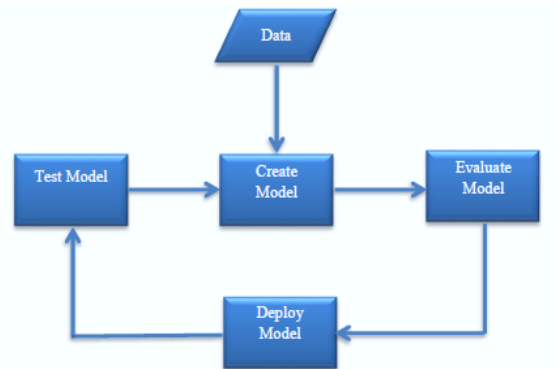
		<b>Application-Bug Level DoS</b>
JA19	Cyber security threats, challenges and defence mechanisms in cloud computing (Ahanger & Aljumah, 2020)	<b>MITM</b>
		<b>Sniffer Attack</b>
		<b>DoS</b>
		<b>DDoS</b>
		<b>Connection Flooding Attack</b>
		<b>Port Scanning</b>

The categorization of cyber security attacks and threats has remained uneven despite the wealth of literature on cloud security, by the fact that the variety of cyber security risk keeps expanding (Jang-Jaccard et al., 2014). Those who discuss numerous cyber security types of attacks make recommendations to hold against them in several different methods. Several options were thoroughly tested (S. Zaman et al., 2021).

Securing a cloud service aims to guarantee that everything created only performs as intended (Nunnikhoven, 2021). In order to integrate with the architectural architecture of the cloud, new security techniques must be developed (Carlin & Curran, 2011). As a result, more study is required to determine the current state of cloud computing security, and this article attempts to fill that gap.

#### 2.4. Cloud Security Using Machine Learning

This study considered Azure as the only object. The reason Azure was selected is that it offers the most adaptable machine learning (ML) platform to enable the capabilities in building, training, and implementing ML. As seen in Fig. 3, Nketah (2016) showed to us that Microsoft Azure also offers MLaaS based on a standard workflow.



**Fig. 3. Workflow for Azure Machine Learning**

### 3. METHOD

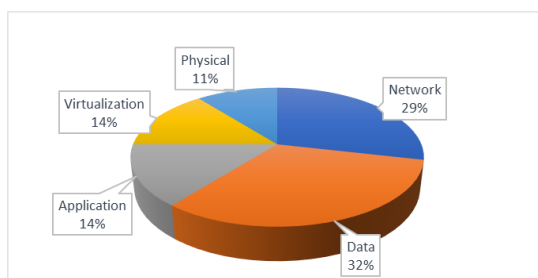
In qualitative research, the level of significance of the implications for cyber security incidents are represented in words and analysed through interpretations and categorization (Bhandari, 2020). A new insight can be gained by using qualitative methods to explain phenomena, come up with fresh concepts, or develop and test existing hypotheses (Fujs et al., 2019). The literary works included for the study span the years 2010 through 2020. In summary, we attempted to analyse the distinctions between IaaS and PaaS based on the body of literature already in existence from the perspective of a cyber-security incidents. To test our methods, we look for criticisms in relevant papers. By developing a novel model with one cloud service provider as a choice, this research also demonstrates the applicability of Machine Learning (ML) in cloud security. As a result, we concentrated on security

methods that have been utilised to address security issues in a cloud computing.

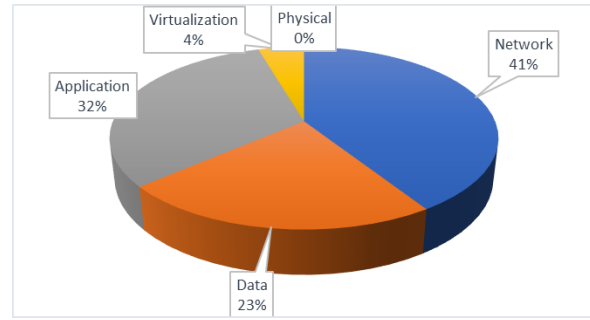
#### 4. RESULTS AND DISCUSSION

##### 4.1. Secure Cloud Services

As previously indicated, the capabilities and security issues of the cloud model underneath it will be inherited by the cloud service models. We contend that five security levels may be utilised in attacks on the IaaS and PaaS tiers. The virtual layer, physical layer, data storage layer, application layer, and network layer. In terms of their definitions, the five layers are as follows: Physical layer, where all the hardware required to run cloud services is located (NIST, 2018). Virtualization layer, which divides infrastructure resources into virtual computers known as Virtual Machines (Fitzek et al., 2020). Data Storage layer consists of storage used to store data on the Internet. Lastly, Application layer itself. When viewed from the perspective of the attacker, figs. 4 and 5 demonstrate how the proliferation of attacks in each tier of security.



**Fig. 4. Responsibility Assumed by the Cloud Provider for Each Security Layer**



**Fig. 5. Cloud User's Responsibility Percentage for Each Security Layer**

Cloud service providers focus mostly on threats that target the data layer. Most attacks on cloud tenants, however, take place at the network layer. Given that communication involves networking, which comprises the network interface layer and network access layer, this scenario is plausible (Evangelopoulou, 2021). Aside from that, cloud tenant is not potentially liable for any physical attacks. After all, they have control over the physical network and infrastructure. As a result, the security of the physical layer is entirely the responsibility of the cloud provider.

Then, in relation to the overall number of attacks included in this analysis, nearly every form of attack (84.8%) may be the responsibility of the cloud provider. In the meantime, 66.67% of the different sorts of attacks can be the fault of cloud tenants. One of the attack types for which the cloud provider is not liable is the "replay attack." This attack can be executed by monitoring messages delivered or received by cloud tenants. The seized message will then be sent back to the original recipient by the attacker. The recipient will presume that the reply message came from the trusted sender and will accede to the attacker's demands on faith. Other forms of attacks, that become cloud users' responsibility, can



be lessened in many ways, including the following: (Tables 2 and 3)

**Table 2. Cloud Users' Responsibility Types of Attacks**

No	Attacks/Threats	Mitigation
1	Phishing	<ul style="list-style-type: none"> <li>- Eliminating the use of static credentials to access web services (Indu et al., 2018)</li> <li>- Choose a database set such as phishtank.com and use it with SVM, Decision Tree, AdaBoost, or Random Forest (Mao et al., 2019)</li> </ul>
2	Spoofing	<ul style="list-style-type: none"> <li>- Using a network firewall</li> <li>- Setting up two-factor authentication (2FA)</li> </ul>
3	Session Hijacking	<ul style="list-style-type: none"> <li>- Using one-time cookies</li> <li>- Implementing protection mechanism against session hijacking such as "SessionShield" (Nikiforakis et al., 2011)</li> </ul>

**Table 3. Lowest Occurrence Rate of Cyber Attack based on Journal Articles**

Layer	Virtualisation	Network	Data	Application
<b>Attack / Threat</b>	<ul style="list-style-type: none"> <li>• Virtual Network Attack</li> <li>• Multi Tenancy</li> </ul>	<ul style="list-style-type: none"> <li>• Snooping Attack</li> <li>• Port Scanning</li> <li>• Sniffer Attack</li> <li>• Network Under-Provision</li> <li>• Connection Flooding</li> <li>• Traffic Analysis Attack</li> </ul>	<ul style="list-style-type: none"> <li>• Data Lock-In</li> <li>• Data Remanence</li> <li>• Data Manipulation</li> <li>• Data Deduplication</li> </ul>	<ul style="list-style-type: none"> <li>• Dictionary Attack</li> <li>• MITB</li> </ul>

The low occurrence rate might lead to a number of different causes. To begin with, cloud tenants rarely experience attacks of this nature. The impact of the attack is also less severe than DoS or DDoS, which result in physical harm (shutting down the service). Third, not many people are aware of the attack's nature. Fourth, because attack types are not standardised, it is challenging to group related attack types together. IaaS and PaaS-based cloud services continue to have a wide range of cyber security implications.

#### **4.2. Threats and Security Attacks Against IaaS and PaaS Cloud Models**

Because this service model only covers the most basic services, an IaaS cloud provider provides its tenants with the fewest security protections. A SaaS cloud provider, however, would offer the most services (Sosinsky, 2011). IaaS users should be aware of the requirement to offer sufficient security for the information and applications they deploy to the cloud. The cloud vendor bears a greater degree of responsibility in the PaaS model because tenants get a freedom implementing protection for their data in the applications. The operating system they employ serves the same purpose in helping them create their applications.

When expressing worries about cloud services' security, researchers differ from one another. Several of them have made their cyber security flaws public. Table 4 shows an attack pattern that spans different cloud security layers.

**Table 4. CIA Triad Indicators of Cyber Attacks/Threats on Cloud Models**

Attack Target Location	Attack Types	Cloud Models		Codes	Cyber Security Indicators
		IaaS	PaaS		
Physical	DoS	•	•	JA1, JA3, JA4, JA5, JA6, JA8, JA9, JA10, JA11, JA13, JA14, JA18, JA19	A
	DDoS	•	•	JA1, JA5, JA6, JA11, JA13, JA18, JA19	A
	Side-channel Attack	•	•	JA6, JA12, JA15	C, I, A
Data Storage	Malware	•	•	JA1, JA6, JA11, JA12, JA13	C, I, A
	Data Scavenging	•	•	JA7, JA17	C
	Data Loss	•	•	JA9, JA11, JA14	A
	Data Leakage	•	•	JA9, JA11	C
	Data Breaches	•	-	JA4, JA14	C, I
	Data Lock-In	•	•	JA4	A
	Data Remanence	•	-	JA4	C
Virtual	Data Manipulation	•	-	JA9	C
	Virtual Machine Attack	•	-	JA2, JA4, JA6, JA7, JA11, JA12, JA13, JA15, JA16, JA17, JA18	C, I, A
	Virtual Network Attack	•	-	JA1, JA17	C, A
	Hypervisor Security Breach	•	-	JA1, JA2, JA15, JA17	C, A
Network	Multi Tenancy	•	•	JA17, JA18	C, A
	XML-related attack	•	•	JA1, JA8, JA18	A
	Snooping Attack	•	-	JA10, JA15	C
	Port Scanning	•	-	JA7, JA18, JA19	C
	Sniffer Attack	•	•	JA19	C, I, A
	Connection Flooding	•	-	JA19	C
	Replay Attack	•	•	JA1, JA13	C

	MITM	•	•	JA1, JA10, JA11, JA12, JA13, JA16, JA18, JA19	C, I, A
Application	Phishing	•	-	JA2, JA12, JA16	C
	Spoofing	•	•	JA7, JA8, JA15, JA16, JA18	C, I
	Brute Force Attack	•	•	JA13	C, I
	Injection Attack	•	•	JA1, JA18	C, I, A
	Dictionary Attack	•	•	JA1	C, I
	Session Hijacking	•	•	JA13, JA14	C, I, A
	MITB	•	•	JA18D	C

A. B. Nassif et al., (2021) and Makkawi & Yousif (2020) claim that DDoS and DoS are the two most common types of cyberattacks. The frequency of incidence of assault kinds is shown in Table 4 reveals that the most frequent attacks are Virtual Machine Attack (48%) and DoS (71%).

This section tries to evaluate the data in Table 4. and to observe and describe how cyber security threats in the IaaS and PaaS model clouds have increasing and decreasing effects. The CIA triad in the given figure shows their impact on the cyber security layer. Fig. 6 shows the effects of cyber-attacks as mentioned in Table 4.

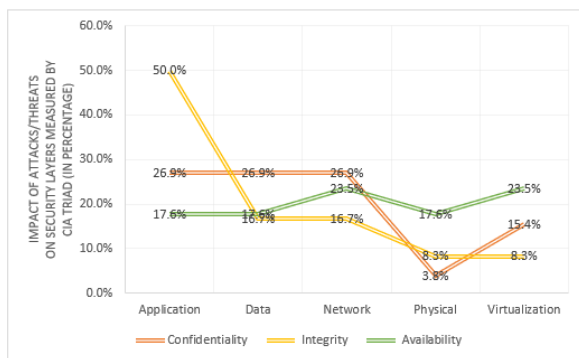


Fig. 6. Effect of Attacks on Security Layers.

As depicted in Fig. 6, the application level is where the most substantial effects of cyberattacks in the IaaS and PaaS cloud service models occur. Such attacks can be mitigated or prevented by several proactive measures, including robust authentication standards, hashing technology, encryption, or application updates. While only 3.8% of all current cyberattacks have a physical component, this is where confidentiality is least affected. The likelihood of it occurring is high since cyberattacks on the physical infrastructure of public cloud services will only take place on the premises of cloud service providers. Additionally, the physical restrictions on the cloud provider's authorization of access privileges to the cloud centre are very severe. For instance, Google has six layers of tight security to prevent unauthorised access to the Google Cloud Data Center area, starting with the most basic precautions like signage and fencing and moving up to smart fencing and thermal cameras on the second tier (Google Cloud Tech, 2020).

Attacks and threats on the CIA Triad component in Fig. 6 have varying degrees of impact. For instance, integrity at the data and network levels is where the lowest implication values are derived. The highest value for both levels has effects on the same side, notably confidentiality, at the same time. Due to a person's intense desire to discover the secret of confidential material, one might hypothesise that a high score on confidentiality is most often the result of hacking or social engineering, posing the risk of insufficient authentication or authorization.

The high number of attacks threatening the availability of virtualization are undoubtedly influenced by growing network and device deployment, as well as developer ignorance of the hypervisor code. A single management console's efficient management, monitoring, and configuration of VMs and VNs can lessen the risks they pose (A. Tripathi & A. Mishra, 2011).

From Table 1, we discovered fascinating information on the researchers' classification of the various cyberattacks. There is a lack of standardisation in the name and categorization of cyber-attacks when looking at the sorts of attacks in the researchers' findings above. For instance, some researchers include MITM kind of attack as a component of service-oriented architecture (Almorsy et al., 2010; Iqbal et al., 2016). While (Indu et al., 2018) put this attack into human-centered security due to an insecure SSL architecture. Interestingly, (De Donno et al., 2019) took this issue as a result of a lack of network security.

Even though the methodology used in MITM attacks and MITB attacks is the same (OWASP, n.d.), De Donno et al. (2019) distinguish between those two methods and classify MITM in network security level. Interesting distinction between the two is made by the method used. MITB can use trojans like Zeus when launching attacks. While MITM will employ a physical technique to access a Wi-Fi router, such as in public area, houses without sufficient security measures in place, or websites without an SSL certificate configured (use HTTPS).

To demonstrate that these two attacks operate at the same security level, the analysis below uses attacking experiments with MITM and MITB applications.

#### 1) MITM

IP Target : 10.0.2.2

Target URL : http://libgen.li

Method : MITM and ARP poisoning

Tool : Ettercap version 0.8.3.1

An illustration of the MITM attack is shown in Figs 7 and 8. The web server and the web browser connection is not protected when users check in to sites like http://libgen.li without an SSL certificate, making it possible for attackers to intercept sensitive data like usernames and passwords.

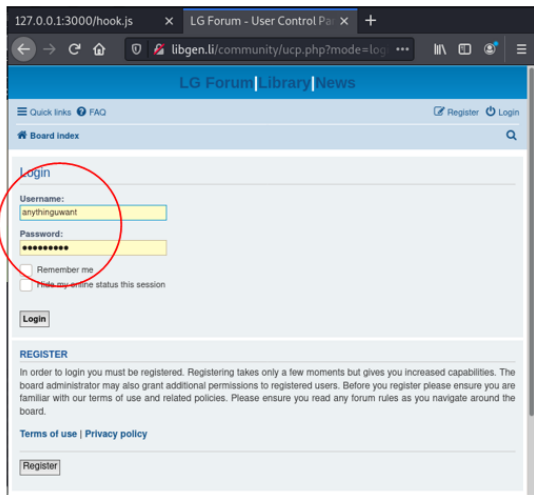


Fig. 7. Display of the Site Login Page at libgen.li

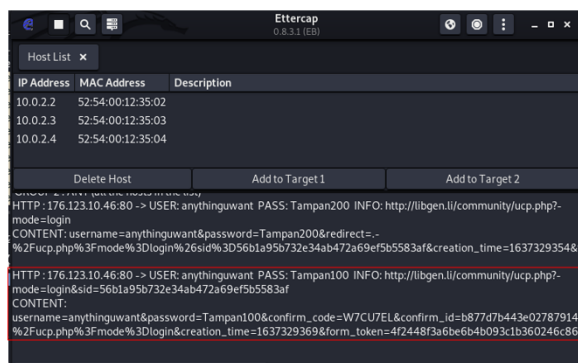


Fig. 8. Successful MITM Method Login Information Capture

The possible risks that MITM provides to targets are demonstrated in Figs. 7 and 8. The victim of the assault provided a username and password to <http://libgen.li> using the ARP Poisoning technique, which the MITM that was performed was able to retrieve using the Ettercap attack programme version 0.8.3.1. The MITM method may be used to attack cloud tenants with a more advanced strategy.

1) MITB

Google Chrome is the preferred browser

Method : XSS Hooking with Javascript Injection

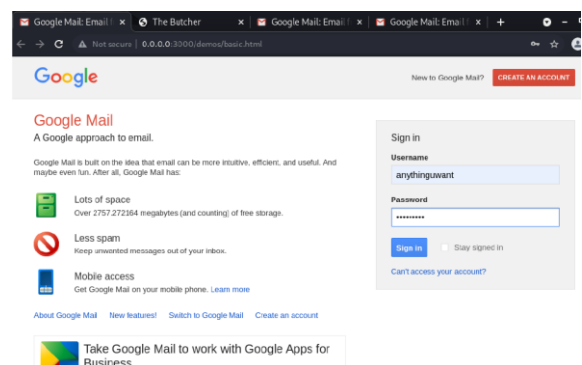
Tool : BeEF version 0.5.3.0

Fig. 9. shows an illustration of the MITB attack pattern. Unfortunately, in the experiment, MITB assaults could not be launched using the Zeus Trojan. On the other hand, the hook.js Trojan, which is utilised as a pilot in the BeEF application, might be used to conduct the MITB attack simulation. Figs. 9-11 show the simulation of the MITB assault.



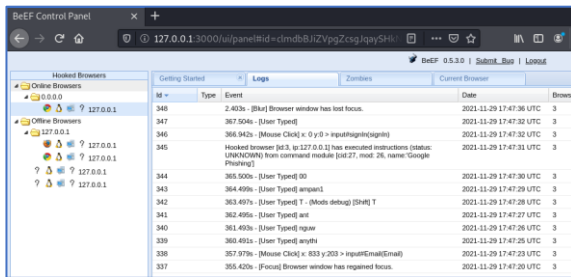
Fig. 9. Map of MITB Attack Using Hooked Browser and BeEF

Fig. 9 shows the position of the attackers in MITB. The hook.js Trojan was successfully installed by the attacker (BeEF) on the target's Google Chrome browser. The attacker could continue their operations after successfully hijacking the Chrome browser. As an example, as seen in Fig. 10, it was done by spoofing the target's Google Chrome browser with a Google Mail login page.



### Fig. 10. Webpage Phishing on MITB Attack

The target's information in the aforementioned example is username: anythinguwant and password: Tampan100. As seen in Fig. 11, the credential used could be noted in the BeEF application.



ID	Type	Event	Date	Browser
346	2.403s - [User Type] [Browser window has lost focus.		2021-11-29 17:47:36 UTC	3
347	367.504s - [User Type] [		2021-11-29 17:47:32 UTC	3
346	368.942s - [Mouse Click] x: 0 y: 0 => input[type=		2021-11-29 17:47:32 UTC	3
346	Hooked browser [id:3, to:127.0.0.1] has executed instructions (status: UNKNOWN) from command module [id:27, mod: 26, name: Google Phishing]		2021-11-29 17:47:31 UTC	3
344	365.500s - [User Type] [00		2021-11-29 17:47:30 UTC	3
343	364.499s - [User Type] [empan1		2021-11-29 17:47:29 UTC	3
342	363.497s - [User Type] [T - (Modes debug) [SH4] T		2021-11-29 17:47:29 UTC	3
341	362.496s - [User Type] [ent		2021-11-29 17:47:27 UTC	3
340	361.495s - [User Type] [ngaw		2021-11-29 17:47:26 UTC	3
339	360.491s - [User Type] [anyth		2021-11-29 17:47:25 UTC	3
338	357.979s - [Mouse Click] x: 633 y: 203 => input[Email>Email)		2021-11-29 17:47:23 UTC	3
337	355.420s - [Focus] [Browser window has regained focus.		2021-11-29 17:47:20 UTC	3

### Fig. 11. Information Retained on the Infected Chrome Browser

Via Fig. 11, MITB noted that the username and password used to attack the target were exactly the same as those used by the victim. As a result, the two attacks (MITM and MITB) may have a similar structure. The inference that may be made is that attacks like MITM and MITB can be executed at the same level, by taking advantage of network security flaws. The vulnerability results in packets being sent over the network, giving attackers access to view data traffic.

Then, as was already noted, the replay attack by uses the same attack strategy as MITM. It entails the presence of undesirable people in the communication path between the sender and the recipient. However, due to the lack of standardised knowledge of the consequences of cyber security, some people now view it as of human-centered security issue (Indu et al., 2018) while Almorisy et al. (2010), saw it from the

perspective of network security. In addition, DoS and XML attacks are distinguished by Almorisy et al. (2010). However, a closer look reveals that DoS is actually an assault on the XML parser. Therefore, we contend that these two ideas can be combined into one section, namely DoS.

Since the beginning of the relationship, the cloud service provider has been responsible for data security. As a result, tenants will be subject to local and international laws that are in force in the countries where the cloud service provider stores their data. However, if a data leak occurs while a tenant is using cloud computing services provided by a cloud provider, the tenant could still be held accountable for the data loss. A service that handles everything from physical security to environmental security to virtualization security is EC2, for instance. Tenants are in charge of all application- and data-related problems. The idea to include security as a form of cloud computing service (Forcepoint, 2019; Hawedi et al., 2018) seems like it could advance given the significance of cyber security risks.

### 4.3. Cloud Security as a Service

The security of PaaS and SaaS will also be impacted in the event of an attack on the IaaS platform (Hashizume et al., 2013). These interdependencies put these systems' security in jeopardy. solution offered by Hawedi et al. (2018) focuses on providing a security service that enables cloud tenants to keep an eye on their virtual machines (VMs) by putting in place a security mechanism that is tailored to their specific requirements.

The results of the initial examination show that researchers still lack a comprehensive manual on cloud service dangers and attacks. Using alarm signals as warnings, all forms of cloud system security services halt till the investigation stage. Therefore, the policies chosen by cloud tenants will dictate the subsequent actions. There is a danger involved in regarding secrecy or confidentiality. Data loss or leakage may occur while cloud tenants are deliberating how to proceed. In accordance with this, an ML system could be created as a further development in this situation.

#### **4.4. Technology & Tools for Cloud Computing Security**

In terms of security, more consideration should be given to cloud development. Several cloud services companies, including Amazon, Google, and Microsoft, presently offer MlaaS. The algorithm is capable of overcoming the attack pattern. Thus, the subsequent attack pattern will guide cloud security systems to function successfully. As a result, when the model is deployed, it can be used appropriately.

Microsoft Azure offers a variety of algorithms that users can carry out the most suitable predictive analytics tasks. Cyber threats, however, are usually more difficult to anticipate and have no real economic value. It is possible, though, for a deep learning framework to measure the risk of cyberattacks and to handle them precisely.

A summary of the calibre of each ML technology provided is given through comparisons ever done by the three biggest cloud providers (Amazon, Azure, and Google). Even so, the assessment

considers a few factors, including the mode of operation, the forecast result, the data processing time, and the algorithm, various datasets can yield different results (Nketah, 2016).

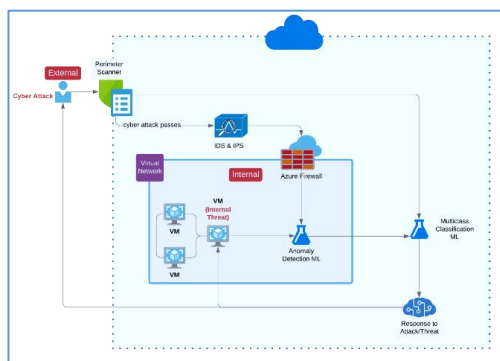
##### **4.4.1. Proposed Design**

Azure Web Application Firewall, Azure AD Identity Protection, Azure DDoS Protection are just a few of the choices Microsoft Azure offers to increase the security of tenant-run cloud systems. Even connecting to Amazon Web Services is possible with some of them. Predictive analytics can be developed as an extra autonomous cloud security system to identify internal and external assaults using ML technology operating within Azure Security. The tenants themselves can put together the necessary algorithm to produce a desired prediction model if ML can correctly carry out the training, validation, and testing processes. We suggest taking a number of actions to support the adoption of predictive analytics by renters as a remedy by carrying out a number of procedures as follows:

- 1) Select One-Class SVM or PCA-Based Anomaly Detection as your ML algorithm model for anomaly detection;
- 2) Establish the criteria that will be used to classify the assault type. It can also serve as a framework for cloud security implementation;
- 3) Based on the model of choice, set the predefined parameters;
- 4) Run a preliminary supervised ML model to identify anomalies brought on by threats or attacks;
- 5) Verify the output of the suggested ML model;

Because it's possible that a brand-new event happens that wasn't brought on by an attack or threat, but rather something like a brand-new service. In the meantime, the attack must be retaliated to as soon as feasible. However, the disorganised system of categorising cyberattacks to offer the best defence against attacks has not yet attained standardisation. Therefore, we propose that the taxonomy issue should be ignored.

We suggest an ML security detection model for Azure that works at both the IaaS and PaaS levels. The suggested model distinguishes between internal and external threats. For an internal threat, the model combines machine learning (ML) models at the first layer and classifies it based on a number of criteria. Furthermore, an external attack will target the second layer ML because it is more likely to be seen than an internal threat. Fig. 12 illustrates the model's conceptual design.



**Fig. 12. Proposed Combined ML Framework for Microsoft Azure Cloud Service Security**

The following tenets serve as the foundation for this architecture. First, in the above-described architecture, the perimeter scanner serves as the first entry point for external cyberattacks. The firewall serves as a barrier if the attack manages to get past the perimeter

scanner and so does the other security layer. On the other side, every successful assault that gets past the security layers will be detected by the machine learning system. A speedy and accurate response to anomalies brought on by successful external attacks is made possible by the by the anomaly detection machine learning algorithm. The multiclass classification algorithm will be used to re-enter each of these anomalies. This system will identify and look into any unusual behaviour by applying the categorization principle. As a result, if the Azure Defender System's machine learning design for security is sufficiently matured, third-party services to offer additional cloud security services may not be required.

## 5. CONCLUSION

Cyber-attack types and techniques are changing. Unfortunately, there is no shared vocabulary for interpreting this in the cyber security frameworks until today. As a result, there are numerous viewpoints and categorization systems for diverse attacks. It is possible to enhance cyber security studies in the context of cloud technology by fusing the results of that study and developing a single international guiding standard.

The responses to the research questions discovered by this study can be summed up as follows: 1. IaaS and PaaS cloud service model implications for cyber security are still extremely extensive. Integrity impacts from cyberattacks are the most serious consequences and happen at the application level. The lowest implication, which only applies to the IaaS cloud service model, occurs at the physical level in confidentiality. 2.



Researchers categorised several attack methods in non-standard cloud service models. However, many people do not differentiate between different cloud service levels (IaaS and PaaS). Again, this can be troublesome because IaaS and PaaS run on different tiers.

Subjectivity is one of the methods used in this paper's. Researchers have used a variety of techniques to explain the effects of cyber threats on IaaS and PaaS cloud services as a result of this situation. To standardise and streamline the terminology used to describe attacks, several researchers have created a taxonomy for cloud attacks. Nevertheless, the repercussions of cyber-attacks are highly diverse. MLaaS comes as one solution for cloud model security

system. Especially for IaaS and PaaS cloud computing levels.

## RESEARCH SUGGESTIONS

Two of the most significant obstacles to this research is data collection and ML model training to show that MLaaS may become truly possible to run. There must be several distinct and useful attacks carried out to see how ML operates and can perform predictive analytics. The proposed model will be used in subsequent studies to perform trustworthy ML testing. Moreover, since UNSW-NB15 represents contemporary low footprint attacks, guaranteed data sets like these can be chosen as training data in finding the highest rate of successful ML algorithm.

## REFERENCES

- Ahamed, F., Shahrestani, S., & Ginige, A. (2013). Cloud computing: Security and reliability issues. *Communications of the IBIMA*, 2013, 1.
- Alhenaki, L., Alwatban, A., Alahmri, B., & Alarifi, N. (2019). Security in cloud computing: a survey. *International Journal of Computer Science and Information Security (IJCSIS)*, 17(4).
- Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. *IET Communications*, 14(7), 1185-1191.
- Bhandari, P. (2020). *A step-by-step guide to data collection*. Scribbr. <https://www.scribbr.com/methodology/data-collection/>
- Campfield, M. (2021). Mind the gap: the cloud security skills shortage. *Computer Fraud & Security*, 2021(8), 6-10.
- Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*, 59, 126-140.
- Curran, K., Carlin, S., & Adams, M. (2011). Cloud computing security. *Journal of Network Engineering*, 37(1), 4069-4072.
- Darwish, M., Ouda, A., & Capretz, L. F. (2013). Cloud-based DDoS attacks and defenses. In *International Conference on Information Society (i-Society 2013)* (pp. 67-71). IEEE.

- De Donno, M., Giaretta, A., Dragoni, N., Bucchiarone, A., & Mazzara, M. (2019). Cyber-storms come from clouds: Security of cloud computing in the IoT era. *Future Internet*, 11(6), 127.
- Evangelopoulou, M. (2021). *Cyber Security Fundamentals (M)*.
- Fitzek, F. H. P., Granelli, F., & Seeling, P. (2020). Network slicing. In *Computing in Communication Networks* (1st ed., p. 71). Academic Press.
- Forcepoint. (2019). *What is Security as a Service (SECaaS)?* Forcepoint. <https://www.forcepoint.com/cyber-edu/security-as-a-service-secaas>
- Fujs, D., Mihelič, A., & Vrhovec, S. L. (2019, August). The power of interpretation: Qualitative methods in cybersecurity research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (pp. 1-10).
- Google Cloud Tech. (2020). *Google Data Center Security: 6 Layers Deep*. <https://www.youtube.com/watch?v=kd33UVZhnAA>
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *J Internet Serv Appl* 4 (1): 1-13.
- Hawedi, M., Talhi, C., & Boucheneb, H. (2018). Security as a service for public cloud tenants (SaaS). *Procedia computer science*, 130, 1025-1030.
- Help Net Security. (2021). What is the impact of remote work on security best practices? *Help Net Security*. <https://www.helpnetsecurity.com/2021/06/24/remote-work-security-practices/>
- Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal*, 21(4), 574-588.
- Iqbal, S., Kiah, M. L. M., Dhaghghi, B., Hussain, M., Khan, S., Khan, M. K., & Choo, K. K. R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and Computer Applications*, 74, 98-120.
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.
- Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In *2009 IEEE international conference on cloud computing* (pp. 109-116). Ieee.
- Kaelin, M. (2019). *How to create a cloud-based virtual network in Microsoft Azure*. TechRepublic. <https://www.techrepublic.com/article/how-to-create-a-cloud-based-virtual-network-in-microsoft-azure/>
- Khan, M. A. (2016). A survey of security issues for cloud computing. *Journal of network and computer applications*, 71, 11-29.
- Kofahi, N. A., & Al-Rabadi, A. R. (2018). Identifying the top threats in cloud computing and its suggested solutions: a survey. *Networks*, 6(1), 1-13.

- Makkawi, A. M., & Yousif, A. (2020). Machine Learning for Cloud DDoS Attack Detection: A Systematic Review. In *2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)* (pp. 1-9). IEEE.
- Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 2(2), 109-134.
- Microsoft. (2021a). *Virtual Network – Virtual Private Cloud | Microsoft Azure*. Virtual Network. <https://azure.microsoft.com/en-gb/services/virtual-network/>
- Microsoft. (2021b). *What is a virtual machine and how does it work | Microsoft Azure*. <https://azure.microsoft.com/en-gb/overview/what-is-a-virtual-machine/>
- Monika, G., & Kalpana, Y. (2016). Data Security is the Major Issue in Cloud Computing-A Review. *Indian Journal of Science and Technology*, 9, 43.
- Mouli, V. R., & Jevitha, K. P. (2016). Web services attacks and security-a systematic literature review. *Procedia Computer Science*, 93, 870-877.
- Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. *IEEE Access*, 9, 20717-20735.
- NIST. (2018). *Evaluation of Cloud Computing Services Based on NIST SP 800-145*. <https://www.nist.gov/publications/evaluation-cloud-computing-services-based-nist-sp-800-145>
- Nketah, G. U. (2016). Comparison of Machine Learning Services. *University of Stavanger, Norway*. <http://hdl.handle.net/11250/2413901>
- Nugraha, B. (2016). Analisis Teknik-Teknik Keamanan Pada Future Cloud Computing vs Current Cloud Computing: Survey Paper. *Jurnal Nasional Teknologi dan Sistem Informasi*, 2(2), 35-42.
- Nunnikhoven, M. (2021). *Top Cloud Security Challenges for 2021*. Trend Micro. [https://www.trendmicro.com/en\\_se/devops/21/b/top-cloud-security-challenges-for-2021.html](https://www.trendmicro.com/en_se/devops/21/b/top-cloud-security-challenges-for-2021.html)
- OWASP. (n.d.). *Man-in-the-browser Software Attack | OWASP Foundation*. Retrieved November 15, 2021, from [https://owasp.org/www-community/attacks/Man-in-the-browser\\_attack](https://owasp.org/www-community/attacks/Man-in-the-browser_attack)
- Singh, A. (2019). Security concerns and countermeasures in cloud computing: a qualitative analysis. *International Journal of Information Technology*, 11(4), 683-690.
- Singh, S., & Jeong, Y. S. park, Jong.(2016). A Survey on Cloud Computing Security: Issues, Threats, and Solutions. *Journal of Network and Computer Applications*, 75.
- Sosinsky, B. (2011). *Cloud Computing Bible*. Wiley Publishing, Inc.
- Subashini, S., & Kavitha, V. (2011). Review: A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl*, 341.
- Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. *Computers & Electrical Engineering*, 71, 28-42.
- Tchifilionova, V. (2010). Security and privacy implications of cloud computing—Lost in the cloud. In *International Workshop on Open Problems in Network Security* (pp. 149-158). Springer, Berlin, Heidelberg.

- Tripathi, A., & Mishra, A. (2011). Cloud computing security considerations. In *2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)* (pp. 1-5). IEEE.
- Wang, X., Zhang, Y., Zhang, H., Wei, X., & Wang, G. (2019). Identification and authentication for wireless transmission security based on RF-DNA fingerprint. *EURASIP Journal on Wireless Communications and Networking*, 2019(1), 1-12.
- You, P., Peng, Y., Liu, W., & Xue, S. (2012). Security issues and solutions in cloud computing. In *2012 32nd International Conference on Distributed Computing Systems Workshops* (pp. 573-577). IEEE.
- Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, 9, 94668-94690.