**A Study to Cloud Computing**

Table of Contents

[1. Introduction 4](#_Toc153117085)

[1.1 Overview 4](#_Toc153117086)

[1.2 Background 4](#_Toc153117087)

[Cloud Computing Evolution 4](#_Toc153117088)

[1. Cluster computing 4](#_Toc153117089)

[2. Grid Computing 5](#_Toc153117090)

[3. Utility Computing 5](#_Toc153117091)

[4. Cloud 5](#_Toc153117092)

[4.1 Layered architecture and service models 5](#_Toc153117093)

[4.1.1 Infrastructure as a Service (IaaS) 6](#_Toc153117094)

[4.1.2 Platform as a service (PaaS) 6](#_Toc153117095)

[4.1.3 Software-as-a-Service (SaaS) 6](#_Toc153117096)

[5. Types of clouds 7](#_Toc153117097)

[6. Cloud Architectures and Deployment 7](#_Toc153117098)

[6.1 Public Cloud 7](#_Toc153117099)

[6.2 Private Cloud 7](#_Toc153117100)

[6.3 Hybrid Cloud 8](#_Toc153117101)

[6.4 Multi Cloud 8](#_Toc153117102)

[2. Security challenge 8](#_Toc153117103)

[2.1 Data Breach 8](#_Toc153117104)

[2.2 Insecure APIs 8](#_Toc153117105)

[2.3 Malicious Insider 8](#_Toc153117106)

[2.4 Data Loss 9](#_Toc153117107)

[2.5 Insufficient Due Diligence 9](#_Toc153117108)

[2.6 Account Hijacking 9](#_Toc153117109)

[2.7 Denial of Service Attack 9](#_Toc153117110)

[2.8 Abuse and Nefarious use of Cloud 10](#_Toc153117111)

[2.9 Shared Technology Issues 10](#_Toc153117112)

[2.10 Phishing Attack 10](#_Toc153117113)

[3. Literature Review on Phishing Attack 10](#_Toc153117114)

[4. Mitigation strategies and Recommendations 16](#_Toc153117115)

[5. Trends and Solution 16](#_Toc153117116)

[6. Conclusion 17](#_Toc153117117)

[7. References 18](#_Toc153117118)

**List of Figures**

[Figure 1 Results of IDC ranking security challenges (Popović, K. and Hocenski, Ž., 2010). 6](#_Toc152849986)

[Figure 2 Cloud paradigm: an overall view. (Botta, A, et al., 2016) 7](#_Toc152849987)

[Figure 3 Cloud computing service delivery models taken from IEEE Xplore.( Bassi, S. and Chaudhary, A., 2015) 8](#_Toc152849988)

[Figure 4 illustrates a three-dimensional approach of NCC-SRA for data collection, aggregation and data classification with respect to cloud types taken from MDPI.(Ahmad, W, et al., 2021) 9](#_Toc152849989)

[Figure 5 Graphical Representation of an account hijacking attack. (Ahmad, W., et al., 2021) 11](#_Toc152849990)

[Figure 6 Graphical representation of a denial of service attack. . (Ahmad, W., et al., 2021) 11](#_Toc152849991)

[Figure 7 Phishing attack types taken from SpringerLink(Gupta, B.B., et al., 2017) 13](#_Toc152849992)

[Figure 8 Fighting against phishing attacks: state of the art and future challenges taken from SpringerLink (Gupta, B.B., el at., 2017). 13](#_Toc152849993)

# **1. Introduction**

## **1.1 Overview**

The fundamental concept of cloud computing is not new. John McCarthy anticipated in the 1960s that computing resources will be made available to the general people on a utility-like basis (Zhang, Q., et al., 2010).

Public acceptance of a fundamental cloud computing idea has been suggested by the National Institute of Standards and Technology (NIST). As a concept that enables the sharing of numerous computer resources as services to different clients, cloud computing is defined by them. Customers may simply and affordably modify their service needs under this paradigm. The concept of cloud computing by Armbruster and others highlights the importance of services in cloud computing and states that services are delivered by offering both applications and system software in the datacenter (Gai, K. and Li, S., 2012).

Virtualization technologies in conjunction with self-service capabilities are being utilized by cloud service providers (CSPs) such as Microsoft, Google, Amazon, Salesforce.com, and Go Grid, to supply computer resources via the Internet. In these service provider setups, the best use of virtualization requires co-locating virtual machines from several enterprises on the same physical server (Popović, K. and Hocenski, Ž., 2010).

Over the past few years, cloud computing has developed from a potential business idea to one of the fastest-growing IT market areas. However, worries about how safe the cloud is are starting to surface as more and more data on people and businesses is stored there. Customers are still hesitant to move their business to the cloud, even with all the buzz around it. The acceptability of cloud computing has been hindered significantly by security concerns; in fact, as figure 1 illustrates, security was seen as the biggest hurdle to cloud computing (Kuyoro, S.O., et al., 2011).

A graph of a number of people

Description automatically generated with medium confidence

Figure Results of IDC ranking security challenges (Popović, K. and Hocenski, Ž., 2010).

## **1.2 Background**

### **Cloud Computing Evolution**

The history starts from the following technologies.

## **Cluster computing**

In simple terms, this involves grouping connected computers together to do a single computing activity through close coordination, much like a single computer. The components of the cluster are not always linked to one another via fast local area networks. Instead of utilizing a single computer, this cluster of computers increases availability, performance, and speed while lowering total costs (Bassi, S. and Chaudhary, A., 2015).

## **Grid Computing**

For each person, grid computing might imply something different. Grand visions are frequently compared to power networks, in which electricity is obtained by consumers (or appliances) through wall outlets without regard for the location or method of generation. This perspective on grid computing sees computing as becoming ubiquitous, with individual users (or client applications) having access to computing resources (processors, storage, data, apps, and so on) as needed and knowing little to nothing about the underlying technologies, hardware, operating system, and other components (Jacob, B., et al., 2005)**.**

## **Utility Computing**

"On Demand" computing was founded on this ability to be provided as a service. Moreover, the cloud computing paradigm put out the idea of providing network, application, and computer components as a service. As early industry titans in utility computing, IBM, HP, and Microsoft made significant investments in research and development of payment systems, cloud architectures, and development issues. 2008 saw the rise of Google, Amazon, and other companies that created their own utility services for computing, storage, and apps (Bassi, S. and Chaudhary, A., 2015).

## **Cloud**

The National Institute of Standard and Technologies (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." This definition captures the essential elements of cloud computing. Although the basic concept of cloud computing was not new, the word only became well-known after it was coined by Google CEO Eric Schmidt in 2006.

**A diagram of a cloud

Description automatically generated**

Figure Cloud paradigm: an overall view. (Botta, A, et al., 2016)

### **4.1 Layered architecture and service models**

There are four layers to the cloud architecture: platform, application, infrastructure, and datacenter (hardware) (Zhang, Q., et al., 2010).

They may all be viewed as both consumers and services for the layers above and below, respectively. Cloud services fall into three primary categories: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Applications operating in cloud settings are provisioned; this is referred to as SaaS. Usually, a web browser or a thin client is used to access applications. Platform-layer resources, such as software development frameworks and operating system support, are referred to as PaaS. Offering processing, storage, and network resources while letting the user manage the operating system, storage, and apps is known as Infrastructure as a Service (IaaS) (Dukaric, R. and Juric, M.B., 2013).

### **4.1.1 Infrastructure as a Service (IaaS)**

Infrastructure as a Service is a single tenant cloud layer in which contractual clients only have access to the dedicated resources of the cloud computing provider at a pay-per-use cost. This significantly reduces the requirement for a sizable upfront expenditure on computer infrastructure, including servers, networking equipment, and processing power (Kuyoro, S.O, et al, 2011).

### **4.1.2 Platform as a service (PaaS)**

Users can access the computing platform and solution stack as a service using a Platform-as-a-Service (PaaS) paradigm. Users may create their own applications without having to manage the hardware and software requirements for developing their own applications. The PaaS paradigm offers full life cycle support for providing applications and services (Bassi, S. and Chaudhary, A., 2015).

### **4.1.3 Software-as-a-Service (SaaS)**

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model (Satyanarayana, S., 2012).

A diagram of cloud computing models

Description automatically generated

Figure Cloud computing service delivery models taken from IEEE Xplore.( Bassi, S. and Chaudhary, A., 2015)

## **5. Types of clouds**

The challenges has recognized many varieties of clouds, as stated in the following(Mell, P. and Grance, T., 2011): One can categorize cloud computing services into four types: (i) Private Cloud, which is exclusively available to a single organization and is usually owned, managed, and operated by the organization; (ii) Community Cloud, which is available to a specific group of consumers with similar concerns; (iii) Public Cloud, which is available to the general public; (iv) Hybrid Cloud, which combines two or more different cloud infrastructures (private, community, or public); (v) Virtual Private Cloud, which is an alternative to public and private cloud computing and uses virtual private network (VPN) technologies to enable business owners to configure necessary network settings (e.g. security, topology, etc.)( Zhang, Q, et al.,2010).

## **6. Cloud Architectures and Deployment**

Many cloud components, including data centers, software features, services, and applications, are set up in an ideal manner to address both small- and large-scale business issues. This is known as cloud architecture. Wide bandwidth, continuous access to data and applications, an adaptable on-demand network, and security are the goals of cloud architecture. A few key components of generic cloud architecture are as follows: (1) data and resources available with the client, (2) data and resources available on the cloud, (3) software components and services, and (4) middleware (RM, S.P., et al., 2020) (Naeem, A., et al , 2021).

Its deployment model provides information about the cloud's environment and purpose. Figure 4 illustrates the many cloud types that are included in the deployment paradigm, including private, hybrid, and public clouds (Ahmad, W., et al., 2021).

A diagram of cloud architectures

Description automatically generated

Figure illustrates a three-dimensional approach of NCC-SRA for data collection, aggregation and data classification with respect to cloud types taken from MDPI.(Ahmad, W, et al., 2021)

### **6.1 Public Cloud**

This kind of cloud is owned and run by many organizations as public clouds. These networks, infrastructures, and resources are used simultaneously by many thousands of individuals and organizations. Several well-known public cloud providers include Microsoft, Amazon, and Google. The distribution of resources, ownership detection, shared access control, and cloud data security against intrusions are the main issues in this kind of cloud (Rani, B.K, et al., 2015).

### **6.2 Private Cloud**

This type of cloud is usually controlled by one company and has been customized to meet the demands of that company. Organizations can better control their data using private cloud storage (perhaps subject to regulatory compliance restrictions). Either a third party or internal management and hosting is possible. Additionally, trade secrets, medical records, and other classified information may be included in this data (Rani, B.K, et al., 2015).

### **6.3 Hybrid Cloud**

The hybrid cloud concept connects a private cloud to one or more external clouds. This ties together and centrally manages several cloud environments with workload mobility and administration (Rani, B.K., Rani, B.P. and Babu, A.V., 2015).

### **6.4 Multi Cloud**

This model features a multi-cloud system. Clouds can be linked together or not, and they can be private or public. This is also called a community cloud in literature. Better security than public clouds and resource sharing are benefits of using several clouds. Less security than private cloud and the need for controlling policies for management are drawbacks (Rani, B.K, et al., 2015).

# **2. Security challenge**

## **2.1 Data Breach**

Classifying data breach risks according to their origins—i.e., purposeful, or unintentional disclosure of private information—is one method. An alternative method depends on who was responsible for the leak: external or internal threats. Either malicious insiders or outside groups are responsible for purposeful leaks. Malware, viruses, and social engineering are the usual causes of external data breaches (Cheng, L, et al., 2017).

Example: - Over 550,000 blood donors' personal records were inadvertently uploaded to an unprotected public directory of the Australian Red Cross Blood Service website in October 2016 by staff members (Cheng, L, et al., 2017).

## **2.2 Insecure APIs**

We've seen that users interact with one other using APIs, which are available over the internet from any location. They might be used by malicious attackers to undermine integrity, accountability, confidentiality, and availability. In simple terms, cloud APIs are software interfaces—usually standard-based—that consumers may use to manage their cloud services from cloud providers. Transport security, authentication and authorization, code and development processes, and message protection are a few of the crucial topics that users should be paying attention (Pandey, S. and Farik, M., 2015).

## **2.3 Malicious Insider**

The SaaS, PaaS, and IaaS resources will be fully accessible to staff members that work for cloud service providers, including system administrators. Their ability to read private information could represent a serious risk to clients. Because provider processes and procedures are transparent, deliberate insider usage is possible but difficult to identify. Confidentiality, authenticity, authorization, integrity, data protection, accountability, and non-repudiation are among the fundamental information security concepts that are impacted by this (Pandey, S. and Farik, M., 2015).

## **2.4 Data Loss**

Regarding cloud security, data loss is the second most significant problem. Like data breaches, data loss can have disastrous effects on an organization's operations and is a sensitive issue. Malicious hackers, data deletion, data corruption, lost encryption keys, storage system errors, and natural catastrophes are the main causes of data loss (Kazim, M. and Zhu, S.Y., 2015).

Example: - 44 percent of cloud service providers have faced brute force attacks in 2013 that resulted in data loss and data leakage (Kazim, M. and Zhu, S.Y., 2015).

## **2.5 Insufficient Due Diligence**

When people or clients have all the information needed to evaluate the risks associated with a business before employing its services, it's referred to as doing due diligence. Many firms are moving to the cloud without considering the hazards involved since cloud computing provides the exciting opportunities of unlimited computing resources and rapid access (Kazim, M. and Zhu, S.Y., 2015).

## **2.6 Account Hijacking**

This type of attack involves an attacker stealing or taking control of a person's or an organization's cloud account. Sometimes the person or organization is the primary target, and the attacker utilizes the credentials from the stolen account to launch another assault later. An attacker may subsequently engage in nefarious or unlawful action by posing as someone else, which might result in the disclosure of private and corporate data and harm to one's reputation (Ahmad, W., et al., 2021).

A cartoon of a hacker

Description automatically generated

Figure Graphical Representation of an account hijacking attack. (Ahmad, W., et al., 2021)

## **2.7 Denial of Service Attack**

#### On IoT systems, denial of service attacks are the most common and straightforward to execute. When a hacker renders services, apps, or data unavailable to the intended user, it may have quite a negative impact on the cloud(wendi, C., et al., 2021). In order to deprive other requesters of their service, the attacker floods the targeted system, application, or service with requests until it becomes difficult to handle normal traffic. In the end, this type of attack is irresponsible since its primary goal is to force the owner of the cloud service to boost elasticity levels in order to manage the increased traffic and make use of additional virtual resources in order to fulfill requests and maintain quality of service (QoS).Figure 8 shows a graphical depiction of the denial of service attack.

#### A diagram of a person's figure Description automatically generated

Figure Graphical representation of a denial of service attack. . (Ahmad, W., et al., 2021)

## **2.8 Abuse and Nefarious use of Cloud**

Unlimited bandwidth and storage capacity are only two of the many options that cloud providers provide their customers. Certain cloud service providers allow hackers to access the cloud for free during short trial periods, which may be used for illicit purposes such as password cracking and decoding, initiating possible attack points, and executing malicious instructions. Because cloud service providers are targeted for having inadequate fraud detection skills and poor registration processes, spammers, malicious code developers, and other hackers can operate with relative impunity (Bamiah, M.A. and Brohi, S.N., 2011).

Example: - To hide their dangerous code and use users' browsers to install malware, some hackers employ rich content applications like flash files (Bamiah, M.A. and Brohi, S.N., 2011).

## **2.9 Shared Technology Issues**

IaaS providers contribute infrastructure to enable continuous delivery of their services. However, robust isolation properties for a multi-tenant architecture are not provided by this structure. A virtualization hypervisor therefore intervenes in between guest operating systems and the physical computing resources to close this gap. Although these hypervisors offer many benefits, they have shown weaknesses that have allowed guest operating systems to gain unwarranted degrees of power or influence over the underlying platform. No doubt, this resulted in cloud security problems. the client's use of IaaS to streamline hardware or infrastructure use (Parekh, M.D.H. and Sridaran, R., 2013).

## **2.10 Phishing Attack**

Phishing, sometimes known as automated identity theft, is a scam that deceives millions of people and steals substantial sums of money by taking advantage of human nature and the Internet. In April 2004, a study by the IT industry research company Gartner revealed that around 1.8 million Americans had already provided their personal information to phishers. Phishing assaults have been found to have increased significantly over the past few years, posing a danger to international security. These campaigns' primary goal is to take advantage of any technical or user-inadvertent weaknesses in the system. As a result, researchers must offer protection against these assaults from both the technical and user perspectives (Gupta, B.B., Tewari, et al., 2017)

# **3. Literature Review on Phishing Attack**

It is challenging to prevent phishing attacks because they prey on human vulnerabilities, namely those of system end users. As per the evaluation, even after receiving training from the top-performing user awareness program, 29% of phishing assaults were missed by end-users. It is practically unclear, however, how well software phishing detection systems work in relation to tailored kinds of phishing assaults because they are tested against bulk phishing attempts (Khonji, M., et al., 2013). Figure 7 displays the categorization of phishing attacks.

Phishing, as defined by the FBI's Internet Crime Complaint Center, is "the use of unsolicited email...supposedly from a legitimate company requesting personal, financial, and/or login credentials." 23 states in the United States and Guam had legislation against phishing as of February 23, 2020. The remaining states classify this crime as identity theft, computer crime, or fraudulent or misleading conduct. Globally, phishing assaults are on the rise, with phishing being the most common online crime reported to the FBI. As of the third quarter of 2020 (Anti-Phishing Working Group 2020), the top two primary targets were financial institutions (19.2%) and webmail and software-as-a-service users (31.4%). As a result, companies and individuals are suffering increasing financial losses (Suzuki, Y.E. and Monroy, S.A.S., 2022).

Malware- and social engineering-based phishing attempts are the two main categories into which phishing assaults fall. Social engineering-based phishing involves the use of phony websites or emails that look real to deceive the victim into providing their credentials (Gupta, B.B., et al., 2017). Given the severity of the phishing issue, action must be taken to safeguard susceptible people. Consequently, both online browsers and internet security suites are equipped with anti-phishing and broader identity protection functions. There is a tonne of phishing defences at your disposal (Purkait, S., 2012).

A diagram of a computer program

Description automatically generated

Figure Phishing attack types taken from SpringerLink(Gupta, B.B., et al., 2017)

Based on the purpose of phishing, a phishing categorizing is carried out. The many definitions of ransomware and phishing are taken into consideration to do the same. The term "phishing" is defined as follows, combining the several meanings (Chanti, S. and Chithralekha, T., 2022).

In the fourth quarter of 2014, according to APWG's study, the most often utilized domain for phishing schemes was.com (41%) followed by.net (7%),.org (5%) and.br (3%) among the most targeted businesses (Gupta, B.B., Arachchilage, N.A. and Psannis, K.E., 2018).

Groups 1 through 4 consist of external features, group 2 are body-based features, group 3 are URL-based features, and group 4 is featuring header. Phishing emails are a conventional and popular method used in phishing scams. Users move any phishing emails from Mail move Agents (MTA) to Mail Delivery Agents (MDA) through Mail User Agents (MUA), who then receive the emails (Gupta, B.B., el at., 2017).

A screenshot of a computer

Description automatically generated

Figure Fighting against phishing attacks: state of the art and future challenges taken from SpringerLink (Gupta, B.B., el at., 2017).

According to (Safi, A. and Singh, S. (2023)) research done on automated versus conventional phishing detection methods. Using a legal viewpoint, educating users, holding regular training sessions or workshops, and increasing awareness are some of the traditional anti-phishing strategies. List-based and machine learning-based strategies are discussed in computerized or automated anti-phishing efforts. Most significantly, the study contrasts the advantages and disadvantages of different strategies from the viewpoints of users and performance.

Social media began to gain traction as a tool for interpersonal connectedness in the 2000s. Social networking is another term for this subset of social media. These platforms, which enable people with similar interests, circles, or affiliations to connect with one another, include Facebook, Twitter, and Google+. Apart from that, there are other social media sites that target markets, such as Tumblr, Pinterest, Spotify, and Foursquare. The quick information sharing on social media has advantages, but it may also be used by phishers to launch phishing attacks (Chiew, K.L., el at., 2018).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.no** | **Author** | **Year** | **Mitigation** | **Findings** |
| 1 | Khonji, M., Iraqi, Y. and Jones, A | 2013 | To lessen users' vulnerability to phishing attempts, user education and training programs aim to raise users' technical understanding. | General techniques (such as heuristics, machine learning, blacklists, and whitelists) utilized in phishing detection and their FP and FN detection rates. The table also shows whether the methods that are being offered need Internet connectivity to work. |
| 2 | Suzuki, Y.E. and Monroy, S.A.S | 2022 | Phishing kits can be used to initiate phishing attacks when cybercriminals search web sources for emails or acquire hacked emails. Massive phishing emails may be sent with only one click if the necessary phishing infrastructure is in place. Limiting one's presence in publicly accessible data that might be used for open-source intelligence (OSINT), limiting user access, and securing user access are ways to resist phishers' attempts to get PII and the organization's sensitive information. | It is also made easier to comprehend phishing emails holistically from both cybersecurity and criminological viewpoints by applying a sequential schema from the situational crime prevention method. Our model might be a useful addition for cybersecurity experts to evaluate current security measures, with an emphasis on suitable mitigation measures as a security issue develops. Scholars in the field of criminology and other academics might enhance the effectiveness of the situational crime prevention strategy by examining and averting other criminal incidents, particularly those frequently linked to phishing emails, including identity theft and other crimes involving identification. |
| 3 | Purkait, S | 2012 | The severity of the phishing issue has made action to safeguard susceptible individuals necessary. Anti-phishing and comprehensive identity protection capabilities are thus standard in both online browsers and internet security packages. There is a tone of options for phishing defenses. These remedies cover everything from minor tweaks to more comprehensive redesigns. Examining the information flow in phishing assaults of all kinds, he gave thorough insights into the technologies employed by phishers and the various defenses against them. | The results show that the anti-phishing strategies now in use that have been widely implemented online may be divided into eight groups. Furthermore, every method that has been suggested thus far has a preventative focus. It has been observed through numerous usability studies that neither client-side toolbars and warnings nor server-side security indicators are effective in stopping vulnerable users from falling for phishing scams. Phishers primarily target innocent consumers who are the weakest link in the security chain. |
| 4 | Gupta, B.B., Arachchilage, N.A. and Psannis, K.E | 2018 | There are several methods for identifying and blocking phishing attempts, but the online community is still in need of a comprehensive way to protect the network from these assaults. There are almost no other options but to take these devices offline and manually update their firmware to find any breaches. | We concentrate on social engineering assaults since they have a detrimental impact on online sales. Phishers always employ phony websites and counterfeit emails as communication tools for their illicit operations. It casts a negative light on e-commerce, which in this modern Internet era is very vital. Our survey aids novice researchers in comprehending the background, present-day patterns of assaults, and shortcomings of several existing remedies. |
| 5 | Chanti, S. and Chithralekha, T | 2022 | The threat of ransomware-based phishing to online users increases significantly. Since the attacker used symmetric key encryption to encrypt the victims' system, only the attacker has the ability to decode the data because they utilize the same key for both operations. | There are also several real-time phishing assaults included, one for each kind of attack that is included in the taxonomy. Attack data taken from APWG survey reports and OpenPhish phishing feeds is used to do statistical analysis of phishing assaults. |
| 6 | Safi, A. and Singh, S | 2023 | Increasing awareness, educating users, holding recurring training sessions or workshops, and applying a legal viewpoint are some of the traditional anti-phishing strategies. Techniques based on lists and machine learning are discussed in computerized or automated anti-phishing efforts. | The number of results for the term "Phishing" when searched on the databases is 32, which represents 40% of the current research effort. Conversely, Machine Learning ranks as the second most popular term, yielding 16 and 20% of all evaluated articles. Phishing Detection comes up at number two with twelve articles, or 15%. for the terms "cyber security" |
| 7 | Chiew, K.L., Yong, K.S.C. and Tan, C.L | 2018 | A methodical comprehension of these strategies will result in the creation of an anti-phishing methodology that is more comprehensive and successful in addressing the phishing issue. Additionally, by having this knowledge, the public will be better equipped to defend against phishing assaults and policymakers will be able to put rules in place to stop phishers from using their exploits in the future. | Phishers' focus will be directed on the rapidly expanding mobile and cloud computing markets. Particularly in these two domains, anti-phishing efforts are required. |

# **4. Mitigation strategies and Recommendations**

Security has become more and more necessary as technology has grown in importance in our society. Cybercriminals are gaining illegal access to our systems through a variety of methods. But instead of targeting computers, these cybercriminals are now focusing on the "weakest link" in the security chain—people (Sumner, A. and Yuan, X., 2019).

Employees may safeguard themselves and their companies by following to phishing strategies with the use of AI-based cyber security awareness training packages. The following are useful strategies for carrying out phishing attacks:

Falsely represent: This is an accepted method. All that the phishing email does is pretend to be an official company where the victims may have an account. To make the scam email appear legitimate and ask the recipient to check in to decode some difficulties, the phisher communicates the symbols and drawings with the genuine website. Because it will be difficult for regular users to distinguish between reputable and fraudulent emails, this assault lowers user morale (Ansari, M.F., el at., 2022).

Phishing assaults come with several concerns. AI technologies significantly contribute to preventing most of these assaults. This element has been linked to most firms concentrating on AI-based cyber security to safeguard their systems. The strategy guarantees that the businesses have not had internal security breaches. The creation of AI-based cyber security solutions has also increased. For many of its customers, Google created a mechanism that might prevent email phishing. Taking extra precautions and being more mindful when using the internet and opening emails are some more strategies to stop assaults (Ansari, M.F., el at., 2022).

# **5. Trends and Solution**

There are several approaches put out in the literature review to stop and identify phishing attempts, but no one, all-encompassing solution is ideal for combating phishing assaults. As noted before, phishing assaults can be carried out through malware or social engineering, in which case the attackers make use of phony emails or websites. For this reason, there are several ways to identify these emails and webpages. Many strategies were put out and considered to properly regulate phishing emails. Likewise, several remedies were also put out to stop assaults using phishing websites. Phishers utilize phony websites in addition to phishing emails as a means of deception also the phony webpage URL. Phishing websites are more dangerous than phishing emails since many of the former are filtered before reaching the user's inbox and end up buried behind spam. If properly filtered, any knowledgeable user may readily ignore these filtered spam emails.

To regulate phishing emails, DNS-based blacklists (DNSBL) use the DNS protocol. Attackers exploit this by switching IP addresses or gaining access to a genuine computer, as updating the blacklists on a regular basis necessitates interactive activity.

The Google Safe Browsing API requests that client-side apps verify if a given URI is on a list that is updated by Google's blacklist. Several browsers support the protocol, despite its current experimental state (Gupta, B.B., et al., 2018).

As phishing emails are thought to be the most prevalent kind of assault, future work will focus on researching and developing phishing detection systems. The main concept is to analyze emails by splitting them into the Header and Body sections, after which a mining method will be used to extract the hybrid (content and behaviour) characteristics. To aid with user awareness, those characteristics will be assigned a risk value of "severe," "medium," or "low." The second layer, a neural network, receives the result and uses it to provide a final assessment of the email, classifying it as "safe," "partially safe," or "phishy." Additionally, this detection tool will shield users in non-secured environments against phishing assaults.

# **6. Conclusion**

The issue of phishing has been recognized for about two decades now. Nevertheless, malware is still used to steal credit card numbers, online login passwords, and personal information. Although there are a several methods available to counter these assaults, phishers always find a way to exploit those flaws so they can carry out their attacks. Malware assaults, which utilize harmful code or software to obtain the necessary data, and social engineering, which refers to obtaining user credentials through emails or phony websites, are the two general categories under which phishing attacks fall. This article examined many strategies to protect users against phishing emails and websites. Our survey aids novice researchers in comprehending the background, present-day patterns of assaults, and shortcomings of several existing remedies. One of the most difficult problems facing network security these days is defence against phishing attacks. Phishing assaults should be easy to identify by a security system with few false positives. Blacklisting, data mining and heuristics, machine learning, and soft computing algorithms are the protection strategies included in this review. We are aware that one of the factors contributing to the effectiveness of phishing attempts is user ignorance. Considering this, user education is also necessary to reduce phishing assaults, in addition to interface enhancements that issue warnings or the automated removal of dangerous information before to end users, which seems like a more viable strategy (Gupta, B.B., et al., 2017).

# **7. References**

1. Zhang, Q., Cheng, L. and Boutaba, R., 2010. Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*, pp.7-18
2. Popović, K. and Hocenski, Ž., 2010, May. Cloud computing security issues and challenges. In *The 33rd international convention mipro* (pp. 344-349). IEEE
3. Kuyoro, S.O., Ibikunle, F. and Awodele, O., 2011. Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)*, *3*(5), pp.247-255.
4. Gai, K. and Li, S., 2012, November. Towards cloud computing: a literature review on cloud computing and its development trends. In *2012 Fourth international conference on multimedia information networking and security* (pp. 142-146). IEEE.
5. Botta, A., De Donato, W., Persico, V. and Pescapé, A., 2016. Integration of cloud computing and internet of thngs: a survey. *Future generation computer systems*, *56*, pp.684-700.
6. Zhang, Q., Cheng, L. and Boutaba, R., 2010. Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*, pp.7-18.
7. Dukaric, R. and Juric, M.B., 2013. Towards a unified taxonomy and architecture of cloud frameworks. *Future Generation Computer Systems*, *29*(5), pp.1196-1210.
8. Mell, P. and Grance, T., 2011. The NIST definition of cloud computing.
9. Bassi, S. and Chaudhary, A., 2015. Cloud computing data security–background and benefits. *International Journal of Computer Science & Communication*, *6*(1), pp.34-40.
10. Jacob, B., Brown, M., Fukui, K. and Trivedi, N., 2005. Introduction to grid computing. *IBM redbooks*, pp.3-6.
11. RM, S.P., Bhattacharya, S., Maddikunta, P.K.R., Somayaji, S.R.K., Lakshmanna, K., Kaluri, R., Hussien, A. and Gadekallu, T.R., 2020. Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything. *Journal of parallel and distributed computing*, *142*, pp.16-26.
12. Naeem, A., Javed, A.R., Rizwan, M., Abbas, S., Lin, J.C.W. and Gadekallu, T.R., 2021. DARE-SEP: A hybrid approach of distance aware residual energy-efficient SEP for WSN. *IEEE transactions on green communications and networking*, *5*(2), pp.611-621.
13. Ahmad, W., Rasool, A., Javed, A.R., Baker, T. and Jalil, Z., 2021. Cyber security in IoT-based cloud computing/ A comprehensive survey. Electronics, 11(1), p.16.
14. Rani, B.K., Rani, B.P. and Babu, A.V., 2015. Cloud computing and inter-clouds–types, topologies, and research issues. *Procedia Computer Science*, *50*, pp.24-29.
15. Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76*(12), pp.9493-9532.
16. Satyanarayana, S., 2012. Cloud computing: SAAS. *Computer Sciences and Telecommunications*, (4), pp.76-79.
17. Cheng, L., Liu, F. and Yao, D., 2017. Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), p.e1211.
18. Pandey, S. and Farik, M., 2015. Cloud computing security: Latest issues & countermeasures. *Int. J. Sci*, *4*(11), pp.3-6.
19. Kazim, M. and Zhu, S.Y., 2015. A survey on top security threats in cloud computing. *International Journal of Advanced Computer Science and Applications*, *6*(3), pp.109-113.
20. Iwendi, C., Rehman, S.U., Javed, A.R., Khan, S. and Srivastava, G., 2021. Sustainable security for the internet of things using artificial intelligence architectures. *ACM Transactions on Internet Technology (TOIT)*, *21*(3), pp.1-22.
21. Bamiah, M.A. and Brohi, S.N., 2011. Seven deadly threats and vulnerabilities in cloud computing. *International Journal of Advanced engineering sciences and technologies*, *9*(1), pp.87-90.
22. Parekh, M.D.H. and Sridaran, R., 2013. An analysis of security challenges in cloud computing. *International Journal of Advanced Computer Science and Applications*, *4*(1).
23. Gupta, B.B., Tewari, A., Jain, A.K. and Agrawal, D.P., 2017. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*, pp.3629-3654.
24. Khonji, M., Iraqi, Y. and Jones, A., 2013. Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), pp.2091-2121
25. Krombholz, K., Hobel, H., Huber, M. and Weippl, E., 2015. Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, pp.113-122.
26. Yi, P., Guan, Y., Zou, F., Yao, Y., Wang, W. and Zhu, T., 2018. Web phishing detection using a deep learning framework. *Wireless Communications and Mobile Computing*, *2018*.
27. Almomani, A., Gupta, B.B., Atawneh, S., Meulenberg, A. and Almomani, E., 2013. A survey of phishing email filtering techniques. *IEEE communications surveys & tutorials*, *15*(4), pp.2070-2090.
28. Suzuki, Y.E. and Monroy, S.A.S., 2022. Prevention and mitigation measures against phishing emails: a sequential schema model. Security Journal, 35(4), pp.1162-1182.
29. Chanti, S. and Chithralekha, T., 2022. A literature review on classification of phishing attacks. International Journal of Advanced Technology and Engineering Exploration, 9(89), pp.446-476.
30. Gupta, B.B., Arachchilage, N.A. and Psannis, K.E., 2018. Defending against phishing attacks: taxonomy of methods, current issues, and future directions. *Telecommunication Systems*, *67*, pp.247-267.
31. Purkait, S., 2012. Phishing counter measures and their effectiveness–literature review. *Information Management & Computer Security*, *20*(5), pp.382-420.
32. Safi, A. and Singh, S. (2023) A systematic literature review on phishing website detection techniques, *Journal of King Saud University - Computer and Information Sciences*, [online] Available at: <https://doi.org/10.1016/j.jksuci.2023.01.004>.
33. Chiew, K.L., Yong, K.S.C. and Tan, C.L., 2018. A survey of phishing attacks: Their types, vectors, and technical approaches. Expert Systems with Applications, 106, pp.1-20.
34. Sumner, A. and Yuan, X., 2019, April. Mitigating phishing attacks: an overview. In Proceedings of the 2019 ACM Southeast Conference (pp. 72-77).
35. Ansari, M.F., Sharma, P.K. and Dash, B., 2022. Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. Prevention.