# ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ


# Social Engineering Threats, Attacks and Defense Methods in Cloud Environments

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του


Κοτσαράπογλου Ιάσων - Ειρηναίου

**Επιβλέπων: Κρητικός Κυριάκος**

**Μέλη εξεταστικής επιτροπής: Καρύδα Μαρία - Κωνσταντίνου Ελισάβετ**


Σάμος, [Ιούνιος, 2025]

**© 2025**

**του**

**Κοτσαράπογλου Ιάσων - Ειρηναίου**

**Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων**

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ**

# Abstract

Cloud computing has completely changed the landscape of the information technology industry by making it possible to have on-demand, cost-effective access to a shared pool of customizable computing resources. These resources might include networks, servers, storage, applications, and services. In this respect, many companies are increasingly moving their workloads (e.g., applications, services and business processes) to the cloud. However, the frequency of cyber assaults, particularly those involving social engineering methods, has increased along with the rising use of cloud computing. Attacks using social engineering entail persuading or deceiving individuals so as to obtain access to a computer system's hardware or software or to sensitive data.

In this work, we present a comprehensive examination of social engineering assaults in the context of cloud computing, including a breakdown of the many forms these attacks may take and the dangers that are associated with them. The primary contributions that our thesis makes are an in-depth description and analysis of social engineering attacks, a classification of the various types of such attacks, as well as a classification and comparative analysis based on specific well-crafted criteria of respective defense measures. The purpose of this thesis report is to increase awareness of social engineering assaults and to provide guidelines for countering such assaults in cloud computing environments, while also identifying existing research gaps and proposing directions for future investigation.

**Keywords:** Social engineering, cloud computing, cybersecurity, attack classification, risk analysis, defense mechanisms, security awareness.

# Περίληψη

Το υπολογιστικό νέφος έχει μεταμορφώσει τον τομέα της πληροφορικής, προσφέροντας κατ' απαίτηση και οικονομικά αποδοτική πρόσβαση σε μια κοινόχρηστη δεξαμενή παραμετροποιήσιμων υπολογιστικών πόρων, όπως δίκτυα, διακομιστές, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες. Ως εκ τούτου, πολλές εταιρείες μεταφέρουν ολοένα και περισσότερο τα φορτία εργασίας τους, όπως εφαρμογές, υπηρεσίες και επιχειρησιακές διαδικασίες, στο υπολογιστικό νέφος. Ωστόσο, η αυξανόμενη εξάρτηση από το υπολογιστικό νέφος έχει συνοδευτεί από αύξηση των κυβερνοεπιθέσεων, ιδίως εκείνων που βασίζονται σε τεχνικές κοινωνικής μηχανικής. Οι επιθέσεις κοινωνικής μηχανικής επιδιώκουν να παραπλανήσουν ή να χειραγωγήσουν άτομα, με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε συστήματα ή ευαίσθητα δεδομένα.

Η παρούσα εργασία παρουσιάζει μια ολοκληρωμένη εξέταση των επιθέσεων κοινωνικής μηχανικής στο πλαίσιο του υπολογιστικού νέφους. Περιλαμβάνει λεπτομερή ταξινόμηση των τύπων επιθέσεων, ανάλυση των σχετικών κινδύνων, καθώς και συγκριτική αξιολόγηση των αντίστοιχων αμυντικών μηχανισμών βάσει ορισμένων κριτηρίων. Κύριος στόχος της διπλωματικής είναι η ενίσχυση της ευαισθητοποίησης απέναντι στις απειλές κοινωνικής μηχανικής και η παροχή κατευθυντήριων γραμμών για την αντιμετώπισή τους σε περιβάλλοντα υπολογιστικού νέφους.

**Λέξεις κλειδιά:** Υπολογιστικό νέφος, επιθέσεις κοινωνικής μηχανικής, ταξινόμηση επιθέσεων, κυβερνοεπιθέσεις, ανάλυση κινδύνων, αμυντικοί μηχανισμοί, ενίσχυση ευαισθητοποίησης.

# Table of Contents

**1. Introduction** **11**
1.1 Cloud Computing and Social Engineering Attacks 11
1.2 Thesis Contribution 13
1.3 Thesis Structure 15
**2. Security Threats and Risks in the Cloud** **16**
2.1 A Background of Cloud Computing 16
2.1.1 Software as a Service (SaaS) 17
2.1.2 Platform as a Service (PaaS) 20
2.1.3 Infrastructure as a Service (IaaS) 23
2.2 Cloud Computing Vulnerabilities 27
2.2.1 Human Factors 32
2.2.2 Technological Factors 37
2.2.3 Human And Technological Factors 40
2.3 Cloud Threat Assessment 42
2.4 Associated Threats 45
**3. Social Engineering Attacks on Cloud** **47**
3.1 Social Engineering Attack Definition 47
3.2 Attacks Dimensional Classification 48
3.3 Different types of Social Engineering Attacks 51
3.3.1 Impersonation 52
3.3.2 Shoulder surfing 53
3.3.3 Dumpster diving 53
3.3.4 Phishing attacks 53
3.3.5 Baiting attacks 55
3.3.6 Tailgating attacks 57
3.3.7 Pop-up windows 57
3.3.8 Scareware 58
3.3.9 Quid pro quo 58
3.3.10 Reverse Social Engineering Attacks 59
3.4 Social Engineering Attacks and Cloud Computing: The Relationship 60
3.4.1 The Cloud as a Medium and Target 60
3.4.2 Correlating SE Attack Types with Cloud User Roles 61
3.4.3 Reported Frequencies and Trends 63
3.4.4 Real-World Incidents 63
3.4.5 Social Engineering as a Precursor to Technical Cloud Attacks 64
**4. Review Methodology** **65**
4.1 Information Sources 66
4.2 Search Strategy and Pattern 67
4.3 Article Selection And Quality Assessment Process 68
4.4 Final Selection Summary 70

4.4.1 Tracking the Field's Evolution 72
**5. Prevention and Mitigation techniques 73**
5.1 User Awareness and Education 73
5.1.1 Security Awareness Training 74
5.1.2 Social Engineering Awareness Campaigns 77
5.1.3 Best Practices for Passwords and Authentication 79
5.2 Technical Controls/Measures 82
5.2.1 Multi-Factor Authentication (MFA) 82
5.2.2 Authorization and Access Control Models 84
5.2.3 Data Protection 85
5.2.4 Network Segmentation 87
5.2.5 Intrusion Detection and Prevention 88
5.2.6 Sandboxing 89
5.2.7 Threat Emulation 90
5.2.8 Environment Isolation 92
5.2.9 Identity-Based Forensics 93
5.2.10 Behavioral Analytics 93
5.2.11 Summary and Evaluation of Technical Controls 94
5.3 Incident Response and Business Continuity Planning 96
5.3.1 Creating an Incident Response Plan 96
5.3.2 Regular Security Assessments and Testing 96
5.3.3 Recovery Planning 99
5.4 Vendor Management and Due Diligence 100
5.4.1 Cloud Provider Evaluation 100
5.4.2 Security-Aware Service Level Agreements (SLAs) 102
5.4.3 Regular Vendor Audits and Reviews 104
5.5 Conclusions 106
**6. Challenges, Research Gaps and Future Directions 108**
6.1 Lack of Focus on Psychological Components and Adaptive Training Tactics 108
6.2 Adaptive Training Models 109
6.3 Lack of Advanced Detection Techniques 109
6.4 Social Engineering in Edge and Fog Computing Environments 110
6.5 User Privacy Compromise 111
6.6 Missing Links Between Correlated SE Attacks 112
6.7 Lack of Assurance of Regulation and Compliance 112
6.8 Summary 113
**7. Conclusions 114**
**Bibliography 117**

# List of Tables


| Table Number | Table Title | Section | Page |
|---|---|---|---|
| Table 3.1 | Social Engineering Attack Classification Table | 3.3.0 | 60 |
| Table 3.2 | Correlating SE Attack Types with Cloud User | 3.4.2 | 63 - 64 |
| Table 5.1 | Comparison of Training Approaches for SE | 5.1.3 | 77 |

# List of Figures


| Figure Number | Title | Section | Page |
|---|---|---|---|
| Figure 2.1 | Classification of Cloud Vulnerabilities by Origin Category | 2.2 | 29 |
| Figure 3.1 | Social Engineering Attack Types | 3.3 | 50 |
| Figure 4.1 | Distribution of Retained Articles by Source Type | 4..4 | 67 |
| Figure 4.2 | Number of Retained Publications per Year (2016–2024) | 4.4 | 68 |
| Figure 4.3 | Distribution of Publications by Publisher | 4.4.1 | 69 |

# List of Acronyms

| Acronym | Meaning |
|---|---|
| API | Application Programming Interface |
| APT | Advanced Persistent Threat |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CSA | Cloud Security Alliance |
| DoS | Denial of Service |
| DR | Disaster Recovery |
| GDPR | General Data Protection Regulation |
| IaC | Infrastructure as Code |
| IAM | Identity and Access Management |
| IaaS | Infrastructure as a Service |
| IDPS | Intrusion Detection and Prevention System |
| MFA | Multi-Factor Authentication |
| NIST | National Institute of Standards and Technology |
| PaaS | Platform as a Service |
| SaaS | Software as a Service |
| SE | Social Engineering |
| SIEM | Security Information and Event Management |
| SLA | Service Level Agreement |
| VM | Virtual Machine |

# 1. Introduction

## 1.1 Cloud Computing and Social Engineering Attacks

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, 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."(*Mell, P., & Grance, T. , 2011).* Cloud computing allows users to access these computing resources whenever and wherever they need them. On-demand self-service, broad network / ubiquitous access, scalability, multitenancy, and measured or metered service are the six basic features that characterize cloud computing.

In the realm of information technology, the field of cloud computing is one that is seeing significant expansion (Smith, 2023). As a result of the advent of resource virtualization as a service, network, storage, server, application, and service provisioning can now be tailored to the specific requirements of individual users and organisations. With cloud computing, users are able to access a shared pool of IT resources that are both controlled and expandable from any location in the world as long as they have an internet connection. Because of this, small, medium and big-sized firms will only be invoiced for the cloud services that they really utilise, which will result in a reduction in their capital expenditures and operational costs. Consequently, an increasing number of organizations are migrating their workloads, including applications, data, and business processes, to the cloud in order to leverage its scalability, flexibility, and cost-efficiency.

On the other hand, the number of cyber attacks has been on the rise, particularly during the COVID-19 pandemic, which has coincided with the surge in popularity of cloud computing (Khatri, Cherukuri & Kamalov, 2023). According to the findings of the most recent edition of the annual Verizon Data Breach Investigation Report, the number of data breaches that occurred as a result of social engineering attacks has significantly increased (Verizon, 2023). According to the findings of the survey, 85 percent of data breach occurrences in 2021 were caused by human mistakes. While not all of these mistakes are directly attributed to social engineering, this figure strongly suggests that a significant portion may have involved manipulation or deception of users, core elements of social engineering attacks.

Attacks that include social engineering have emerged as a primary source of worry for the security of cloud computing. Hackers, now, have an easy platform to carry out social engineering attacks due to the widespread adoption of cloud computing. In order to unauthorized access systems, attackers take advantage of the human factor that is present in various forms in a system by impersonating or scamming users via email and phone so as to disclose their respective credentials, as well as deriving (e.g., from disclosed personal data) and exploiting user credentials that are not strong enough.

The Advanced Persistent Threat, often known as APT, is particularly well-suited to the cloud environment since the objective of the attacker is to steal data by infiltrating a network, e.g., utilizing spear phishing, and remaining undiscovered for a considerable amount of time (Johnson & Miller, 2023). The primary aim of employing such tactics is to acquire sensitive data or valuable information from the system. However, the consequences of APTs can extend beyond mere data theft. The obtained information can be leveraged to facilitate a wider breach, inflict financial damage, compromise system integrity, or cause reputational harm. Thus, APTs pose a multifaceted threat to cloud environments, necessitating robust defense mechanisms to counteract both the immediate and long-term impacts of such attacks.

Given the increasingly human-focused nature of data breaches, as one observer aptly noted, "**Why waste your efforts on cracking passwords when you can ask for them**?", it becomes clear that organizations must prioritize user awareness and education alongside technical controls for effective security, especially in the context of Social Engineering attacks.

User awareness and education are undeniably critical components in mitigating the risks of social engineering attacks. Educated users can act as the first line of defense, identifying suspicious activities and avoiding potential traps. However, while these measures are indispensable, they alone are not sufficient to counter the sophisticated tactics used by attackers. Therefore, it is equally important to implement robust technical controls and security measures, such as multi-factor authentication, access control and authorization, encryption and data protection, and network segmentation and monitoring. These technical measures play a vital role in creating a multi-layered defense strategy, enhancing the overall security posture, and mitigating the risks posed by APTs, social engineering and other kinds of attacks.

## 1.2 Thesis Contribution

While social engineering attacks and counter-measures have been analyzed in depth in the literature, their connection with cloud computing has not yet been fully unveiled. To this end, the goal of this thesis is to highlight this connection, analyzing how well cloud computing environments are vulnerable to social engineering attacks, which kinds of attacks are the most dangerous in such environments and which kinds of measures can be applied in order to prevent, detect and mitigate such attacks.

Based on the above multi-fold goal, the main contributions of this thesis are the following:

- We provide an extensive and in-depth explanation and analysis of the concept of social engineering attacks, the steps that criminals take to carry them out, as well as examples from the real world that show the significant losses that many large companies have suffered as a result of being exposed to such attacks.
- Our thesis introduces an expanded framework to further enrich an existing classification (proposed by Salahdine and Kaabouch (2019)), which has categorized social engineering attacks based on three dimensions: operator, deception techniques, and communication style. Our framework integrates these established dimensions with novel elements specific to cloud computing environments, creating a more comprehensive taxonomy tailored to the current and emerging threats in this domain. This newly presented classification framework, therefore, constitutes a significant contribution to our research.
- Subsequently, we employ a rigorous and systematic methodology to identify and compare various defense strategies that businesses and organizations can utilize to lessen the risks of social engineering (SE) attacks and prevent their success in cloud computing environments. We aimed to incorporate strategies that address both the human and technological factors contributing to the success of these attacks. These strategies were carefully selected based on their efficacy in addressing the security gaps and vulnerabilities in existing (cloud) systems. The selection of these strategies was indeed primarily driven by their relevance in addressing social engineering attacks. However, their effectiveness in filling other security gaps and mitigating

vulnerabilities in existing systems also played a significant role in their inclusion in our research. Moreover, in the comparison and evaluation of these strategies, we considered various relevant criteria, such as their efficacy in mitigating threats, ease of implementation, cost-effectiveness, and adaptability to evolving attack strategies. Thus, our study provides a comprehensive examination of potential strategies and offers valuable insights into their benefits and limitations in thwarting social engineering attacks in the cloud.

- In addition to these broader defense strategies, we also provide a set of practical security measurestailored to preventing specific types of social engineering attacks in cloud environments. These measures serve as complementary, user-focused actions that can be easily implemented by individuals or organizations to enhance daily cloud security practices. They are designed either specifically for cloud-based contexts or can be readily adapted to them. This differentiation allows our work to address both strategic, system-level defenses and operational, user-level safeguards, offering a layered approach to security.
- Finally, we outline remaining challenges and provide directions for future work in order to better cope with SE attacks in cloud computing environments.

## 1.3 Thesis Structure

The remainder of this thesis is structured as follows:

- **Chapter 2** introduces the key security threats and risks associated with cloud computing, including both technological and human-centric vulnerabilities.

- **Chapter 3** focuses specifically on social engineering attacks in cloud environments, offering definitions, real-world examples, and a comprehensive classification framework that expands upon existing taxonomies.

- **Chapter 4** presents the research methodology and literature review process used to identify relevant sources and structure the analysis of defense strategies.

- **Chapter 5** discusses in detail the prevention and mitigation strategies and measures for social engineering attacks in cloud computing, categorized into user awareness, technical controls, incident response planning, and vendor management.

- **Chapter 6** highlights open challenges, research gaps, and future directions in the field, emphasizing areas where further study and innovation are needed to enhance security against social engineering threats.

- **Chapter 7** presents the conclusions of the thesis, summarizing the key findings, emphasizing the importance of integrating human and technological defense strategies, and outlining potential gaps for future research.

# 2. Security Threats and Risks in the Cloud

## 2.1 A Background of Cloud Computing

The term 'cloud computing' refers to the on-demand delivery of computing resources, such as servers, storage, applications, and services, over the internet. Cloud computing can be seen as a specific kind of utility computing, which includes various forms of distributed computing. This example has brought about a significant change in the way businesses manage their information technology (IT) resources. Compared to more traditional forms of IT infrastructure, cloud computing offers superior scalability, flexibility, and cost-effectiveness (Mell & Grance, 2011).

In the realm of cloud computing, understanding delivery models is essential as they delineate the level of abstraction and control that users have over the computing resources they utilize (Smith, 2023). A delivery model in cloud computing refers to the way cloud services are provided to users, specifying the scope of services offered and the responsibilities of both the service provider and the user.

There are three primary delivery models in cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Cloud delivery models offer substantial benefits to organizations, yet they also introduce novel security concerns and threats that require careful attention. Each from the three dominant models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) - presents unique security vulnerabilities. It is worth noting that users who are less familiar with the intricacies of cloud security may be more susceptible to manipulation techniques, such as phishing scams. Hence, in cloud environments, social engineering attacks can be particularly effective.

Thus, analyzing these delivery models is crucial as they introduce unique security challenges, particularly in the context of social engineering attacks. In the subsequent sections, we will delve into the advantages and security issues associated with each model, focusing specifically on how they intersect with social engineering threats. By examining these models through the lens of social engineering attacks, we aim to identify vulnerabilities and develop targeted strategies to mitigate risks and enhance security in cloud computing environments (Johnson & Miller, 2023).

### 2.1.1 Software as a Service (SaaS)

The acronym SaaS stands for "software as a service," a cloud computing model where software programs are hosted in a cloud environment and accessed via the internet through web browsers or thin clients. Examples of SaaS include Salesforce[1], Microsoft Office 365[2], and Google Apps[3].

With SaaS, users are freed from infrastructure, platform and application management as the provider maintains full control of all these management activities. However, in this model, user data and behavior can become attractive targets for attackers. Thus, it is crucial to understand that even though the provider manages the complete application stack and might have suitable security measures, users are still responsible for maintaining safe and secure practices (e.g., by utilising strong passwords such that their application accounts are not easily hacked).

The use of SaaS has grown more common among businesses that wish to lessen the financial and administrative burden of administering and managing software applications, such as those that have been traditionally bought from third-party software vendors by following the traditional software delivery model. SaaS providers are responsible for the hosting infrastructure, the maintenance, updating and scaling as well as for providing support for the software (application) that they offer in the form of a cloud service. This frees up organisations to concentrate on their primary business operations.

On the cost side, SaaS providers often offer subscription-based or pay-as-you-go pricing plans, which give businesses the ability to pay only for the resources they actually use. This not only minimizes investment costs by eliminating the need for infrastructure, but it also reduces operational costs as the maintenance and updating of software services, which are traditionally resource-intensive activities, are handled by the service provider. Thus, compared to traditional software delivery models, SaaS can significantly reduce both capital and operational expenses.

Scalability is one of the primary advantages offered by SaaS, ensuring that the service level remains stable (as e.g., promised in the Service Level Agreements - SLAs with the clients) even when the load

[1] https://www.salesforce.com/eu/
[2] https://www.microsoft.com/en-us/microsoft-365
[3] https://workspace.google.com/

increases. This is particularly valuable for businesses with fluctuating demands. Businesses can efficiently adjust their usage based on their requirements, leveraging the scalability provided by the SaaS provider. This scalability allows businesses to expand or reduce their usage of software applications without worrying about the underlying infrastructure, as it is managed by the service provider. The ability to adapt to changing business needs, without the necessity for large upfront infrastructure investments, is one of the significant benefits of using SaaS.

Another key advantage of Software as a Service (SaaS) applications lies in their user-centric design. SaaS applications are often designed with a wide range of users in mind, making them user-friendly and accessible to customers with varying degrees of technical skills. This intuitive design extends to the user interface (UI) of these applications. SaaS applications typically feature uniform, easily navigable, and responsive UIs, which can be rendered in multiple platforms, including mobile ones. This consistency in design not only aids in user navigation but also reduces the learning curve for new users, enabling them to quickly adapt to and efficiently use the software. Furthermore, SaaS providers often prioritize user experience in their design, resulting in applications that are responsive, meaning they quickly react to user inputs, and adaptable, adjusting their display and functionality based on the user's device, location, or preferences. These features enhance the overall user experience, contributing to the growing popularity of SaaS applications.

One further advantage of using SaaS is the simplicity of its setup. The fact that software as a service (SaaS) applications are provided over the Internet means that users may use them from any location as long as they have a connection to the Internet. This makes SaaS applications particularly well-suited for remote work and teams that are scattered across many locations. In addition, the provider of a SaaS service will often automatically update the software on a regular basis. This ensures that customers will always have access to the most recent features and security patches.

On the other hand, SaaS brings with it a new set of security risks and challenges that need to be handled. Given their internet-based nature, Software as a Service (SaaS) applications are potentially exposed to a variety of cyber threats, widely known to traditionally hold for web applications (such as, DoS, SQL or command injection, XSS, CSRF, etc.), which include but are not limited to, social engineering attacks like phishing and data breaches.

The accessibility and widespread usage of SaaS applications present lucrative opportunities for cybercriminals (Kumar, et al., 2020). Social engineering attacks leverage human psychology to manipulate individuals into divulging confidential information, bypassing technical security measures. Phishing, one of the most prevalent social engineering methods, exploits users' trust to deceive them into revealing their credentials or sensitive information (Kim, et al., 2019). As such, it can lead to accessing the sensitive/personal information of the user as managed by the application or to the execution of application-related actions (e.g., purchasing goods) on behalf of the user (once the attacker utilises the disclosed user credentials).

Attackers frequently target users of SaaS applications rather than the applications or infrastructure themselves (Mohammadi, et al., 2020) (as it is easier to deceive users than conducting successful attacks on cloud applications and infrastructures). By compromising user accounts through phishing or other social engineering tactics, attackers can gain unrestricted access to sensitive data hosted on the SaaS platform.

However, this does not mean that SaaS applications are not targeted as a whole by the attackers. SaaS applications often involve the handling of sensitive data, making them prime targets for attackers seeking unauthorized access to valuable information (Zhang & Liu, 2021). Thus, any successful breach (at the application level) can have severe implications, potentially resulting in data leakage, financial losses, and reputational damage for the affected organization. This is due to the fact that an application-level breach can extend over the whole user set managed by the SaaS application in contrast to an attack that targets only a specific user (e.g., a phishing attack that leads to the user’s account violation in the affected SaaS).

Therefore, while SaaS applications offer considerable benefits in terms of scalability and cost-effectiveness, their susceptibility to social engineering attacks underscores the importance of robust security measures and user education initiatives (Alazab, et al., 2019). Continuous vigilance and proactive defense strategies are essential to mitigate the risks posed by social engineering threats in SaaS environments.

According to Gartner (2021), organizations should thoroughly assess potential SaaS providers in terms of the security posture of their offered applications and services, including their data protection policies, compliance with industry standards (e.g., ISO/IEC 27001, SOC 2), vulnerability

management practices, and incident response capabilities. Additionally, organizations should configure access controls to meet security requirements and preferences, and ensure data encryption in transit. Furthermore, employee training and awareness programs are essential in empowering users to recognize and prevent social engineering attacks. This can help mitigate risks associated with deceptive tactics that seek to exploit human vulnerabilities, which are prevalent in environments that facilitate user communication and data sharing.

In conclusion, software as a service (SaaS) has developed into a well-liked alternative for businesses that want to cut the expenses and complexity of administering software programs that they have traditionally bought. Scalability, ease of use, setup simplicity, and accessibility are just some of the numerous advantages offered by SaaS. However, organisations must also be aware of the security risks and dangers connected with SaaS and take proper measures to mitigate them in order to avoid potential damage.

### 2.1.2 Platform as a Service (PaaS)

Platform as a Service, often known as PaaS, is a computing paradigm that allows software developers to develop, test, and deploy their applications in a cloud platform via the Internet. Heroku[4], Google App Engine[5], and Microsoft Azure App Service[6] are a few examples of similar platforms.

PaaS hosts development tools on cloud infrastructure, accessible over the internet through APIs, web portals, or gateway software. Besides managing the underlying infrastructure (or delegating this to a well-known cloud infrastructure provider), PaaS providers also oversee runtime, middleware, and operating systems. However, users have control over their application development and operation. While this model simplifies development and operational overhead, it introduces potential vulnerabilities at both the application and platform levels. For example, inadequate input validation can lead to application-level attack, whereas flaws or misconfigurations in the runtime environment or middleware stack can expose the underlying platform to exploitation if not properly secured (Devi & Ganesan, 2015).

[4] https://www.heroku.com/
[5] https://cloud.google.com/appengine
[6] https://azure.microsoft.com/en-us/products/app-service

The PaaS paradigm of cloud computing enables software developers to construct, test, and deploy their applications via the Internet. PaaS frees businesses from the obligation of making major initial investments in infrastructure, making it possible for them to build and deploy applications in well-established platforms offered and maintained by third-parties. PaaS providers oversee the infrastructure, including the operating system, as well as the platform itself, including middleware and the required runtime environment. This allows developers to concentrate on developing the application itself in the offered platforms such that they can become more productive

Another advantage of using PaaS is that it is flexible. PaaS offers a standardized development environment, which frees developers from the need to worry about the underlying components of this environment and the infrastructure that hosts them. This enables developers to concentrate solely on the process of developing their applications. PaaS providers also often offer a variety of platforms that covers a diverse combination of development tools and frameworks, giving developers the ability to select the platform that is the most suitable to their individual requirements. Further, each platform is always up-to-date, incorporating the latest versions and patches of all relevant platform components, such as middleware, runtimes and application frameworks and tools.

While Platform as a Service (PaaS) offers a flexible and scalable environment for developers, this model also introduces specific security vulnerabilities and threats that must be addressed to ensure a secure cloud environment. These can include:

1. *Inherited Software Vulnerabilities*: PaaS environments often involve multiple software components, including third-party libraries and dependencies. These can introduce inherited vulnerabilities if not properly managed and updated. Regular scanning and patching of these vulnerabilities are crucial to prevent potential exploits (Nordic Defender, 2023) .
2. *Configuration Issues*: Misconfigurations in PaaS can lead to significant security risks, including unauthorized access and data leaks. Ensuring proper configuration management and adherence to best practices is essential to mitigate these risks (Moghaddasi et al., 2016).
3. *Access Control Weaknesses*: Implementing robust role-based access control (RBAC) is critical in PaaS environments. Inadequate access controls can lead to unauthorized access and potential data breaches. Properly configuring these controls to align with organizational policies is necessary (Bastani et al., 2016).

4. *Data Encryption*: Both data at rest and data in transit must be encrypted to protect against interception and unauthorized access. This is particularly important for sensitive information handled within PaaS applications (Nordic Defender, 2023).

PaaS platforms are also susceptible to social engineering attacks, which can be particularly damaging due to the nature of the services provided. Such attacks can include:

- *Phishing*: Attackers may target developers and administrators through phishing emails, tricking them into revealing their credentials or downloading malicious software. These attacks can lead to unauthorized access to PaaS environments, where attackers can manipulate or steal data (Ranganathan et al., 2016).
- *Pretexting and Baiting*: Employees with access to the PaaS environment can be manipulated through social engineering techniques to perform malicious actions. Regular training and strict access controls can mitigate this risk (Ranganathan et al., 2016) .
- *Impersonation*: Attackers can impersonate legitimate users or support personnel to gain access to sensitive areas of the platform.
- *Credential Theft*: Social engineering techniques can be used to steal login credentials, giving attackers access to the platform where they can manipulate or steal data.

The potential for attack not only lies in the applications that developers build on the platform, which could contain their own vulnerabilities, but also in the platform's APIs. If not properly secured, these APIs could present security holes (misconfigurations or vulnerabilities like lack of input validation) that attackers could exploit. Therefore, while PaaS offers many advantages for developers, it is of utmost importance that platform providers, as well as developers, emphasize and prioritize security measures in order to mitigate these associated risks. (Cloud Security Alliance, 2016).

Furthermore, the analysis of PaaS disadvantages should encompass a broader range of factors, including both security and non-security-related issues. These may include considerations, such as performance limitations, vendor lock-in risks, interoperability challenges, scalability constraints, and potential legal and compliance complexities. By thoroughly evaluating and understanding these disadvantages, organizations can make informed decisions and implement necessary measures to effectively navigate the PaaS landscape.

In conclusion, Platform as a Service has turned into a popular option for businesses that want to build and deploy their own applications but do not desire to make a substantial initial investment in platforms and respective hosting infrastructures. PaaS has several advantages, some of the most notable of which include scalability, flexibility, and simplicity of deployment. However, organisations must also be aware of the security risks and threats associated with PaaS and take appropriate measures to mitigate them in order to avoid any potential consequences.

### 2.1.3 Infrastructure as a Service (IaaS)

IaaS refers to Infrastructure as a Service, which is a paradigm of cloud computing that delivers virtualized computer resources, including servers, storage, and networking through the Internet. Amazon Web Services (AWS)[7], Microsoft Azure[8], and Google Cloud Platform[9] are a few examples of cloud computing platforms that offer such infrastructural services.

In IaaS, users are provided with virtualized computing resources over the internet. While this service eliminates the need for physical infrastructure, it demands that users manage their applications, data, middleware, and operating systems on top of the service's virtual infrastructure. This setup makes IaaS environments potentially vulnerable to security attacks if users fail to implement robust security measures.

IaaS enables businesses to adjust the size of their computing resources in accordance with their current requirements without requiring to make major initial investments in new hardware. IaaS providers are responsible for managing the infrastructure of the (offered virtual) computing resources, as well as their maintenance and support, while (cloud consumer) organisations retain control over the operating systems, programs, and data that will be placed in such resources.

The flexibility of IaaS to deliver resources on-demand is recognized as one of its primary advantages. Organizations can provision on-demand as many resources as needed, allowing for agility and adaptability in meeting fluctuating demands. In this context, it is important to clarify that scalability pertains to the flexible adjustment of resources according to needs. By acquiring as many resources

[7] https://aws.amazon.com/
[8] https://azure.microsoft.com/en-us/products/
[9] https://cloud.google.com/?hl=el

as needed, the application performance level can remain stable, thus enabling the application to be adapted accordingly based on the varying customer workload

IaaS providers often offer pricing plans based on the pay-as-you-go model, where businesses are billed for the actual usage of the offered infrastructural services on an hourly basis. This pricing approach enables organizations to pay only for the resources that they utilize, offering flexibility and cost-effectiveness in managing their infrastructure costs. Due to this, companies are able to quickly scale on-demand the amount of computing resources they use, either up or down, depending on their requirements, without having to make a substantial initial investment in hardware. In addition, IaaS providers often give access to a broad variety of computing resources, giving businesses the ability to select the resources that are the most suitable (in terms of the resources‘ characteristics) to their requirements.

Flexibility is yet another advantage that comes with utilizing IaaS. IaaS gives businesses the ability to exercise control over the underlying computing environment, including the operating system, programs, and data, which enables them to tailor their computing environment to match the requirements of their particular operations. In addition, IaaS providers often supply to their customers a variety of management tools, which makes it simple for businesses to take control of the (virtualized) computing resources that they have rented.

The main advantages of IaaS are the following:

- *Resource Scalability*: IaaS offers the ability to quickly scale computing resources up or down based on the demand. Businesses can easily adjust their resource allocation to accommodate fluctuations in workload, ensuring optimal performance and cost efficiency.
- *Geographic Flexibility:* With IaaS, organizations can deploy and access resources from multiple geographic locations. This allows for improved redundancy, disaster recovery capabilities, and the ability to serve customers in different regions with reduced latency.
- *Reduced Capital Expenditure:* By leveraging IaaS, businesses can eliminate or significantly reduce the need for upfront capital investment in hardware infrastructure. This shifts the financial burden from large upfront costs to ongoing operational expenses, resulting in improved financial flexibility.

- *Rapid Provisioning:* IaaS enables rapid deployment of computing resources. Organizations can quickly provision virtual machines, storage, and networking components, reducing the time required for setting up infrastructure and accelerating time-to-market for new projects.
- *Enhanced Security and Compliance:* Reputable IaaS providers often implement robust security measures and adhere to industry-standard compliance frameworks. By leveraging these providers' expertise and infrastructure, businesses can benefit from enhanced security features and better meet compliance requirements.
- *Disaster Recovery and Business Continuity:* IaaS providers typically offer features and services for data backup, disaster recovery, and business continuity planning. This ensures that businesses can easily recover their systems and data in the event of a disruption or disaster, minimizing downtime and data loss.

Reflecting on the key attributes of the Infrastructure as a Service (IaaS) model, organizations are privy to significant advantages. It is essential to note that these advantages, already discussed in earlier sections, are not merely supplementary. Instead, they represent the core benefits that make IaaS an appealing solution for organizations.

IaaS does, however, introduce unique security challenges that stem from the cloud delivery model and the complexity of the virtualized environment. To clearly understand these challenges, it is essential to distinguish between vulnerabilities, attacks, and risks, which are often interrelated but conceptually distinct.

**Vulnerabilities in IaaS**

- *Improper Isolation of Resources*: In a multi-tenant environment, where multiple users share the same underlying infrastructure, there is a risk of inadequate isolation. If not properly implemented, this can potentially allow unauthorized access or data leakage between different users' virtual resources (deployed on the same physical resource).
- *Vulnerabilities in Hypervisors:* Hypervisors, the software that enables virtualization, can introduce security risks if they are not hardened or not properly configured and secured. Exploiting vulnerabilities in hypervisors can potentially lead to unauthorized access or control over both virtualized and physical resources - this is due to the fact that hypervisors manage

virtual resources on top of the physical resources on which they operate. Additionally, they can lead to various security issues over user data (e.g., exposure of private/sensitive data).

- *User Misconfigurations and Mistakes:* User mistakes, such as misconfigurations, weak access controls, or forgotten credentials, can create security vulnerabilities within the IaaS environment. It is important for users to follow best practices and employ proper security measures to prevent these types of issues.
- *Insecure APIs and Communication Channels:* Cloud management APIs and remote access interfaces (e.g., SSH, REST APIs) may be vulnerable if not protected using secure protocols or strong authentication mechanisms.

**Common Attacks in IaaS**

- *Distributed Denial-of-Service (DDoS) Attacks:* IaaS environments can become targets for DDoS attacks. These attacks aim to disrupt services and make them unavailable by overwhelming the infrastructure with a flood of illegitimate traffic.
- *Side-Channel Attacks:* These target shared hardware resources, attempting to infer sensitive data from co-located VMs.
- *VM Escape Attacks:* Exploiting hypervisor vulnerabilities, attackers can break out of the virtual machine to access the host or other guest VMs.
- *VM Migration Attacks:* Targeting live migration processes, attackers may intercept data in transit if migration is not securely managed.

**Risks and Consequences**

- *Data Breach:* Unauthorized access to sensitive data due to isolation failure or stolen credentials.
- *Data Corruption or Loss:* Malicious activity or operational failures can lead to loss or compromise of critical business data.
- *Service Disruption:* DDoS or resource abuse may result in downtime, affecting service availability and business continuity.

By highlighting these additional security concerns, a more comprehensive understanding of the potential security issues faced in IaaS setups can be attained.

To conclude, Infrastructure as a Service (IaaS) has turned into a well-liked option for businesses that want to scale up or down their computing capabilities depending on their requirements and workload, but do not want to make a substantial initial investment in hardware. IaaS comes with a plethora of advantages, including scalability, cost reduction and flexibility. However, organisations (both cloud providers and customers) must also be aware of the security risks and dangers connected with IaaS and take proper measures to mitigate them in order to avoid any potential consequences.

## 2.2 Cloud Computing Vulnerabilities

Cloud computing introduces a new set of security challenges that need to be handled in order to protect the confidentiality, integrity and availability of data stored in the cloud. The human elements and the technology aspects are the two primary groups that may be used to cluster such hazards (Reason, 2016).

The term "technological factors" refers to the vulnerabilities that are caused by the technology itself. Examples of technological factors include software flaws, inadequate resource isolation, and use of insufficient encryption algorithms/schemes. Threats posed by malware, denial-of-service (DoS) attacks, and data breaches are examples of risks that can be attributed to both technological and human elements. While malware attacks are often associated with technological factors, they can also result from human errors, such as unknowingly downloading infected files or falling victim to social engineering tactics. Similarly, data breaches can be caused by human actions, such as mishandling sensitive information or becoming victims of phishing scams. Although Denial of Service (DoS) attacks are typically launched externally, the impact of such attacks can be exacerbated by technical vulnerabilities, such as flaws in network protocol implementations or system architecture, as well as by human-related factors like system misconfigurations or the improper implementation of security measures, including insufficiently configured intrusion detection systems (IDS). Therefore, it is important to recognize the interplay between technological vulnerabilities and human factors when assessing security risks in cloud environments.

Cloud environments are becoming increasingly popular as a means of storing and transferring data. Thus, inadequate encryption is a key vulnerability in cloud settings since it may lead to the exposure of sensitive information and enable unauthorized access or data manipulation. While such

vulnerabilities are often considered technological in nature, it is important to distinguish between two contributing factors: (a) technological flaws, such as the use of outdated or inherently weak encryption algorithms embedded in software or hardware systems, and (b) human errors, such as the misconfiguration of encryption settings or the choice of insufficiently strong keys during implementation. While both types of issues can compromise security, this distinction helps clarify the root causes of encryption-related vulnerabilities in cloud infrastructures (NIST 2016).

According to Cloud Security Alliance (2016), the disclosure of sensitive data or the compromise of cloud resources can result from both human-based errors and technological vulnerabilities. Human errors often involve the improper configuration or management of cloud services, while technological vulnerabilities stem from flaws in the underlying software or infrastructure. Below are examples that illustrate both types:

- *Misconfigured Access Controls (Human Error):* Improperly configured access controls, such as granting excessive permissions or not revoking access when necessary, can result in unauthorized users gaining access to sensitive data or cloud resources.
- *Lack of Proper Monitoring and Logging (Both Human and Technological):* Insufficient monitoring and logging of cloud resources and activities can hinder the timely detection of security incidents or breaches. This may stem from human-related issues, such as the incorrect selection, configuration, or use of monitoring tools, or from technological flaws, such as limitations or implementation errors in the tools themselves. In both cases, the result can be undetected unauthorized access, data exfiltration, or prolonged attacks with greater impact.
- *Unpatched or Outdated Software (Human Error):* Neglecting to apply necessary security patches or updates to cloud systems and software can leave them vulnerable to known exploits and attacks. Attackers can take advantage of these vulnerabilities to gain unauthorized access or exploit system weaknesses.
- *Weak Authentication Mechanisms (Both Human and Technological):* Weak password policies, poor key management, and lack of multi-factor authentication (human errors) combined with vulnerabilities in identity management systems and authentication protocols (technological flaws) increase the risk of unauthorized access.
- *Inadequate Encryption (Both Human and Technological):* Failure to encrypt sensitive data in transit or at rest can expose it to interception or unauthorized disclosure (human errors). Weak

encryption algorithms or improper implementation of encryption mechanisms (technological flaws) can also render data susceptible to compromise.

- *Insecure API Implementations (Technological Flaw):* Cloud services often rely on APIs (Application Programming Interfaces) to enable communication and interaction with external programs and agents. If APIs are not securely implemented or adequately protected, they can be targeted by attackers to gain unauthorized access, manipulate data, or perform malicious actions.
- *Infrastructure Failures (Technological Flaw):* Failures in supporting infrastructure, such as networking, physical security, or platform software can lead to service outages and security breaches if not properly corrected.
- *Improper Resource Isolation (Technological Flaw):* In multi-tenant cloud environments, insufficient separation of virtual machines or containers may lead to side-channel attacks or data leakage between tenants. This vulnerability is architectural and typically stems from flaws in the virtualization layer.

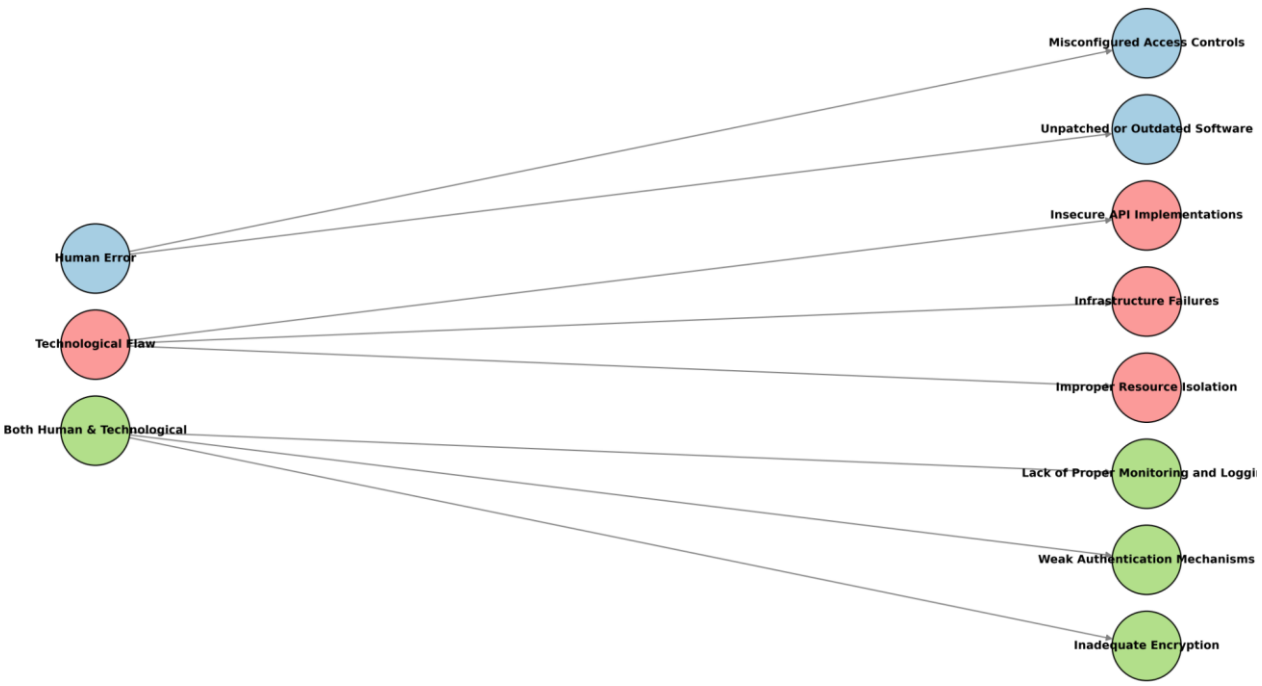


**Figure 2.1**: *Classification of Cloud Vulnerabilities by Origin Category*

It is crucial for organizations to properly set up and configure their cloud services, follow security best practices, and employ robust security measures to mitigate the risks associated with these vulnerabilities. By doing so, they can significantly reduce the chances of sensitive data disclosure and compromise of cloud resources.

In order to protect themselves from these dangers, businesses should put adequate security measures into place, run training and awareness programs, and thoroughly investigate the security posture of any prospective cloud service provider. To effectively mitigate the risks associated with cloud computing, it is crucial to employ a multi-faceted strategy, involving various security measures:

- *Two-Factor Authentication (2FA):* Adding an extra verification step beyond passwords significantly strengthens security. However, the effectiveness of 2FA depends not only on users consistently applying it, but also on the strength and reliability of the second factor (e.g., hardware tokens vs. SMS), as well as the cost, usability, and complexity of its implementation and maintenance.
- *Access Controls :* Enforcing least-privilege policies and regularly reviewing user permissions is essential to preventing unauthorized access. Access control can be managed through structured schemes, such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC), which help ensure users only have access appropriate to their roles or attributes. While these schemes aim to mitigate both human-related errors (e.g., misconfigured permissions or failure to revoke access) and technological flaws (e.g., errors in policy enforcement or control logic), vulnerabilities can still arise if controls are improperly implemented, misconfigured, or inherently flawed.
- *Regular Audits and Monitoring:* Continuously observing cloud system activity and conducting regular audits are essential for early detection of irregular or malicious behavior. Success relies on the attentiveness and responsiveness of security personnel (Røisland, 2019).
- *Employee Training:* Regular training sessions should be held for employees to educate them about the best practices in cloud security and awareness about various threats, including social engineering attacks.
- *Backup and Recovery:* Regular backups combined with tested recovery strategies help organizations quickly restore operations following data loss events. Ensuring these processes are performed correctly requires human diligence.

- *Cloud Security Architecture and Strategy:* Develop and maintain a clear, well-documented security architecture and strategy tailored to organizational needs, ensuring systematic risk management and control implementation.
- *Encryption:* Protecting sensitive information both during transmission and storage is critical. This requires using robust, well-accepted encryption methods with sufficiently large key sizes. Proper encryption helps prevent unauthorized data access (Rosado et al., 2012).
- *Secure APIs:* Developing secure APIs requires a security-aware approach throughout the entire software development lifecycle (SDLC), including planning, design, implementation, testing, and maintenance. Strong authentication, encryption, and input validation are fundamental elements, but alone are not sufficient. Vulnerabilities can arise from both development oversights and systemic issues, underscoring the importance of ongoing security assessments, code reviews, and adherence to secure coding practices.(McGraw, 2006)
- *Firewalls and Intrusion Detection Systems (IDS):* These tools act as frontline defenses by filtering harmful traffic, identifying suspicious activity and automatically responding where possible. Proper setup and maintenance of such measures are vital to protect against network-based threats (Ammann et al., 2002).
- *Security Incident and Event Management (SIEM) Systems:* SIEM platforms collect and analyze security data from various sources in real time, enabling prompt incident identification and response.

Each of these measures plays a significant role in building a secure cloud computing environment. However, the most effective approach will depend not only on the organization's specific security requirements and threat model, but also on its available resources and budget. Since not all security controls can be implemented simultaneously due to cost or complexity, organizations should adopt a risk management approach that evaluates potential threats, available defense options, and associated costs, enabling them to select the most cost-effective and impactful security measures.

Please note that user awareness training and clear policies are essential in mitigating risks associated with human factors. In any case, by addressing both technological and human factors, organizations can establish a comprehensive approach to cloud security.

In conclusion, cloud computing presents new security dangers and concerns that need to be handled in order to ensure that the data stored in the cloud is secure and does not violate any privacy regulations. There are two primary kinds of hazards to confront for this purpose: human factors and technology aspects. Appropriate security measures, such as training and awareness programs, and rigorous screening of cloud providers are vital to managing these risks.

### 2.2.1 Human Factors

In the context of information security, human factors refer to vulnerabilities that arise due to the actions, behaviors, or characteristics of individuals involved in the use, management, or administration of systems. These vulnerabilities can stem from both intentional and unintentional activities. Here are a few examples of human factors in the context of cloud environments:

- *Inability to correctly install security measures:* Users or administrators may lack the necessary knowledge or skills to properly configure and apply security measures in cloud environments, leaving systems exposed to potential threats.
- *Weak password usage:* Users may choose weak or easily guessable passwords, or they may reuse passwords across multiple accounts, which increases the risk of unauthorized access to cloud resources.
- *Lack of awareness and insufficient training:* Users may be tricked into revealing sensitive information or credentials through social engineering tactics, such as phishing. The underlying vulnerability lies in a lack of user awareness or insufficient training on how to recognize and respond to such threats. When exploited, this can lead to unauthorized access to cloud accounts and potential data breaches
- *Inadequate User Access Management:* Improper management of user access privileges, such as failure to revoke access when an employee leaves the organization, can lead to unauthorized access or misuse of cloud resources.
- *Insufficient Security Awareness and Training:* Lack of awareness and understanding among users about potential security threats and best practices can make them more susceptible to social engineering attacks, phishing attempts, or unintentional data exposure.

- *Insider Threats:* Malicious or negligent actions by internal employees with authorized access can pose significant security risks, including unauthorized data access, data theft, or intentional disruption of cloud services.

The statement that users of cloud environments are less familiar with security controls and therefore more susceptible to phishing scams and manipulation is accurate in many contexts. Cloud environments often introduce new security controls and practices that users may not be familiar with, for example, Multi-Factor Authentication (MFA), Identity and Access Management (IAM) role assumptions, or API access tokens. While administrators and security professionals typically understand these mechanisms, end-users and less technical personnel may lack awareness of how they function or why they are critical. A user who does not fully understand the importance or function of temporary session credentials in IAM might, for instance, be tricked via phishing into approving a fraudulent sign-in request or sharing a token. Such social engineering tactics exploit human trust and lack of technical understanding to bypass otherwise robust security controls.

Attacks that are based on social engineering are one of the most important human factor threat associated with cloud computing, targeting unauthorized access to sensitive information or systems through manipulation and deception. Social engineering attacks exploit human vulnerabilities rather than technical weaknesses, and they rely on psychological manipulation to trick individuals into revealing confidential information, performing certain actions, or bypassing security measures. It is important to recognize social engineering attacks as a distinct category of cybersecurity attacks.

Users' lack of knowledge and training on cloud security safeguards and best practices is a critical concern resulting from human factors. Due to this lack of familiarity, users may be more vulnerable to the dangers and risks associated with cloud computing. It is essential to educate and raise awareness among users about cloud security best practices to mitigate potential vulnerabilities and enhance overall security (Cloud Security Alliance, 2016).

In addition, there is the potential for insider attacks that can pose significant risks to cloud environments, as their motivations and potential actions can vary widely. It is crucial to implement access controls not only to prevent intentional or accidental disclosure of sensitive data or cloud resources to attackers but also to address other potential insider threats. (Gartner, 2021).

Insiders may have different objectives that motivate their actions, including:

- *Data Theft:* Insiders might be driven by the desire to steal sensitive data for personal gain, corporate espionage, or to sell the information on the black market.
- *Sabotage:* In some cases, insiders may seek to disrupt cloud services, compromise systems, or cause damage to the organization out of revenge (e.g., if they got fired), dissatisfaction, or ideological reasons.
- *Data Manipulation:* Insiders may attempt to manipulate or alter data within the cloud environment as a means to achieve malicious objectives — such as spreading misinformation, committing fraud, causing financial loss, or damaging an organization's reputation. The act of data manipulation serves as a tactic to realize broader strategic goals and can be particularly difficult to detect in cloud environments without robust monitoring and audit controls.

Insiders can employ various attack techniques, such as:

- *Unauthorized Access:* Insiders may abuse their legitimate access privileges to access sensitive data or systems beyond their intended scope. Such incidents often occur due to insufficiently granular access control policies or a lack of enforcement of the principle of least privilege, allowing users to reach resources they do not strictly need for fulfilling their role.
- *Data Exfiltration:* Insiders may use their authorized access to secretly extract and transfer sensitive data outside the organization's cloud infrastructure.
- *Malicious Code Insertion:* Insiders may introduce malicious code or backdoors into the cloud environment, allowing for unauthorized access or control over systems.

The main outcomes of insider attacks can include:

- *Data Breaches:* Insiders can compromise the confidentiality, integrity, and availability of sensitive data stored in the cloud, potentially leading to financial and reputational damage.
- *Service Disruption:* Insider attacks can disrupt cloud services, causing downtime, loss of productivity, and financial loss for the organization and its customers.
- *Loss of Trust:* Insider incidents erode trust among customers, partners, and stakeholders, damaging the organization's reputation and relationships.

Therefore, implementing proper and sufficient access control is just one aspect of mitigating insider threats. Organizations should also focus on detection mechanisms, monitoring user activities, conducting regular audits, and fostering a culture of security awareness to minimize the risks associated with insider attacks.

In conclusion, human factors can provide major security threats in contexts that are associated with cloud computing. Attacks based on social engineering, a lack of user knowledge and training, and threats from insiders are all examples of human factor concerns that need to be handled to guarantee the data stored in the cloud is secure and there is no intrusion on the user's privacy.

As a means of mitigating these dangers, organizations should implement proper security measures, offer training and awareness programs (educating employees on best practices, recognizing phishing scams, and maintaining strong passwords), and thoroughly investigate any potential cloud service provider (conducting thorough security assessments, reviewing their certifications and compliance measures, and evaluating their track record in terms of security incidents).

Examples of security measures that organizations can implement include:

- *Sophisticated Access Control:* Implementing role-based or attribute access control (RBAC or ABAC), two-factor authentication (2FA), and least privilege principles to ensure that only authorized individuals have access to sensitive data and cloud resources.
- *Encryption:* Encrypting data both in transit and at rest to protect it from unauthorized access. This can include using encryption protocols, such as HTTPS for data transmission, and symmetric encryption algorithms to efficiently secure stored data.
- *Intrusion Detection and Protection Systems (IDPS):* IDPS solutions monitor network traffic and system activity to detect suspicious behavior or known attack patterns. They can generate alerts or take proactive measures (such as blocking IPs or terminating sessions) to prevent intrusions. In the context of insider threats, IDPS can also play a key role in malware detection by identifying unusual file behavior, unauthorized script execution, or known malware signatures, enabling containment actions like quarantining malicious code before it spreads.
- *Antivirus and Anti-Malware tools:* Antivirus and anti-malware tools provide an essential layer of defense by detecting, blocking, and removing malicious software before it can compromise systems or data. In cloud environments, host-based or agent-based antivirus mechanisms can

be integrated into virtual machines or containers, while cloud-native solutions (such as AWS GuardDuty or Microsoft Defender for Cloud) offer continuous threat monitoring and automated remediation. Such tools are particularly relevant for mitigating threats where malicious code may be deliberately or unintentionally introduced into the environment

Examples of training and awareness programs include:

- *Phishing Awareness Training:* Providing employees with training to recognize phishing emails, suspicious attachments, or malicious links, and educating them on the importance of not divulging sensitive information to unauthorized sources.
- *Password Security Best Practices:* Employees should be trained on essential password hygiene principles and best practices, including the creation of strong, unique passwords, the importance of regular password updates, and avoiding password reuse. Training should also promote the use of secure tools, such as password managers, and encourage techniques like using passphrases to enhance memorability without compromising security.
- *Incident Response Training:* Conducting training exercises to familiarize employees with proper incident response procedures, including reporting incidents, preserving evidence, and following established protocols to mitigate and recover from security breaches.

On the other hand, thoroughly investigating cloud service providers involves:

- *Security Assessments:* Conducting comprehensive assessments of the provider's security controls, vulnerability management processes, incident response capabilities, and adherence to industry standards and best practices.
- *Certifications and Compliance*: Reviewing the provider's certifications, such as ISO 27001[10] or SOC 2[11], and evaluating their compliance with relevant regulatory frameworks, such as GDPR[12] or HIPAA[13], depending on the organization's specific requirements.

[10] https://www.iso.org/standard/27001
[11] https://www.aicpa-cima.com/home
[12] https://gdpr.eu/
[13] https://www.hhs.gov/hipaa/index.html

- *Security Incident History:* Investigating the provider's track record regarding security incidents, reviewing their response to past breaches or vulnerabilities, and evaluating their transparency and communication practices.

By implementing these security measures, conducting training and awareness programs, and thoroughly assessing cloud service providers, organizations can enhance their overall security posture and reduce the risks associated with cloud computing.

### 2.2.2 Technological Factors

The term “technological factors” refers to vulnerabilities originating from flaws within hardware, software, or system components that can be exploited to compromise the security of cloud environments. These vulnerabilities typically result from errors in the design, development, implementation, or deployment of such components. Unlike human-factor vulnerabilities, they may be exploited by attackers without requiring direct user interaction or human error.

Common technological vulnerabilities in cloud computing include issues such as insecure APIs, improper resource isolation, unpatched or outdated hypervisors, weak encryption mechanisms, vulnerable virtual machine images, inefficient intrusion detection systems (IDS), and insufficiently scalable Security Information and Event Management (SIEM) platforms. Exploiting these weaknesses can lead to unauthorized access, data breaches, service disruption, or data manipulation. Below are some key technological vulnerabilities relevant to cloud environments, along with recommended mitigation strategies:

- *Improper Resource Isolation:* Inadequate resource isolation in virtual machines (VMs) or containers can lead to unauthorized access or interference between different workloads. To mitigate this, organizations should implement proper isolation techniques, such as high and robust hypervisor or container security, network segmentation, and strong access control.
- *Insecure Hypervisors:* Vulnerabilities in hypervisor software can be exploited to compromise the underlying infrastructure (both VMs and physical machines hosting them). It is essential to keep hypervisors up to date with the latest security patches, to harden them and conduct regular security assessments to identify and remediate any potential vulnerabilities.

- *Inneficient Security Information and Event Management (SIEM) Platforms:* SIEM tools are designed to collect, correlate, and analyze security-related data across systems. However, when these platforms are outdated, for example, no longer supported or patched, they may become vulnerable to known exploits. In addition, outdated or poorly scalable SIEM systems may lack the performance and intelligence needed to process the volume and complexity of cloud environment data, limiting their effectiveness in threat detection and incident response.
- *Inneficient Intrusion Detection Systems (IDS):* IDS solutions monitor network traffic for unusual or harmful patterns. If these systems have inadequate detection algorithms or generate a high rate of false alarms, their practical effectiveness is diminished, leading to delayed or missed identification of security breaches.

It is critical to recognize that weaknesses in cloud service technologies can expose sensitive data or cloud resources to significant risks. To reduce these technological vulnerabilities, organizations should implement robust security measures, such as:

- *Automated Configuration Management:* Using automated tools to ensure cloud services are configured securely and in line with industry best practices, reducing the risk of misconfiguration.
- *Cloud Security Posture Management (CSPM):* Utilizing specialized CSPM tools that continuously assess cloud configurations against industry standards, benchmarks, and security policies. These tools can identify misconfigurations and provide recommendations for remediation.
- *Automated Remediation:* Implementing automated remediation processes or utilizing cloud-native security solutions that can automatically correct misconfigurations or security issues based on predefined policies.
- *Continuous Vulnerability Scanning***:** Implementing ongoing vulnerability scanning to identify weaknesses or outdated components that could be exploited.
- *Advanced Cloud Security Features:* Utilizing built-in security offerings or measures from cloud providers, such as automated patching services, encryption mechanisms, and integrated firewall protections, to strengthen the security posture.

In addition to addressing misconfigurations, organizations should also consider, apart from continuous vulnerability scanning, conducting regular penetration testing of their cloud environments. These activities can help identify potential security weaknesses, validate the effectiveness of security measures, and uncover vulnerabilities that may be exploited by attackers. By proactively conducting these tests, organizations can make informed decisions to strengthen the security of their cloud environments.

Furthermore, monitoring for potentially malicious activity, such as unusual logins or unauthorized access attempts, and regularly reviewing logs and audit trails are crucial measures to detect and prevent security breaches. These practices are typically supported by Security Information and Event Management (SIEM) solutions, which centralize log collection, correlated events, and generated alerts based on suspicious patterns. By leveraging SIEM tools effectively, organizations can improve their ability to identify and respond to threats promptly, thereby strengthening their overall security posture (SANS Institute, 2020).

In conclusion, technological factors play a critical role in the security of cloud computing environments. Vulnerabilities such as inadequate encryption, improperly configured cloud services, and platform weaknesses can expose sensitive data and cloud resources to significant risks. To mitigate these risks, organizations must implement robust technical security controls, including automated configuration management, continuous vulnerability scanning, patch management, and leveraging advanced cloud provider security features. Regular examination of logs and audit trails is also essential to promptly detect and respond to potential security incidents, ensuring the integrity and confidentiality of data stored in the cloud.

### 2.2.3 Human And Technological Factors

In cloud security, certain vulnerabilities arise from the interplay between technological limitations and human actions. These factors cannot be attributed exclusively to either technology or human behavior but rather to how individuals interact with available technologies and tools. Understanding this combined nature is essential to properly address these security challenges in cloud environments. Some notable examples include:

- *Weak Authentication:* Authentication-related vulnerabilities in cloud environments often arise from a combination of human and technical factors. On the technological side, inadequate implementation of authentication protocols, such as poor integration of MFA, outdated algorithms, or lack of support for strong authentication standards, can expose systems to attack. On the human side, users may choose weak or reused passwords, fail to enable available security features (e.g., MFA), or misconfigure identity settings. This interplay between improper user behavior and flawed implementation increases the likelihood of unauthorized access, especially in cloud environments that rely heavily on remote and distributed authentication mechanisms.
- *Lack of Patch Management:* Failing to apply timely patches to cloud systems can leave them exposed to known vulnerabilities. The human factor often involves neglecting updates, misunderstanding patch criticality, or applying poor change management policies. The technological factor may involve flaws in the cloud platform's patching mechanisms, lack of automated update support, or incomplete vendor documentation about vulnerabilities and their patches. When both factors combine, such as an administrator delaying updates on a component with known exploitable bugs, the risk of successful attacks increases significantly.
- *Insufficient Network Security:* Network security weaknesses often arise from a combination of human error and technological factors. While modern cloud platforms provide a range of powerful tools, such as firewalls, network access controls, and security group configurations, to establish strong network defenses, their effectiveness depends heavily on proper implementation and management.
  Commonly, misconfigurations caused by human oversight, lack of expertise, or procedural gaps lead to vulnerabilities. For example, improperly set firewall rules, incorrect network access permissions, or overly permissive security group settings can inadvertently expose cloud resources to unauthorized access. Although inherent technological vulnerabilities may exist and require regular updates or patches, the predominant source of insufficient network security is operational mistakes.

To reduce risks stemming from human-technological interactions, organizations should adopt a multi-layered approach:

- *Implement Strong Authentication Controls:* Deploy and enforce multi-factor authentication across cloud services. Ensure that authentication systems are properly integrated and tested to minimize technological gaps. Educate users on the importance of strong authentication and proper usage.
- *Automate Patch Management:* Use automated patch management solutions to streamline and accelerate the deployment of security updates, thereby reducing the risk of human error or oversight in manual patching processes. To address technological risks, such as faulty or incomplete patches, organizations should follow secure and validated patch development and testing practices, rely on vendor-signed patches, and perform staging or rollback testing before full deployment. Additionally, establish clear policies, roles, and responsibilities for patching, and provide personnel with training to reinforce the importance of timely and reliable patch application.
- *Enhance Network Security Configuration***:** Train network and security administrators in best practices for configuring firewalls, security groups, and access controls, to reduce the likelihood of misconfigurations. In parallel, improve the technological robustness of network security measures by adopting secure-by-design network architectures, leveraging next-generation firewalls with deep packet inspection, and applying principle-of-least-privilege defaults in security group configurations. Use automated tools for continuous monitoring, configuration auditing, and anomaly detection to identify and correct misconfigurations quickly and accurately.
- *Foster Security Awareness and Accountability:* Promote a security-conscious culture where employees understand the role they play in technology security. Regular training and clear communication of security policies can help reduce human errors that lead to vulnerabilities.
- *Continuous Monitoring and Auditing:* Leverage security information and event management (SIEM) tools, intrusion detection/prevention systems (IDPS), and log analysis to detect suspicious activity arising from both human mistakes and technological failures.

In conclusion, human and technological factors in cloud security are deeply interconnected, and vulnerabilities often arise from their interplay. Weak authentication, poor patch management, and misconfigured network security exemplify how human errors combined with technological weaknesses can expose cloud environments to threats. Organizations must implement robust technical

controls while simultaneously strengthening processes, training, and awareness to effectively mitigate these combined risks. By addressing both the human and technological aspects, organizations can significantly enhance the security posture of their cloud infrastructures.

## 2.3 Cloud Threat Assessment

The process of detecting and evaluating the risks and dangers posed to the confidentiality, integrity, and availability of data and all other resources stored in the cloud is referred to as cloud threat assessment. The purpose of a cloud threat assessment is to recognize and eliminate the dangers that are linked with cloud computing, as well as to protect the confidentiality and integrity of any data that is stored there.

An evaluation of the risks posed by the cloud must be carried out on a regular basis to guarantee that the organisation maintains an effective and up-to-date security posture. (SANS Institute, 2020) The assessment should involve a comprehensive review of the security measures already in place, as well as a thorough analysis of the potential risks and threats that may impact the organization's data and other digital assets stored in the cloud. This assessment can be performed by both the cloud customers and the cloud provider to ensure a holistic evaluation of the security posture as both parties have respective responsibilities in terms of (cloud) security.

The evaluation needs to take into account every facet of the cloud environment, such as the cloud service provider, the programs and services that are installed in the cloud, the kind of data that are stored in the cloud, the users and administrators who access and administer the cloud resources, the security architecture and measures that are being applied in the cloud, the security practices and processes that are in place in the cloud and so on. In addition to this, the evaluation must consider any regulatory and compliance requirements that are pertinent to the company's/organisation’s data (and other assets) stored in the cloud.

To successfully complete a cloud risk management, organisations need to adhere to a defined methodology that consists of the following steps:

- *Determine the scope of the evaluation*, which should include the cloud service provider, the data, the applications and services that are housed in the cloud, as well as the users and administrators that access and administer the cloud resources.
- *Define the criteria for the evaluation*, which should include assessing the effectiveness of the necessary security measures, best practices, and processes that should be in place within the cloud environment. Additionally, the evaluation should encompass an examination of known risks and threats specific to cloud computing, as well as compliance requirements relevant to the organization.
- *Carry out a vulnerability assessmen*t to determine whether or not the cloud environment contains any flaws or vulnerabilities.
- *Conduct an in-depth analysis of the findings of the vulnerability assessment* and arrange the potential dangers and threats in descending order of likelihood and potential effect.
- *Create a mitigation plan for risk management* that incorporates the use/application of adequate security measures, carefully selected based on the available budget and the criticality of the identified risks, so as to reduce/mitigate these risks.
- *Put the strategy for risk management into action*, making sure to include the required security measures, and continue to keep an eye on how well the measures are working, indeed reducing/mitigating the identified risks.

In the first place, it is essential to carry out a cloud threat/vulnerability assessment if one wants to recognize and eliminate the dangers and problems that are related with cloud computing. Organisations can detect any flaws or vulnerabilities in their cloud environments by doing a comprehensive evaluation and then developing a risk management strategy to remedy such weaknesses and vulnerabilities. This contributes to ensuring that the data (and other digital assets) stored by the organisation in the cloud continues to be safe and is protected from any possible risks (SANS Institute, 2020).

An organization's ability to satisfy regulatory and compliance standards can significantly benefit by undertaking a cloud threat assessment. When it comes to storing and managing data in the cloud, organisations must comply with the various legislation and compliance standards that are required by many different sectors. According to research published by the Cloud Security Alliance (2016),

organisations that carry out a cloud threat assessment are able to discover any loopholes in their compliance and then take the necessary measures to close such gaps.

In addition, carrying out a cloud threat assessment may assist organisations in reaching well-informed conclusions on the cloud service provider and cloud environment in which they operate. The purpose and outcomes of such an assessment depend on the organization's current cloud strategy:

- For organizations already operating in the cloud, a threat assessment can help evaluate whether their current cloud environment sufficiently meets their security requirements. Based on the findings, the organization may decide to retain its current provider while implementing security enhancements, or in some cases, consider migrating to a different provider if critical risks cannot be mitigated effectively.
- For organizations considering a migration from on-premises infrastructure to the cloud, a threat assessment — though potentially more resource-intensive — can offer valuable insights when comparing candidate providers. In this context, organizations may rely on publicly available information, such as security certifications (e.g., ISO 27001, SOC 2), documented security practices, and service-level agreements (SLAs). Where feasible, conducting a limited security evaluation using trial or sandbox environments can provide additional assurance before final selection.

In both cases, such assessments allow organizations to better understand the security posture of different cloud services, whether these services are offered by a single provider (e.g., IaaS vs. PaaS offerings within AWS) or span multiple providers. In multi-cloud or cross-cloud environments, however, these assessments often need to be enhanced to account for the increased complexity of managing different platforms, security models, and varied compliance frameworks. This may involve adopting unified assessment frameworks, integrating provider-agnostic monitoring tools, and ensuring consistent policy enforcement across all cloud environments. Such practices enable organizations to make more informed decisions about which services to adopt, retain, or migrate based on risk tolerance, compliance needs, and operational requirements (NIST, 2018).

In general, carrying out a cloud threat assessment is critical for protecting the confidentiality of data that is stored in the cloud. It offers organisations with useful insights into the risks and threats that are

associated with their cloud environment as well as enables them to establish a risk management strategy to reduce such risks. In addition to this, it assists businesses in meeting regulatory and compliance obligations and in making educated decisions regarding their utilised cloud environments and services.

## 2.4 Associated Threats

Threats are specific instances or manifestations of risks that could be realized in the course of an attack that exploits a specific vulnerability. Here are some examples of associated threats that organizations may face in relation to vulnerability realization:

- *Unauthorized Access:* Attackers may exploit vulnerabilities to gain unauthorized access to systems, networks, or sensitive data. This can lead to data breaches, unauthorized data modifications, or unauthorized system usage.
- *Data Loss or Theft:* Vulnerabilities in data storage or transmission mechanisms can lead to the loss or theft of sensitive information. Attackers may gain access to confidential data, intellectual property, or personal identifiable information (PII), compromising the privacy and security of individuals or organizations.
- *Malware Infections:* Vulnerabilities in software or systems can allow for the installation and execution of malware. Malware can include viruses, worms, ransomware, or spyware, which can disrupt operations, steal sensitive data, or gain unauthorized control over systems.
- *Service Disruption:* Attackers may cause service disruption, making cloud systems or networks unavailable to legitimate users. This interruption can lead to significant operational downtime, loss of productivity, and can cascade into further consequences such as financial loss and reputational damage (SANS Institute, 2020).
- *Insider Threats:* Malicious or negligent insiders, including employees, contractors, or third-party partners, can intentionally or unintentionally exploit vulnerabilities to cause harm. This includes unauthorized access, sabotage, or data leakage, and is often difficult to detect due to the insider's legitimate access.
- *Data or System Destruction:* Certain threats aim not just to steal or access data, but to permanently destroy it, either as an act of sabotage, retaliation, or ransomware. This can involve wiping databases, encryption without decryption keys, or deleting critical system files.

- *Loss of System Control:* In some cases, attackers may exploit vulnerabilities to seize full administrative control over systems or cloud infrastructure. This enables them to override security settings, manipulate logs, or launch further attacks, including lateral movement within the cloud environment.
- *Non-Conformance*: Organisations that employ cloud computing services have the potential danger of being exposed to compliance risks, which include the possibility of failing to comply with contractual commitments or regulatory requirements.
- *Excessive Costs*: While cloud computing offers scalable and cost-efficient solutions, it can also expose organizations to security-related financial risks. For instance, attackers who gain unauthorized access to a cloud account may provision large amounts of compute or storage resources (e.g., for crypto mining), resulting in unexpectedly high bills. Similarly, Distributed Denial-of-Service (DDoS) attacks or intentional misuse may trigger auto-scaling mechanisms, inflating resource consumption and associated costs.
- Inadequate cost monitoring, combined with overprovisioned services or misconfigured billing alerts, can further exacerbate these issues. Therefore, integrating **cost governance** with **security monitoring** is essential to detect anomalies, enforce usage policies, and prevent cost-related exploitation (Cloud Security Alliance, 2016).

# 3. Social Engineering Attacks on Cloud

## 3.1 Social Engineering Attack Definition

The term "social engineering" carries different meanings depending on the field of study. In political science, it is often used to describe top-down efforts to influence societal behaviors through public policies and institutional design (Baldwin, 2016). In contrast, in the field of cybersecurity, *social engineering* refers to manipulative tactics employed by malicious actors to deceive individuals into compromising systems or divulging confidential information (Hadnagy, 2018).

Within cybersecurity, social engineering is classified as a non-technical attack vector that relies on human psychology rather than software or hardware vulnerabilities. These attacks are typically crafted to exploit cognitive biases, emotional triggers, and social norms. The attacker's objective is to manipulate the target into performing actions, such as clicking a malicious link, sharing credentials, or granting unauthorized access (Alshamrani et al., 2020). Phishing, pretexting, baiting, and tailgating are just some of the various techniques that may be used in social engineering assaults.

Because of the vast number of users and the intricate architecture of the cloud ecosystem, social engineering attacks can be especially successful in cloud systems. According to research published by the Cloud Security Alliance (2016), cloud environments frequently involve various users who have varying degrees of access to the data and systems. In this respect, deceiving such users can lead to varying effects, some of which can be quite critical for an organisation or even a cloud provider.

Scholars and security practitioners have identified several core **psychological principles** frequently exploited in social engineering campaigns (Pattinson et al., 2016; Hadnagy, 2018):

1. *Authority:* The attacker pretends to be a person in power to compel obedience.
2. *Intimidation:* Victims are coerced through fear, threats, or consequences.
3. *Consensus/Social Proof:* Individuals are influenced by perceived behavior of others.
4. *Scarcity:* The perception that a resource, opportunity, or service is limited (e.g., *"Only the first 10 employees to respond will receive secure VPN access"*) increases the likelihood that the target will comply with the attacker's request without scrutinizing it.

5. *Urgency:* Time pressure is applied to prevent careful consideration (e.g., *"Your account will be locked in 10 minutes unless you verify your credentials now"*).
6. *Familiarity/Trust:* Existing relationships or perceived legitimacy are leveraged to reduce suspicion.

These principles are widely used in modern cybercrime, particularly because humans are consistently the weakest link in organizational security (Hernandez-Castro et al., 2020). Despite increasing technical safeguards, social engineering attacks remain prevalent due to their adaptability and low-cost execution.

This section introduces the SE concept from a **security-focused** perspective. A breakdown of specific social engineering techniques and their implications in cloud environments is provided in the following sections.

## 3.2 Attacks Dimensional Classification

Attacks in cloud environments, particularly those involving social engineering, can be effectively categorized based on a three-dimensional taxonomy proposed by Odeh et al. (2021). This model classifies attacks using the following dimensions:

**Environment***:* Refers to the context in which the attack occurs:

- *Human-centered*: Involves direct or indirect psychological manipulation of the victim, relying on verbal, written, or digital communication (e.g., phishing emails, phone scams, or in-person deception). The emphasis is on exploiting human behavior rather than systems or infrastructure. Although they can take place through digital or in-person channels, their defining feature is that the attacker's success depends on influencing the victim's cognitive and emotional response. In contrast to physical or technical attacks, the environment here is defined by social engagement rather than by material or digital systems.
- *Technical/software-based*: Involves the manipulation of cloud systems, software, or digital interfaces to deceive users or gain unauthorized access. This may include the use of spoofed login portals, malicious scripts embedded in shared cloud documents, or the exploitation of misconfigured access controls to trick users into performing insecure actions.

- *Physical/material*: Exploits the physical infrastructure or assets (e.g., tailgating into a restricted data center area, stealing an employee's access badge or cloud-connected laptop, or placing rogue devices inside an organization's network perimeter). While human behavior may indirectly contribute to these attacks (e.g., through negligence or distraction), it is not the principal focus. The attack environment is defined by the physical domain of access and control, rather than social or digital interaction.

**Approach**: Refers to the method or tactic used by the attacker:

- *Impersonation*: The attacker deliberately assumes a false identity or role to deceive the victim (e.g., posing as IT support, a system administrator, or a vendor). The key feature is that the attacker fabricates a persona, regardless of whether a relationship previously existed, to gain credibility and influence behavior.
- *Lure and Enticement*: The attacker presents an attractive bait to provoke action from the target (e.g., a free software tool, a fake prize, or a job opportunity). This method leverages curiosity, greed, or desire, often without direct interaction until the bait is taken.
- *Trust Abuse*: The attacker exploits an existing or perceived relationship or trust, not by inventing a new identity (as in impersonation), but by co-opting or hijacking real relationships or access. This may involve account compromise (e.g., taking over a known colleague's email), insider manipulation, or leveraging organizational affiliations. The deception relies on the validity of the identity, not the creation of a false one.

**Medium**: Refers to the channel used to deliver the attack:

- *Digital*: The attack is conducted through electronic communication channels or digital interfaces, such as email, messaging apps, cloud service portals, collaboration platforms, or malicious websites. The medium is entirely virtual and network-based, enabling the attacker to reach victims remotely without any physical presence. This is the most common medium in cloud-based social engineering campaigns (e.g., phishing emails with embedded malicious links or cloud document sharing with embedded payloads).
- *Physical*: The attack is delivered through in-person interaction or physical objects, such as printed documents, USB drives, or direct conversation. This includes methods like leaving infected media in public areas ("USB drop"), hand-delivered forged documents, or face-to-

face pretexting during unauthorized facility access. Unlike the digital medium, which operates through data exchange over networks, the physical medium depends on direct material contact or personal presence.

This three-dimensional taxonomy serves as an analytical framework rather than a standalone classification. The following attack types are presented not as a new taxonomy, but as composite manifestations of combinations across the three dimensions: environment, approach, and medium. Each type demonstrates how social engineering attacks can occur through different contextual alignments.

Based on this classification, attack types can be grouped as follows:

- *Human-based social engineering attacks:* These attacks are characterized by direct interpersonal interaction, where the attacker engages the victim in real-time to manipulate behavior, typically through verbal or written communication. The focus is on psychological influence, not technical compromise or physical manipulation of infrastructure. These attacks occur in a human-centered environment, utilize either digital or physical media, and often employ tactics, such as impersonation, trust abuse, or pretexting. A common example of this category is:
    - *Tailgating: This is a trust abuse attack in a human-centered environment using a physical medium*. The attacker physically follows an authorized person into a restricted area (e.g., data center) without authentication, exploiting trust or distraction. The success of this tactic relies on exploiting implicit trust, for example, the victim assumes the attacker is a colleague or contractor who belongs in the facility. Distraction may also be leveraged, such as engaging the target in casual conversation or timing entry during busy periods when individuals are less vigilant about enforcing access protocols.
- *Technical/Software-Based Social Engineering Attacks:* These attacks occur in technical or software-based environments and are typically delivered via digital media. They do not involve direct human-to-human communication.
    - *Malicious Cloud Document Links:* Shared files or collaboration links containing embedded scripts or hidden redirections that compromise accounts.

- *Spoofed Login Portals:* Fake authentication pages that mimic legitimate cloud services to harvest user credentials.
- *Trojans:* Malicious programs disguised as legitimate software, tricking users into unknowingly installing them, which can lead to data theft or unauthorized access.

- *Physical-based attacks:* These attacks are characterized by the use of physical presence to exploit non-digital vulnerabilities in processes, spaces, or assets. These attacks typically require the attacker to be on-site and rely on direct interaction with physical environments that do not involve direct interaction with a human, rather than remote digital channels. Examples included:
  - *Dumpster diving:* Dumpster diving is a technique used to retrieve information that could be used to carry out an attack or gain access to a computer network from disposed items. Dumpster diving is not limited to searching through the trash for obvious treasures, such as access codes or passwords written down on sticky notes. It could also include searching for seemingly innocent information, such as a phone list, calendar or organizational chart, which can be used to assist an attacker using social engineering techniques to gain access to the network.

## 3.3 Different types of Social Engineering Attacks

Social engineering encompasses a wide variety of attacks (see Figure 3.1), each designed to exploit human psychology in different ways. These attacks vary in delivery method, complexity, and impact, but they all share a common goal: to manipulate individuals into revealing sensitive information, granting access (to systems or data), or performing actions that compromise security.

This section categorizes and analyzes several prominent types of social engineering attacks. Each type is discussed with reference to its attack mechanism, medium, and examples relevant to cloud and IT-based environments.

**Figure 3.1** Social Engineering Attack Types.

### 3.3.1 Impersonation

An impersonation attack occurs when an attacker pretends to be someone else, such as a trusted employee or a member of the IT support staff, in order to obtain access to sensitive information or systems. Impersonation assaults may be quite dangerous. These assaults may be carried out in person or by electronic communication methods, such as texting or email (Cisco, 2020).

An impersonation attack is a very common social engineering attack. In fact many other social engineering attacks use impersonation (as a manipulation/social engineering method) in order to achieve their goal, often in combination with other tactics/methods. Such as :

- *Pretexting Attacks:* Attacks that utilize pretexting entail the fabrication of a bogus scenario or pretext in order to deceive users into giving away critical information. These assaults frequently include posing as someone else and can take place either in person or via the use of technological communication (Cisco, 2020). When a false identity is employed (e.g.,

pretending to be an IT technician or vendor), the attack overlaps with impersonation. However, pretexting can also occur without impersonation, for example, by presenting a plausible but false situation (such as a system malfunction or policy requirement) without claiming a specific identity. In such a case, the attacker might send a generic system alert informing users that their cloud storage account requires "urgent synchronization" due to a technical error and instruct them to follow a link to "revalidate" their credentials. Here, the deception relies on the credibility of the situation itself, not on a fabricated persona, since the attacker poses as an *organizational process* or *system-generated message* rather than a named individual.

### 3.3.2 Shoulder surfing

Shoulder surfing is a type of physical attack in which an attacker gains access to sensitive information by physically witnessing a victim's actions, such as the victim's input on a keyboard or the information shown on his/her screen. These assaults may be carried out in person or with the use of video surveillance equipment (SANS Institute, 2020).

### 3.3.3 Dumpster diving

This assault type involves an attacker looking through a target's discarded materials, such as paper documents or computer hardware, in order to obtain access to sensitive information. Such an assault may take place on physical premises (e.g., garbage cans/bins/dumpsters). (SANS Institute, 2020).

*Note:* While traditionally physical, a digital analogue exists; for example, recovering files from a system's recycle bin, misconfigured cloud storage, or unencrypted media marked for deletion but not properly wiped (a data remanence issue). These digital scenarios may resemble dumpster diving conceptually, but are typically classified under technical-based attacks involving data recovery or misconfiguration exploitation.

### 3.3.4 Phishing attacks

Phishing attacks deceive people into giving away critical information by sending them deceptive emails or messages, or by tricking them into clicking on links that lead to malicious websites via

which various kinds of information might be requested from them. The following are some examples of distinct types of phishing attacks:

*Spear Phishing*: These are targeted phishing attacks that are customized for specific individuals or organizations. Attackers conduct thorough research on their victims to create personalized and highly convincing phishing messages. These messages can take various forms, such as seemingly legitimate emails from trusted sources, HTML-formatted messages that mimic legitimate communication and direct users to fake login pages designed to steal credentials, or malicious attachments disguised as important documents.

*Whaling*: These phishing attacks differ from traditional phishing attacks in that they are specifically tailored and targeted towards high-profile individuals or specific organizations. The attackers invest time and effort to gather detailed information about their victims, such as their roles, responsibilities, or affiliations. By customizing the phishing messages to appear more personalized and legitimate, the attackers aim to deceive their targets into divulging sensitive information or performing certain actions.

The targeting of high-profile individuals in whaling attacks can lead to the potential acquisition of more crucial information about a company or its employees than spear-phishing attacks. Since high-profile individuals often have access to valuable data or have decision-making authority, compromising their accounts can provide attackers with privileged access to confidential information, sensitive systems, or critical resources. This can further enable them to carry out more sophisticated and damaging cyber attacks, such as data breaches, corporate espionage, or identity theft.

*Pharming*: Pharming is a type of attack that involves manipulating the Domain Name System (DNS) to redirect users to fraudulent websites. Attackers tamper with DNS settings or compromise DNS servers to misdirect users' web traffic to malicious sites that are designed to resemble legitimate ones. The goal of pharming attacks is to deceive victims into unknowingly providing sensitive information, such as login credentials or financial details, to the attackers.

*Smishing*: Phishing attacks carried out via SMS (text messages) or other messaging platforms, where the attacker impersonates a legitimate source to trick recipients into sharing personal information or clicking on malicious links.

*Vishing*: Vishing is a subtype of phishing and impersonation attacks that are conducted over phone calls or voice messages, where the attacker impersonates a trusted entity and tries to manipulate victims into divulging sensitive information.

*Angler Phishing:* Angler phishing is a subtype of phishing attacks that specifically targets users on social media platforms. Attackers leverage social media networks, such as Facebook, Twitter, or LinkedIn, to create convincing profiles (e.g., customer support staff) and establish trust with their targets. They then use these profiles to distribute malicious links or messages, tricking users into visiting fraudulent websites or downloading malware. Angler phishing exploits the familiarity and trust associated with social media platforms to deceive victims and steal their sensitive information.

*Email Phishing*: Email phishing is one of the most common and well-known types of phishing attacks. Attackers send fraudulent emails that appear to be from legitimate sources, such as banks, government agencies, or trusted organizations. These emails often contain alarming or enticing messages to manipulate recipients into clicking on malicious links, downloading infected attachments, or providing sensitive information. Email phishing attacks exploit the trust and familiarity users have with email communication, making it easier for attackers to trick unsuspected individuals into falling for their scams.

### 3.3.5 Baiting attacks

Baiting attacks are a form of social engineering that exploit human curiosity, greed, or the desire for free rewards to trick individuals into taking actions that compromise their security (SANS Institute, 2020). Unlike phishing attacks, which primarily rely on deception through impersonation, authority, or trust, baiting attacks focus on the enticing nature of the bait itself to provoke action from the victim.

While phishing attacks, including spear phishing, angler phishing, and email phishing, aim to deceive users into revealing sensitive information or performing harmful actions by exploiting trust or familiarity, baiting differs in its psychological mechanism. Baiting leverages curiosity, temptation, or perceived personal gain, rather than trust in an external source.

These attacks often involve physical media, such as infected USB drives or CDs, that are deliberately left in public areas or workplaces. The bait may be labeled in a way that picks interest (e.g., "Executive

Salaries Q4" or "Confidential Strategy Plan"), prompting the target to interact with it. Baiting can also take digital forms, such as enticing downloads (e.g., fake software cracks, multimedia content) or fraudulent promotions, all designed to manipulate the victim through desire rather than deception.

A key difference between phishing and baiting lies in the psychological mechanism:

- *Phishing:* manipulates victims by exploiting trust, authority, or urgency (e.g., an urgent email from IT).

- *Baiting:* in contrast, tempts victims with something appealing (e.g., a free download or device), triggering curiosity or desire.

While the use of physical media, such as USB sticks or CDs, is one example, baiting attacks can also take other forms. Here are a few additional examples:

- *Fake Downloads:* Attackers may create enticing offers or free downloads, such as software cracks, games, or multimedia content, and distribute them through unofficial or malicious websites. Users who unknowingly download and install these files may inadvertently introduce malware onto their devices.
- *Fake Wi-Fi Hotspots:* Attackers may set up rogue Wi-Fi hotspots in public places, such as airports or coffee shops, with names that appear legitimate. When unsuspecting users connect to these networks, attackers can intercept their internet traffic, capture sensitive information, or deliver malware.
- *Phony Promotions:* Attackers may create fraudulent advertisements, online surveys, or promotional campaigns that promise exclusive deals, discounts, or rewards. Users who fall for these scams may be directed to malicious websites, prompted to provide personal information, or tricked into downloading malware.

### 3.3.6 Tailgating attacks

An attacker will physically follow a legitimate user into a protected location in order to sneak into restricted systems or data. These assaults are carried out in person and rely on social engineering and deceit as their primary methods of operation (SANS Institute, 2020).

Tailgating typically occurs in one of two ways:

- *Passive Tailgating:* The attacker does not directly engage the target but rather waits for an opportunity to slip through a door as it is closing behind a legitimate employee, for example, by grabbing the door before it locks. This form of tailgating relies on the attacker's stealth and the victim's unawareness.

- *Impersonation-Based Tailgating:* In this variant, the attacker engages the target directly, possibly posing as an employee, contractor, or delivery worker. They may ask the legitimate user to hold the door open or claim they forgot their badge. In such cases, tailgating overlaps with impersonation, as the attacker assumes a false identity or role to gain trust (Fortinet, 2023; PrivacySense, 2023).

### 3.3.7 Pop-up windows

Pop-up window assaults relate to the use of harmful pop-up windows to deceive users (e.g., through urgency) into clicking on a dangerous link, downloading malicious software or supplying sensitive information. These attacks can occur either due to the compromise of a web application/site or the visiting of malicious sites by the victim. Web browsers and other software programs may be utilised in the commission of these attacks (SANS Institute, 2020). Examples Included:

- *Adware:* Adware is an example of Pop-up windows attack that can occur when you may have accidentally downloaded the respective adware program, possibly by clicking on a malicious advert. Alternatively, adware may have infected your computer through a link in a compromised web application/site or an attachment that you have opened. When the victim's computer is turned on, adware automatically displays pop-ups in the victim's browser when the victim is online.

### 3.3.8 Scareware

Scareware is a form of social engineering attack that leverages fear, panic, or a false sense of urgency to trick users into taking harmful actions, such as downloading fake antivirus software, clicking on

malicious links, or disclosing sensitive information (Symantec, 2020). The goal of scareware is to intimidate the user into immediate compliance.

Scareware does not rely on a single medium. It can be delivered through:

- *Pop-up windows*
- *Email messages*
- *Malicious websites*
- *Fake advertisements*
- *Software bundles or installers*

A common example is when a user sees a pop-up alert while browsing the web, which falsely claims:

> "Warning! Your PC is infected with 5 viruses. Click here to scan your system now."

Upon clicking, the user is taken to a malicious site or is prompted to install a fake antivirus tool. Once installed, this tool may demand payment, install actual malware, or harvest data, all under the guise of protecting the user's device.

### 3.3.9 Quid pro quo

Attackers will carry out a quid pro quo attack when they are supposed to be willing to give a reward or service in return for sensitive information or access to a system given by the victim. These assaults may be carried out either in person or via the use of technological communication (Cisco, 2020).

As an example, an attacker calls a victim's phone pretending to be from one of his/her service providers' technical support representatives. As such, the attacker will offer to the victim some assistance. This would, however, only work if the victim is experiencing some difficulty. In need of the attacker's "service", the victim actually gives the attacker access to his/her computer, device, or home network.

### 3.3.10 Reverse Social Engineering Attacks

In reverse social engineering attacks, the attacker first creates a specific issue to the victim like damaging the victim's equipment. Then, the attacker should send a phishing link or ad to the victim pretending to be the victim's savior (e.g., advertise as a person of authority, ably skilled in solving that problem). The victim would then utilise the link in order to contact the attacker. In this attack type, the reverse social engineering one, the victim unwittingly goes to the attacker. This is in contrast to normal social engineering attacks where the attacker makes the first contact to the victim. These assaults frequently entail the sending of fake messages or warnings to users in an effort to deceive them into making the first contact (Cisco, 2020).

**Social Engineering Attack Classification Table**

| Attack Type | Environment | Approach | Medium |
|---|---|---|---|
| Impersonation | Human-centered | Impersonation | Any |
| Shoulder Surfing | Physical/material OR Human-centered | Trust Abuse | Physical |
| Dumpster Diving | Physical/material | - | Any |
| Phishing | Human-centered OR Technical/software-based | Lure and Enticement OR Impersonation | Digital |
| Baiting | Human-centered OR Physical/material | Lure and Enticement | Any |
| Tailgating | Physical/material | Trust Abuse OR Impersonation | Physical |
| Pop-up Windows | Technical/software-based | Lure and Enticement | Digital |
| Scareware | Technical/software-based | Lure and Enticement | Digital |
| Quid Pro Quo | Human-centered | Impersonation | Any |
| Reverse Social Engineering | Human-centered | Trust Abuse OR Impersonation | Any |

**Table 3.1** Social Engineering Attack Classification Table.

## 3.4 Social Engineering Attacks and Cloud Computing: The Relationship

Social engineering (SE) and cloud computing are interconnected in a dual and evolving relationship. On one hand, cloud users can become victims of SE attacks due to their reliance on online communication and authentication. On the other hand, cloud platforms themselves can serve as delivery vectors for launching social engineering attacks against others, leveraging the scale, accessibility, and services the cloud offers.

### 3.4.1 The Cloud as a Medium and Target

Cloud environments facilitate social engineering attacks in two primary ways:

- *As a medium for attack:* Attackers exploit a wide range of cloud services, including collaboration services (e.g., Microsoft 365, Google Workspace, Slack) and storage services (e.g., Dropbox, Google Drive) to deliver phishing emails, malicious files, or spoofed login pages hosted on legitimate cloud domains. In this context, any cloud-based application or infrastructure component can serve as a vector for social engineering attacks, depending on how it is misconfigured, abused, or presented to the user.
- *As a target environment*: Cloud users, both internal and external, are attractive victims due to the sensitive data, systems, and privileged access they often have. Cloud resources can be hijacked for broader campaigns once access is gained via SE.

Both internal users (employees, admins) and external users (clients, partners) can be targeted, depending on the attack objective:

- *Internal users* (e.g., cloud admins, DevOps personnel) are often targeted by spear phishing, whaling, pretexting, or quid pro quo attacks to gain privileged access to cloud infrastructure.
- *External users* (e.g., SaaS customers) may be targeted with email phishing, tech support scams (a form of quid pro quo attack), or scareware delivered via cloud-hosted websites.
- *Remote/third-party users* (e.g., supply chain partners) may be targeted as stepping stones into a cloud environment (supply chain SE) through specific social engineering techniques, particularly those that exploit trust relationships and inter-organizational communication

channels. Common examples include impersonation and phishing attacks that mimic official vendor notifications or collaboration invitations. These methods leverage the inherent trust and routine data exchange that characterize supply chain integrations, making such external users effective entry points for cloud-targeted attacks.

### 3.4.2 Correlating SE Attack Types with Cloud User Roles

| Attack Type | Internal Cloud Users (e.g., employees, admins) | External Cloud Users (e.g., customers, clients) | Remote/Third-Party Users (e.g., suppliers, external orgs) | Typical Goal |
|---|---|---|---|---|
| **Phishing (Email/Web)** | ✓ | ✓ | ✓ | Steal credentials, spread malware, obtain access to cloud systems/services |
| **Whaling** | ✓ | ✓ | ✓ | Target high-privilege accounts |
| **Pretexting / Quid Pro Quo** | ✓ | ✓ | | Impersonate cloud support or admin staff - Gain system access by offering fake technical assistance |
| **Baiting (Digital)** | | ✓ | | Deliver malware via enticing downloads or malicious VM/container images to compromise cloud environments (e.g., data exfiltration, remote control, or host access) |
| **Tailgating** | ✓ | | | Bypass physical security to access cloud infrastructure |
| **Scareware** | | ✓ | | Trick user into installing fake antivirus/malware to gain control of cloud-based VMs, access sensitive data, or disrupt hosted cloud services |
| **Reverse Social Engineering** | ✓ | ✓ | | Trick users into contacting the attacker, who then gains access to cloud accounts or services by offering fake support or guidance |

**Table 3.** SE Attack Types with Cloud Users.

### 3.4.3 Reported Frequencies and Trends

According to the IBM X-Force Threat Intelligence Index (2023) and Verizon's Data Breach Investigations Report (2023):

- Phishing remains the #1 social engineering threat in cloud environments, accounting for over 70% of initial access attempts in reported breaches.
- Business Email Compromise (BEC[14]), a form of spear phishing targeting cloud-based email systems, is among the most costly social engineering attacks.
- Credential theft via pretexting has risen significantly in SaaS-based enterprises, particularly those using Microsoft 365 or Google Workspace.
- According to Proofpoint (2022), cloud-based impersonation in phishing emails increased by 144% compared to the previous year.

### 3.4.4 Real-World Incidents

Social engineering (SE) attacks are often not standalone events, but rather form part of larger, multi-stage attack chains. In many real-world incidents, SE tactics are used during the initial access phase, such as credential harvesting or reconnaissance, before being followed by technical exploitation or privilege escalation. Furthermore, these attacks exploit various media, including phishing emails, cloud-hosted phishing pages, and impersonation via trusted communication channels, demonstrating their adaptability in targeting both cloud infrastructure and users. Below are illustrative examples of SE incidents that have had significant consequences in cloud environments:

- *Capital One (2019):* A former employee exploited a misconfigured firewall rule after conducting SE-based reconnaissance through insider impersonation tactics. The breach exposed the data of 100 million customers.
- *Dropbox (2022):* Attackers used phishing emails impersonating CircleCI, a software service provider, to collect employee credentials and access internal GitHub repositories hosted on cloud platforms.

[14] https://secure-iss.com/wp-content/uploads/2023/02/IBM-Security-X-Force-Threat-Intelligence-Index-2023.pdf

- *Microsoft 365 BEC Cases (2021–2023)*: Numerous organizations were compromised when executives or employees clicked phishing links hosted on cloud file-sharing platforms, such as SharePoint or OneDrive, which appeared legitimate.

### 3.4.5 Social Engineering as a Precursor to Technical Cloud Attacks

Social engineering often serves as the initial access vector (see also first incident in Section 3.4.4) that precedes more destructive or technically complex attacks in cloud environments, such as:

- Privilege escalation (after credential theft via phishing).
- Cloud infrastructure abuse (e.g., cryptomining after a successful access).
- Data exfiltration or man-in-the-middle attacks.
- Account takeovers and SaaS exploitation.
- (D)DoS attacks

In this sense, social engineering is not just a threat in isolation, it is a gateway that prepares the ground for multi-stage cyberattacks involving malware deployment, persistence mechanisms, and system compromise.

# 4. Review Methodology

This chapter outlines the systematic review methodology employed to identify, analyze, and synthesize relevant literature on social engineering threats and mitigation strategies in cloud computing environments.

The review process followed the guidelines proposed by Kitchenham and Charters (2007) for conducting *Systematic Literature Reviews (SLRs)* in software engineering and information systems research.

According to these guidelines, the review process consists of five distinct stages, summarized below:

1. **Planning the Review**: Establishing motivation, scope, and research objectives; formulating the research questions (RQs).
2. **Search Strategy Definition**: Designing comprehensive search strings, selecting databases, and defining inclusion and exclusion criteria.
3. **Study Selection and Quality Assessment**: Applying the criteria systematically to filter relevant studies, ensuring reliability and reproducibility.
4. **Data Extraction and Synthesis**: Collecting, categorizing, and synthesizing key data elements (e.g., threats, countermeasures, and methodologies).
5. **Analysis and Reporting**: Performing quantitative and qualitative analyses, identifying research gaps, and mapping findings to the established RQs.

The review was guided by the following primary research questions (RQs)**:**

- **RQ1:** What are the strategies and measures for the mitigation, detection, and prevention of social engineering attacks?
- **RQ2:** How can these strategies and measures be classified, and according to which dimensions?
- **RQ3:** What are the current research gaps and future directions that should be followed to ensure a more comprehensive, effective, and efficient response to social engineering attacks?

Each subsequent section of this chapter corresponds to a specific step of the methodology and its outcomes:

- **Section 4.1 (Information Sources)**: Lists the databases, repositories, and grey literature platforms consulted.
- **Section 4.2 (Search Strategy and Pattern)**: Details the search terms, Boolean expressions, and filtering logic used to identify relevant literature.
- **Section 4.3 (Article Selection and Quality Assessment)**: Explains the multi-stage screening process and inclusion/exclusion criteria applied.
- **Section 4.4 (Final Selection Summary)**: Presents the quantitative overview of the final literature set, including type, publisher, and temporal distribution (Figures 4.1–4.3).
- **Section 4.4.1 (Tracking the Field's Evolution)**: Analyzes the publication trends, highlighting the increasing academic focus on social engineering threats in the cloud.

By following this structured methodology, the review ensures transparency, reproducibility, and academic rigor, laying the foundation for the subsequent analysis of prevention and mitigation techniques discussed in Chapter 5.

# 4.1 Information Sources

We searched multiple academic databases to ensure comprehensive coverage of high-quality and peer-reviewed research relevant to social engineering and cloud security. The selected databases include:

- IEEE Xplore
- ACM Digital Library
- ScienceDirect
- Google Scholar

These sources were chosen because they are widely recognized and reputable within the fields of computer science, information systems, and cybersecurity.

To complement the academic perspective with real-world applications and emerging trends, we also consulted grey literature from two main categories of non-academic sources.

The first category includes institutional and industry sources, such as technical reports, white papers, and security advisories published by recognized cybersecurity organizations. While the second category consists of expert and practitioner sources, including specialized cybersecurity blogs, professional forums, and expert-authored analyses.

This dual-source approach ensured the inclusion of both authoritative institutional perspectives and current practitioner insights, offering a comprehensive view of contemporary social engineering threats and mitigation practices in cloud environments. These were primarily accessed through:

- General-purpose search engines like Google Search
- Official websites of cybersecurity organizations, such as:
    - ENISA (European Union Agency for Cybersecurity)
    - NIST (National Institute of Standards and Technology)
    - CISA (Cybersecurity and Infrastructure Security Agency)
    - Microsoft Security Blog
    - IBM X-Force
    - Symantec Threat Intelligence Center

## 4.2 Search Strategy and Pattern

A structured Boolean query was applied to the selected databases and search engines. The query was designed to balance precision and recall in capturing literature relevant to social engineering and its mitigation in cloud environments. The search string was as follows:

> **"Social engineering" AND ("mitigation" OR "protection" OR "prevention" OR "addressing") AND ("strategies" OR "methods" OR "measures" OR "techniques" OR "solutions") AND "cloud"**

This expression ensured a comprehensive scan of relevant studies, including foundational frameworks, experimental results, and industrial practices. Although the search included all years to

allow for historical context, publications from 2016 onwards were prioritized for inclusion due to their direct relevance to current/most recent technologies and threat models.

## 4.3 Article Selection and Quality Assessment Process

After collecting the articles based on the following search strategy, a two-stage filtering process was applied to reduce the volume of material and ensure the relevance and quality of the retained sources.

From the outset, two distinct categories of sources were recognized:

- *Academic literature:* Used as the basis for in-depth analysis.
- *Grey literature and non-academic sources:* Collected for contextual relevance, practical insights, and illustrative examples, but excluded from the formal analytical dataset.

Stage 1 – Exclusion and Inclusion Criteria

Title and Abstract Screening (Exclusion Criteria):

- Articles not explicitly address social engineering or cloud computing.
- Articles written in languages other than English as we could not study them.
- Duplicate entries retrieved from multiple databases.
- Publications with no accessible full text as this would impede their study and analysis.

Full-Text Review (Inclusion Criteria):

- Articles that explicitly propose strategies, methods, or techniques for the prevention, detection or mitigation of social engineering attacks.
- Studies presenting case analyses, experiments, or Social-engineering related studies directly applicable to cloud environments.
- Credibility of authors and affiliated institutions: Preference was given to works authored by researchers or practitioners affiliated with recognized universities, research centers, or reputable cybersecurity organizations. Author credibility was verified through institutional affiliation and publication record.

- Reputation of publication venues: Only studies published in respected and indexed venues were retained. Venue quality was evaluated based on peer-review status, indexing in major databases.

Additionally, publication type served as an inclusion criterion. Only the following types of academic/white literature manuscripts were retained:

- Peer-reviewed journal articles
- Peer-reviewed conference papers
- Books and book chapters published by established academic or professional publishers

Grey literature and non-academic sources were excluded from the analytical sample but were cited for contextual value where relevant.

Stage 1 – Quality Assessment:

To further ensure the reliability of the selected sources, the following quality criteria were evaluated during the second filtering stage:

- Soundness of methodology and data analysis
- Practical relevance and innovation of proposed strategies
- Presence of a clear methodological structure and theoretical foundation

Sources that demonstrated at least medium quality across these dimensions were retained. While preference was given to studies with high academic rigor and institutional credibility, medium-quality sources were also considered acceptable if they contributed meaningful insights relevant to the research questions.

This disciplined process ensured that the synthesis of findings in Chapter 5 is grounded in credible, well-structured, and practically significant research

## 4.4 Final Selection Summary

Upon completion of the filtering process, a total of 80 sources were initially identified across academic databases and reputable industry repositories. During the first-stage screening, 60 sources (75%) were retained after removing duplicates and clearly irrelevant items. The final selection consisted of 40 academic publications (50% of the initial set), which were subjected to in-depth qualitative and thematic analysis.

Grey literature sources, including reports, white papers, and technical blog posts, were not included in the core analytical dataset but were retained as a supplementary reference set to provide contextual insight into current industry practices and emerging trends. These supporting materials accounted for approximately 25% of the initially identified items and were used to triangulate findings from academic research rather than being included in the quantitative analysis.

The final dataset of academic sources was distributed as follows:

- **45% journal articles**
- **25% conference papers**
- **10% books**
- **10% book chapters**
- **10% PhD theses**

A pie chart of this distribution is provided in Figure 4.3 to visually highlight the proportional representation of each source type. The dominance of journal and conference papers reflects the maturity and rigor of scholarly discourse in this area, while the inclusion of books, book chapters, and these adds theoretical depth and breadth.

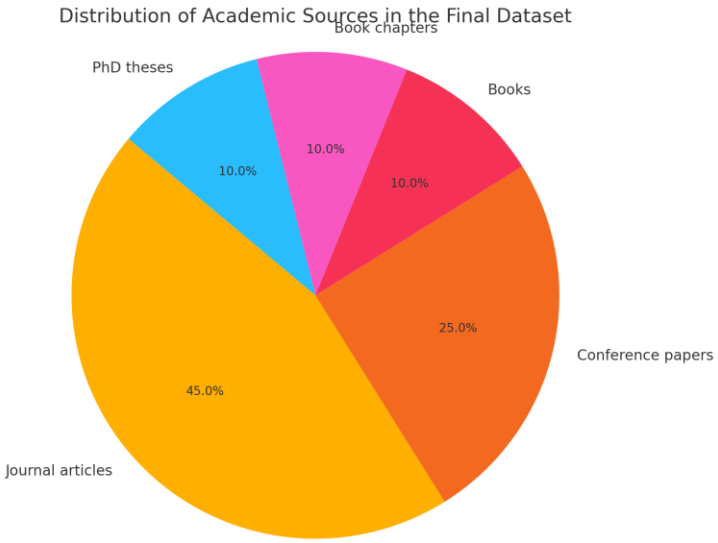


**Figure 4.1**: *Distribution of Retained Articles by Source Type*

This disciplined review methodology ensured the credibility, relevance, and comprehensiveness of the review, providing a strong foundation for the identification of social engineering mitigation strategies and the analysis of research gaps in cloud computing contexts.

To complement this breakdown, Figure 4.2 shows the temporal distribution of the retained publications from 2016 to 2021. A gradual rise is observed over the years, with a notable peak in 2020 (15 publications). This sharp increase likely correlates with the global shift to remote work and cloud service adoption during the COVID-19 pandemic, which may have triggered a surge in academic interest on cloud-based threats such as social engineering.

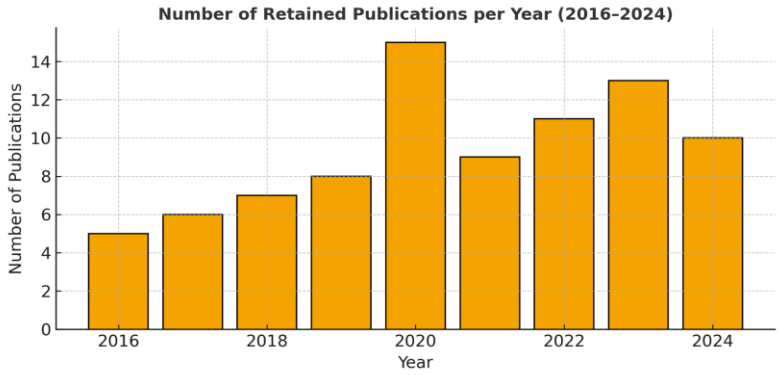


**Figure 4.2**: *Number of Retained Publications per Year (2016–2024)*

### 4.4.1 Tracking the Field's Evolution

To illustrate the evolution and composition of the reviewed literature, three key distributions were analyzed:

(a) publication **type**,

(b) **publisher or source**, and

(c) **year of publication**.

As previously shown in **Figure 4.2**, the number of publications addressing social engineering in cloud computing has grown steadily from 2016 to 2024. This upward trend highlights the increasing recognition of human-centric security as a major component of cloud defense strategies.

Figure 4.3 presents the **distribution of publications by publisher or source**. The most represented outlets include IEEE (30%), Elsevier (20%), Springer (15%), and ACM (10%), with the remaining 25% distributed among various other publishers such as MDPI, Taylor & Francis, and independent conference proceedings. The dominance of IEEE and Elsevier reflects their central role in disseminating high-quality research on both cybersecurity and cloud computing.

Together, these distributions confirm that research in this area has not only expanded over time but also diversified in terms of source and publication type. This indicates a maturing research domain with growing academic and industrial interest.

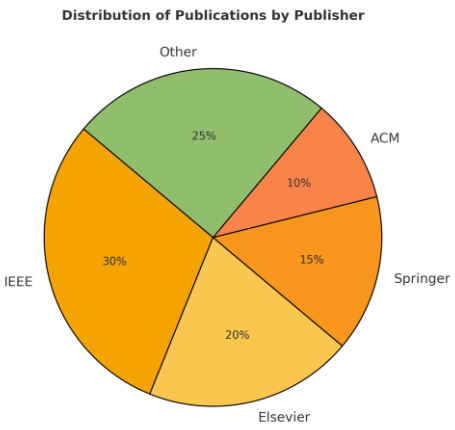


**Figure 4.3**: *Distribution of Publications by Publisher*

# 5. Prevention and Mitigation techniques

This chapter presents the principal strategies and techniques identified in the literature to prevent and mitigate social engineering attacks in cloud computing environments. Based on a structured review of selected academic literature, four main categories of countermeasures emerged:

- User Awareness and Education
- Technical Controls and Security Measures
- Incident Response and Business Continuity Planning
- Vendor Management and Due Diligence

These categories are derived from the thematic clustering of measures found across the reviewed works (cf. Chapter 4) and were further validated by best practices outlined in industry standards (e.g., NIST, SANS, CSA).

Each of the following sections presents one of the identified categories of countermeasures, outlining its specific contributions to social engineering defense. Collectively, these categories form a comprehensive security posture against social engineering threats in cloud computing environments.

## 5.1 User Awareness and Education

User awareness and education constitute a foundational category of prevention and mitigation strategies against social engineering attacks in cloud computing environments. This category includes methods, such as security awareness training, phishing simulation campaigns, password and authentication best practices, and behavioral conditioning. These methods aim primarily at prevention, by improving the user's ability to identify, resist, and respond to social engineering techniques to impede the success of the respective attack.

The relevance of this category stems from the human-centric nature of social engineering. Technical controls alone cannot fully protect an organization when users are the primary attack vector. Therefore, educating internal users, such as employees, administrators, and contractors, about common social engineering tactics is essential. These users are often targeted via phishing, pretexting, baiting, or impersonation, and user behavior is often the decisive factor in an attack’s success or failure. (Symantec, 2021)

While the focus of most organizational programs is on internal users, the need to educate external users (e.g., customers or third-party users) about secure usage of cloud services is equally important. However, a clear distinction should be made between these two groups. Employees within organizations should be trained by their respective companies as part of internal cybersecurity awareness programs, whereas citizens and independent users can be educated through initiatives led by governmental or regulatory bodies. Moreover, academic institutions, particularly universities, can play a vital role by integrating cybersecurity awareness and digital hygiene topics into their curricula, helping to foster a more security-conscious digital culture from an early stage.

The subsections that follow reflect the key areas of focus in this category.

### 5.1.1 Security Awareness Training

Security awareness training is considered one of the most effective human-centric defenses against social engineering attacks. It seeks to develop the knowledge and behavioral response of users to suspicious events, phishing attempts, or deceptive requests (Symantec, 2021).

Effective training covers:

- The nature of social engineering threats (e.g., phishing, baiting, pretexting)
- The importance of data protection and secure behavior
- Password hygiene and MFA practices
- Reporting protocols for suspicious activity

The design and delivery of training can take several forms:

| Training Approach | Description | Pros | Cons |
|---|---|---|---|
| **Classroom Training** | Instructor-led sessions conducted in person or digital, where participants can ask questions and engage in live discussions. | Interactive, immediate feedback | Hard to scale, time-consuming |
| **Online Modules** | Self-paced digital courses or e-learning platforms that deliver standardized | Flexible, trackable | Risk of disengagement if content is generic |

| | | | |
|---|---|---|---|
| | content to users across different locations. | | |
| **Gamified Training** | Training that incorporates game-like elements such as points, challenges, and rewards to motivate participation and reinforce learning. | High engagement, reward-based | Requires investment in design and tools |

This training must be **ongoing and continuously updated** to reflect emerging tactics and new attack surfaces, especially in cloud-based environments where users often interact with multiple systems and services daily (US-CERT, 2020).

Furthermore, training is most effective when it is **interactive and engaging**, employing real-world attack examples, simulations, and hands-on exercises (SANS Institute, 2020). Repetition, feedback, and behavioral reinforcement are essential elements that improve retention and encourage safer practices.

**Requirements of an Effective Training Program**:

- *Tailored to user roles and levels of responsibility:* Cloud environments involve diverse user roles (e.g., administrators, developers, and end-users) with different access privileges. Training should reflect these distinctions, emphasizing role-specific threats such as credential misuse or misconfiguration.
- *Regularly updated based on threat intelligence:* The dynamic and rapidly evolving nature of cloud ecosystems requires that training content be continuously updated to reflect new attack vectors, service vulnerabilities, and emerging social engineering tactics targeting cloud accounts.
- *Interactive and scenario-based, including real case studies:* Realistic simulations and cloud-specific scenarios (e.g., spoofed login portals or fraudulent cloud console alerts) enhance user preparedness and help bridge the gap between theoretical knowledge and actual practice.

- *Includes follow-up assessments to gauge knowledge retention:* Continuous evaluation through quizzes or phishing simulations tailored to cloud use cases allows organizations to measure user improvement and adjust training programs accordingly.

To evaluate how well these methods satisfy the stated requirements, a qualitative assessment **was conducted** based on a uniform three-level scale (*High, Medium, Low*). Each training approach was examined against the four effectiveness criteria discussed above, considering factors such as adaptability to cloud-specific roles, frequency of content updates, level of user engagement, and support for follow-up assessment. The following table summarizes the results of this evaluation:

| Training Approach | Tailoring | Up-to-date | Interactivity | Assessment Support |
|---|---|---|---|---|
| Classroom Training | High | Medium | High | High |
| Online Modules | Medium | High | Medium | High |
| Gamified Training | High | High | High | Medium |

**Analytical summary:**

Based on the qualitative assessment, no single training approach universally prevails across all evaluation criteria. Each method demonstrates strengths in specific areas. *Classroom training* excels in interactivity and assessment support but is less scalable. *Online modules* perform best in terms of being up-to-date and flexible for distributed cloud environments, though engagement may be lower. *Gamified training* achieves consistently high scores across most criteria making it the most balanced and effective option overall. However, its higher implementation cost and design complexity may limit its adoption in smaller organizations. Consequently, a hybrid model that combines scalable online delivery with interactive or gamified elements is generally the most effective approach, especially in cloud-centric contexts where continuous adaptation and engagement are essential.

**Pros:**

- *Promotes active learning and behavioral change:* Interactive and scenario-based methods, such as gamified or classroom training, enhance user engagement and facilitate better long-term retention of security concepts.
- *Scalable through digital delivery:* Online and hybrid modules enable organizations to train large, geographically distributed workforces efficiently, making them particularly suited to cloud-based enterprises.
- *Adaptable to emerging threats:* Training content can be regularly updated to reflect evolving attack patterns, ensuring that users remain aware of current social engineering tactics.

**Cons:**

- *Risk of disengagement:* Generic or repetitive online training may lead to low participation and limited behavioral impact if not personalized to user roles.
- *High implementation cost for interactive methods:* Gamified or in-person training requires additional investment in tools, design, and facilitators, which may be prohibitive for smaller organizations.
- *Limited long-term effectiveness without reinforcement:* Without continuous refreshers or integration into a broader awareness culture, the benefits of training tend to diminish over time.

While training alone cannot guarantee absolute protection, it significantly reduces susceptibility to manipulation and improves the organization's ability to detect and respond to emerging threats.

### 5.1.2 Social Engineering Awareness Campaigns

Awareness campaigns are structured efforts to reinforce key messages delivered through training and raise ongoing attention to social engineering threats. These campaigns can include:

- **Simulated phishing attacks:** These are controlled, realistic phishing scenarios crafted by security teams to test how users respond to deceptive emails or messages. The purpose is not only to assess vulnerability but to educate users based on their reactions. For example, users who click on a simulated phishing link might be redirected to a training module that explains

why the message was suspicious. These simulations help build resilience and sharpen recognition of phishing indicators over time.

- **Newsletters, posters, or infographics**: Visual materials placed in strategic office areas (e.g., break rooms, login screensavers) or sent via internal communications channels reinforce critical security messages. These materials often highlight recent threats, behavioral tips, or reminders like "Stop and Think Before You Click."
- **Short video clips or e-learning modules:** These are brief, targeted e-learning videos or animations (typically under 5 minutes) that explain a single risk or attack vector in simple terms. They are often used to break down complex threats (e.g., baiting, tailgating) into digestible content and are delivered periodically to reinforce key topics.
- **Monthly security topics**: These involve promoting monthly or quarterly security themes—such as "Think Before You Click" or "Verify Before You Share." Topics are communicated via internal newsletters, team meetings, or targeted mailers and may be paired with gamified activities or quizzes. These initiatives serve to embed a security mindset into the daily work culture and give users a sense of ownership in the organization's security posture

Such campaigns are **effective in sustaining vigilance** among users and building a long-term culture of security (KnowBe4, 2021). They also provide **feedback loops**, where user responses to simulations guide future training needs.

**Pros**:

- *Increases user engagement and retention through repetition:* By using varied and often interactive methods, campaigns can maintain user interest and avoid the monotony associated with standard training. Repetition through multiple formats enhances retention and encourages good habits.
- *Scalable and cost-effective when implemented digitally:* Most awareness campaigns, particularly digital formats like infographics and emails, are low-cost and scalable across large organizations. Their deployment can be automated or centrally managed with minimal overhead.

- *Encourages a security-first culture within organizations:* Ongoing campaigns help to embed security into an organization's culture. They keep threats visible and ensure that users remain alert, even outside formal training sessions.

**Cons**:

- *Risk of Fatigue or Desensitization:* If the campaign content lacks novelty or becomes overly repetitive, users may begin to ignore messages. Moreover, aggressive phishing simulations can lead to resentment or decreased trust in the security team.
- *Lack of Personalization:* Generic content may not address department-specific risks or user role differences, reducing practical effectiveness.
- *Requires Interdepartmental Coordination:* Effective campaigns often need support from communications teams, HR, and management. Without alignment across departments, campaigns may lack visibility or credibility.

Despite these limitations, social engineering awareness campaigns are recognized as an essential reinforcement tool in many cloud-focused organizations (McAfee, 2021; KnowBe4, 2021).

### 5.1.3 Best Practices for Passwords and Authentication

Another critical component of user education focuses on strengthening password and authentication hygiene. This strategy directly supports the prevention of credential-based social engineering attacks, such as phishing, credential stuffing, and brute-force attempts, especially prevalent in cloud environments where authentication gates access to sensitive resources and services.

Core educational topics in this area include:

- ***Creating strong and unique passwords***, often using passphrases or random generators to reduce predictability.
- ***Changing passwords regularly and following organizational rotation policies:*** Frequent password changes reduce the window of opportunity for attackers to exploit compromised credentials, especially in environments where password reuse or delayed breach detection is possible. Rotation policies should balance security with usability and be supported by awareness training to ensure proper implementation.

- ***Using password managers*** to minimize reuse, enhance complexity, and ease password storage.
- ***Understanding and enabling multi-factor authentication (MFA)***, particularly app-based or hardware token-based solutions rather than SMS alone.
- ***Recognizing and reporting suspicious login pages or abnormal MFA prompts***, which can signal phishing or man-in-the-middle attempts.

**Methodological application:**

In practice, password and authentication hygiene are taught through multiple complementary methods, often integrated into broader awareness programs. Organizations employ interactive e-learning modules, hands-on workshops, and phishing simulation campaigns to illustrate real-world credential threats and reinforce secure behavior. For instance, simulated credential-harvesting exercises can demonstrate the dangers of weak or reused passwords, while role-based training helps administrators and developers understand advanced authentication policies (e.g., privileged access management). Reinforcement mechanisms, such as periodic reminders, password change campaigns help sustain user engagement and long-term retention.

**Pros and Cons of the Strategy**

| Pros | Justification |
|---|---|
| **Directly mitigates high-risk attack vectors** | Most social engineering breaches begin with credential compromise. Strong authentication practices reduce this risk substantially. |
| **Well-aligned with industry standards** | Recommended in all major security frameworks (e.g., NIST, ISO/IEC 27001) and supported by security tools widely available in cloud environments. |
| **Easily measurable** | Organizations can evaluate password strength, MFA adoption, and reporting rates as KPIs for training effectiveness. |

| Cons | Justification |
|---|---|
| **User fatigue or resistance** | Users may resist password managers or MFA adoption, particularly when these are perceived as inconvenient. |
| **Does not address all social engineering tactics** | While effective against credential attacks, this strategy does not mitigate other forms of deception (e.g., baiting, tailgating). |
| **May require technical support and policy enforcement** | Implementing secure authentication often requires backend support, centralized policies, and integration with identity providers. |

While password and authentication training is often delivered through classroom sessions, online modules, or gamified environments, it is important to recognize that these methods are not exclusive to this strategy. Rather, they form part of a shared methodological framework across most user education initiatives, such as general security awareness programs and social engineering prevention campaigns. This overlap highlights that the effectiveness of such training relies less on the delivery format itself and more on how the content is contextualized and reinforced within the organization's broader cloud security practices.

For example, simulated phishing, previously discussed under awareness campaigns, can be used to highlight poor password practices by luring users into entering credentials into fake login portals. In the context of this category, such practical exercises, alongside classroom demonstrations, e-learning modules, and gamified challenges, represent the primary methods through which password and authentication hygiene is taught and reinforced. These methods aim not only to convey knowledge but also to influence user behavior by simulating realistic threat conditions. Thus, the focus of this section encompasses both the methodological approach, how training is delivered, and the educational

objective, promoting secure password behavior and authentication hygiene as fundamental components of user security in cloud environments.

Thus, the effectiveness of this strategy depends not only on the method of delivery, but on the clarity, frequency, and relevance of the content. Tailoring the message to common user mistakes (e.g., reusing passwords across systems, ignoring MFA prompts) and embedding these lessons in real workflows can significantly improve adoption.

## 5.2 Technical Controls/Measures

In cloud computing settings, the implementation of technical controls is fundamental to mitigating the risk of social engineering attacks. This section outlines key categories of technical measures that contribute to defending cloud environments and their users. The identified methods are primarily derived from a structured analysis of academic literature, while industry sources were consulted to validate the practical applicability, feasibility, and real-world adoption of these measures in operational cloud environments.

In addition to the commonly adopted technical mechanisms, such as Multi-Factor Authentication (MFA), Access Control, and Network Monitoring, other critical approaches like sandboxing, thread emulation, behavioral analytics and environment isolation are also considered. These methods are designed not only to prevent unauthorized access but also to detect, contain, and respond to threats introduced by social engineering vectors.

### 5.2.1 Multi-Factor Authentication (MFA)

Authentication, as part of the AAA model (Authentication, Authorization, Accounting), ensures that users are who they claim to be before granting access to cloud services. Among the most common and effective methods is Multi-Factor Authentication (MFA), which strengthens user authentication by requiring multiple forms of identification. These forms can be classified as follows: something the

user knows (e.g., a password), something the user has (e.g., a token), and something the user is (e.g., biometric data) (NIST, 2017). MFA helps mitigate risks arising from credential theft, a common result of phishing and pretexting attacks.

Although MFA is enforced by service providers, users are also responsible for complying with the authentication process by providing all required credentials. This shared responsibility emphasizes the importance of user awareness in combination with technology.

However, multi-factor authentication (MFA) is not infallible. Attackers may still deceive users into disclosing verification codes, typically short-lived, time-based tokens (e.g., one-time passwords sent via SMS or generated through authenticator apps), which fall under the "what the user has" category in authentication factors. Consequently, the effectiveness of MFA depends not only on its implementation but also on adequate user training and complementary security mechanisms.

In cloud environments, MFA is often integrated with centralized identity management systems, enabling consistent policy enforcement across services. A further enhancement is the use of adaptive security policies, which dynamically adjust authentication requirements based on contextual signals (e.g., device trust level, IP reputation, geolocation). These policies are called *adaptive* because they modify their behavior in real-time, rather than relying solely on static, predefined rules.

One example of such a policy is the use of risk-based login prompts, which trigger additional verification steps (e.g., biometric authentication or re-entering credentials) only when a login attempt is deemed anomalous or high-risk—such as from an unknown device or during atypical login hours. This approach supports a balance between usability and security: users are not constantly burdened with secondary authentication unless necessary, reducing friction for legitimate activity while maintaining strong protection against suspicious access attempts.

**Pros:**

- *Significantly reduces risk from compromised credentials:* Even if one authentication factor (e.g., a password) is stolen or compromised, access is blocked without the second factor, thereby minimizing the effectiveness of phishing attacks.

- *Supports context-based authentication with adaptive options:* Adaptive MFA can respond to dynamic risk conditions (e.g., unfamiliar login location) and enforce stronger verification only when necessary, improving both security and user experience.

**Cons:**

- *Susceptible to phishing if users disclose secondary tokens:* Attackers can still deceive users into revealing one-time passcodes or approving malicious login attempts through social engineering.
- *May introduce usability issues without proper configuration:* Frequent or poorly timed prompts for secondary authentication can frustrate users, potentially leading to lower adoption or unsafe workarounds.

### 5.2.2 Authorization and Access Control Models

Whereas authentication confirms a user's identity, authorization defines what authenticated users are allowed to do. It is the second key component of the AAA security model and is central to ensuring that users have appropriate levels of access in cloud computing environments (US-CERT, 2016).

The two most prominent access control models in cloud environments are:

- *Role-Based Access Control (RBAC):* RBAC assigns permissions based on user roles within an organization (e.g., "admin", "developer", "HR manager"). It is widely adopted due to its simplicity and alignment with organizational hierarchies. However, traditional RBAC is static, lacking context sensitivity, which limits its effectiveness against dynamic threats such as social engineering. To address this limitation, dynamic or context-aware RBAC models have been developed, which incorporate additional parameters to adapt permissions in real time. This enhances security by preventing unauthorized actions even when credentials are compromised or misused.
- *Attribute-Based Access Control (ABAC):* ABAC enhances flexibility by considering multiple attributes, such as user identity, time of day, device used, location, and behavioral context, to evaluate access. For example, ABAC can deny access if a login attempt comes from an unrecognized device during off-hours, even if the user's credentials are valid. This granular,

context-aware model is especially suited for mitigating social engineering attacks by minimizing permissions to only those necessary under the current context and reducing attack surfaces. ABAC also helps prevent lateral movement, where an attacker pivots between systems after an initial compromise (NIST, 2017).

- *Contextual and Adaptive Authorization Models:* More advanced approaches combine RBAC or ABAC with behavioral analytics to detect anomalies or abnormal access patterns. These adaptive access solutions use machine learning or risk scores to flag unusual activities and apply step-up authentication or restrict permissions in real-time.

**Pros:**

- *ABAC and adaptive models provide granular, dynamic control:* These models evaluate multiple context-based attributes (e.g., location, device, time) before granting access, making them more resistant to misuse following a social engineering attack.
- *Support for the enforcement of least privilege principles:* Access is granted strictly on a need-to-know basis, limiting the exposure of sensitive data and reducing the attack surface in case of compromised credentials.

**Cons:**

- *ABAC is complex and costly to implement and manage:* Defining and maintaining attribute-based policies across dynamic cloud environments requires specialized knowledge and can increase administrative overhead.
- *Requires ongoing policy evaluation and behavioral baselining:* Adaptive models rely on up-to-date behavioral baselines and continuous monitoring to remain effective, which may demand additional tooling and expertise.

### 5.2.3 Data Protection

Encryption protects the confidentiality of data both at rest and in transit. Even if attackers gain access to an encrypted system, they cannot exploit its contents unless they succeed in deceiving users into decrypting the data, disclosing it, or revealing the encryption keys. This is why social engineering attacks often aim to extract unencrypted data from unsuspecting users.

Beyond encryption, broader data protection techniques, such as secure backup, data masking, secure deletion, anonymization, and tokenization, offer complementary defense mechanisms as they address different stages of the data lifecycle and protect against distinct types of threats. For example, encryption safeguards data confidentiality during storage and transmission, while data masking limits the exposure of sensitive data during use or testing. Secure deletion ensures that no residual data remains after it is no longer needed, and tokenization replaces sensitive elements with non-sensitive equivalents. These methods are typically applied in different contexts rather than simultaneously, with each serving a specific function within the overall data protection strategy. Together, they contribute to a more resilient security posture by reducing the attack surface and mitigating potential harm in the event of a control failure.

Still, a central concern remains: how effective are these techniques specifically against social engineering? The answer depends largely on the use case and the manner of implementation. To better assess their contribution, the following strengths and limitations can be identified:

**Pros**:

- *Confidentiality by default*: Encryption ensures that even if data is intercepted or accessed, it remains unreadable without the decryption key.
- *Minimization of sensitive exposure*: Techniques like data masking, anonymization, and tokenization limit the amount of directly exploitable information available to both insiders and attackers.
- *Damage limitation:* Secure deletion and backups reduce the long-term impact of a successful breach by ensuring that stolen or deleted data can either be restored or rendered useless, respectively.
- *Resilience against indirect attacks:* Even if attackers succeed in phishing a user, well-implemented tokenization can prevent access to raw sensitive data.

**Cons**:

- *Dependent on user behavior:* If users are tricked into decrypting or exporting sensitive data, or into disclosing the respective (symmetric or decryption) keys, these protections can be circumvented.

- *Operational complexity:* Implementing data protection techniques (especially tokenization and anonymization) often requires major changes in data handling procedures and application architecture.
- *Not foolproof against credential theft:* Encryption and data masking protect stored content, but they do not prevent attackers from logging in with stolen credentials and accessing decrypted data legitimately. However, when data masking or anonymization is properly applied, the exposed information is typically de-identified or non-sensitive, which significantly reduces the potential impact of such an incident.

By recognizing these strengths and limitations, organizations can better understand that while data protection mechanisms are essential, they must be complemented by user training and access control to effectively counter social engineering attacks or mitigate their impact.

### 5.2.4 Network Segmentation

Network segmentation plays an essential role in limiting the movement of attackers within cloud environments. Segmentation techniques, such as Virtual LANs (VLANs), subnetting, and micro-segmentation, isolate critical assets and reduce the attack surface. If a social engineering attack leads to credential compromise, segmentation can prevent the attacker from accessing sensitive systems beyond their initial entry point.

**Pros:**

- *Reduces attacker movement post-compromise:* By isolating resources into separate network segments, an attacker who compromises one segment (e.g., via stolen credentials) cannot easily pivot to others, limiting lateral movement.

- *Enables implementation of security zones:* Organizations can group systems by sensitivity or function (e.g., production vs. development), applying stricter controls to high-risk zones, which supports defense-in-depth strategies.

**Cons:**

- *Adds architectural complexity:* Designing and maintaining an effective segmentation strategy, especially in dynamic cloud environments, can require significant planning and expertise.
- *Misconfiguration can negate its benefits:* Poorly implemented segmentation (e.g., overly permissive rules or flat networks) may leave critical systems exposed, undermining the intended security gains.

### 5.2.5 Intrusion Detection and Prevention

Security monitoring is vital. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) continuously monitor not only network traffic but also system-level activities within machines or nodes, whether physical or virtual, for signs of malicious behavior. These systems typically rely on signature-based or anomaly-based detection methods to identify suspicious activity. For example, an IDS may trigger an alert when it detects repeated failed login attempts, unauthorized port scanning, or unusual data transfer volumes

Such technologies do not entirely prevent social engineering attacks, but they are invaluable in detecting and responding to them before severe damage is achieved. Integration with incident response platforms ensures that alerts lead to swift/proper action, either automatically through predefined response rules or manually by security administrators, depending on the nature and severity of the detected event.

**Pros:**

- *Detects real-time indicators of compromise:* Continuous monitoring enables early detection of unusual or malicious activity, helping to stop attacks before they escalate.

- *Identifies insider threats and social engineering patterns:* Behavioral analysis can reveal anomalies—such as unusual access times or unauthorized data access—that often follow successful social engineering attacks.

**Cons:**

- *Prone to false positives:* Automated systems may flag legitimate behavior as suspicious, leading to alert fatigue and reduced trust in alerts if not properly calibrated.
- *Risk of disrupting legitimate activity:* Automated prevention mechanisms can mistakenly block or interrupt valid user actions or processes, potentially causing downtime or workflow interruptions until administrators review and resolve the event.
- *Requires tuning and skilled analysts:* Effective use demands regular tuning of detection rules and involvement of experienced personnel to investigate alerts and distinguish between real threats and benign anomalies.

### 5.2.6 Sandboxing

Sandboxing is a cybersecurity technique that involves executing potentially harmful files, programs, or scripts in an isolated, controlled environment, typically a virtual machine (VM), container, or emulated environment, completely separated from the host system. This technique allows analysts, automated systems, or threat detection tools to safely observe the behavior of suspicious content and determine whether it is malicious, without risking compromise to the main infrastructure.

In the context of social engineering (SE) attacks, sandboxing plays a crucial role in examining files or payloads delivered through phishing emails, deceptive links, or malicious attachments, common vectors in SE scenarios. For example, an email may trick a user into downloading a PDF or Word document containing embedded scripts or malware. Before such files are allowed to reach user endpoints or sensitive cloud resources, they can be executed in a sandbox where their behavior is monitored for malicious indicators, such as attempts to escalate privileges, access sensitive directories, or initiate outbound network connections.

Sandboxing also supports automated malware classification and integration with broader threat intelligence platforms, enabling rapid correlation with known indicators of compromise (IOCs) and the detection of previously unknown threats (zero-day exploits).

**Pros:**

- *Prevents execution of unknown or zero-day malware* on production systems by isolating untrusted code in a safe environment, thus mitigating one of the main risks posed by SE-based payload delivery.
- *Allows real-time observation and behavioral analysis of potentially malicious code*, enabling defenders to understand threat behavior and develop appropriate countermeasures, such as updating antivirus signatures or adjusting detection rules.

**Cons:**

- *Resource-intensive and may introduce operational overhead*, as sandbox environments consume computing power and may require specialized hardware or configuration to run efficiently and scale across multiple analysis tasks.
- *Sophisticated malware may detect sandbox environments and alter behavior*, using sandbox-evasion techniques (e.g., delaying execution, checking for virtualization artifacts) to avoid detection and appear benign during the analysis phase.

### 5.2.7 Threat Emulation

Threat emulation, also referred to as breach and attack simulation (BAS), involves replicating the tactics, techniques, and procedures (TTPs) used by real-world adversaries in a controlled and repeatable way. Unlike traditional vulnerability assessments or penetration testing, threat emulation does not just focus on identifying misconfigurations or software flaws, it evaluates how security systems and personnel respond to complex attack chains, often simulating real-world scenarios from initial compromise to impact.

In the context of social engineering (SE), threat emulation plays a particularly valuable role in testing an organization’s preparedness after the human layer has already been compromised. For example, a

simulation may start from the assumption that an attacker has successfully phished a user and obtained valid credentials. The exercise then explores how the attacker could proceed, attempting lateral movement[15], privilege escalation, or data exfiltration, and how the cloud infrastructure and security operations center (SOC) detect, contain, and respond to these activities.

This approach provides a realistic, end-to-end perspective of an organization's defense posture against sophisticated, multi-stage SE-based attacks. It helps validate detection rules, stress-test response workflows, and uncover defensive blind spots that might not be apparent in isolated technical reviews.

**Pros:**

- *Reveals blind spots in defense mechanisms post-compromise*, especially those that arise only after initial human errors—such as credential theft or privilege abuse—are successfully exploited.
- *Improves incident response capabilities through realistic simulations,* enabling organizations to rehearse their detection and containment strategies under conditions that mirror real-world attacker behavior. This often leads to improved playbooks, tuned monitoring systems, and better-trained SOC personnel.

**Cons:**

- *Requires expertise and careful planning to avoid unintended disruptions,* since improperly scoped or overly aggressive simulations might trigger false alarms or interfere with production systems.
- *May be time-consuming and costly to conduct regularly*, particularly if simulations involve complex environments, require specialized tooling (e.g., MITRE ATT&CK-based emulation platforms), or demand coordination across teams.
- *Potential risk of sensitive data exposure:* Threat emulation activities, especially when executed by third-party providers, may inadvertently access or expose confidential data. To mitigate this

[15] *Lateral movement* refers to the techniques used by attackers to move through a network or system after gaining initial access.

risk, strict data-handling procedures and confidentiality or non-disclosure agreements (NDAs) should be established prior to testing.

### 5.2.8 Environment Isolation

In cloud-native architectures, environment isolation refers to the separation of workloads, applications, or tenants through technologies, such as containers and virtual machines (VMs). This ensures that if one environment is compromised—due to a successful social engineering attack or vulnerability exploitation, the breach does not automatically propagate to other parts of the system. Unlike sandboxing, which isolates and executes specific files or code snippets in a temporary, controlled environment for the purpose of behavioral analysis, environment isolation applies at the broader infrastructure level. It encompasses entire applications or services, enforcing strict boundaries between them to contain the blast radius of a potential attack. This architectural isolation is particularly useful in multi-tenant cloud environments or microservices-based deployments.

**Pros:**

- *Limits the impact of a breach to a single isolated environment:* This containment strategy prevents attackers from pivoting to other services or tenants, reducing potential damage and exposure.
- *Enhances security in shared cloud infrastructures:* Isolation creates clear boundaries between tenants or services, supporting compliance with multi-tenant data protection requirements.

**Cons:**

- *Increases management complexity and infrastructure cost:* Maintaining isolated environments demands additional configuration, monitoring, and resource allocation across multiple layers.
- *Requires sophisticated orchestration and security policies to maintain isolation:* Ensuring isolation effectiveness depends on well-defined container orchestration, network segmentation, and strict access control rules.
- *Risk of non-proper resource isolation:* Even with strong separation mechanisms, misconfigurations or shared hardware resources can enable side-channel attacks or cross-tenant

data leakage, allowing adversaries to exploit vulnerabilities within multi-tenant or containerized environment

## 5.2.9 Identity-Based Forensics

Identity-based forensics is an increasingly vital component of detection frameworks. By leveraging identity and access management (IAM) logs, such as AWS CloudTrail or Azure AD Sign-in Logs, security teams can trace credential misuse, session hijacking, or lateral movement attempts in cloud environments. This helps in post-incident investigation and strengthens defenses by identifying patterns of social engineering exploitation.

**Pros:**

- *Enables forensic investigation into compromised credentials and abnormal behavior:* IAM logs provide detailed records of user activity, helping investigators trace the origin and scope of social engineering incidents.
- *Supports incident response through IAM visibility:* Real-time visibility into account activity allows quick revocation of access and containment of breaches caused by compromised identities.

**Cons:**

- *Requires integration across diverse cloud services:* Centralizing and correlating IAM data from multiple platforms can be technically challenging and time-consuming.
- *Dependent on timely log collection and analysis:* Delays or gaps in log availability may hinder the ability to detect or respond to credential abuse effectively. Moreover, comprehensive log analysis requires sufficient computational and storage resources, which may increase overhead and, in shared cloud environments, temporarily affect system performance or resource availability for tenants.

## 5.2.10 Behavioral Analytics

User and Entity Behavior Analytics (UEBA) play a critical role by analyzing deviations in user behavior to identify potentially malicious activity. For instance, if a user typically logs in from a single

location and suddenly accesses the system from a new country at an unusual hour, UEBA systems can raise alerts or initiate step-up authentication procedures.

**Pros:**

- *Enhances detection of insider threats and social engineering tactics:* By learning normal behavior patterns, UEBA systems can flag deviations that may indicate compromised users or malicious insiders.
- *Provides proactive alerts based on usage anomalies:* Anomaly-based alerts enable earlier detection of potential attacks, allowing preventive actions before serious harm occurs.

**Cons:**

- *Relies on high-quality data and tuning to avoid false positives:* Inaccurate baselines or insufficient data can lead to frequent false alarms, which may reduce trust in the system.
- *Risk of disrupting legitimate activity:* False positives may trigger automated responses, such as account lockouts or access denials, that interrupt valid operations until manual verification occurs.
- *May require integration with multiple monitoring and identity platforms:* Effective behavioral analytics often depends on aggregating data across various sources, which can complicate deployment and maintenance.

## 5.2.11 Summary and Evaluation of Technical Measures

Technical measures provide vital defenses against social engineering threats in cloud environments. However, no single method is sufficient alone. The combination of prevention (e.g., MFA, encryption), detection (e.g., UEBA, IDS), and containment (e.g., segmentation, sandboxing) ensures a more robust protection.

**Overall Pros of Technical Measures:**

- *Automation and scalability in defense:* Many technical tools can be deployed at scale across cloud environments and operate with minimal human input, though the degree of automation

and scalability varies depending on the specific countermeasure and its integration complexity.

- *Objective policy enforcement across infrastructure:* Once defined, policies (e.g., access control) are enforced consistently by automated systems, reducing the risk of human error during execution. However, the initial specification of such policies may still involve subjective decisions or misconfigurations that affect their effectiveness.
- *Immediate threat detection and response:* Certain technical measures, particularly monitoring and detection tools such as IDS/IPS and UEBA, enable real-time identification and mitigation of attacks, limiting potential damage before threats escalate.

**Overall Cons of Technical Measures:**

- *Cannot fully mitigate the human factor:* Social engineering targets human behavior, which technical systems alone cannot predict or control.
- *Require integration with user behavior and organizational culture:* Successful deployment depends on how well tools align with human workflows and training efforts. If security controls are perceived as overly restrictive or disrupt routine tasks, users may attempt to bypass them, reducing overall effectiveness. Therefore, technical solutions must be supported by awareness programs and usability-focused design to encourage consistent adoption.
- *May be expensive to deploy and maintain:* Advanced security solutions often involve licensing, skilled personnel, and ongoing maintenance, posing a challenge for smaller organizations. However, the increasing availability of cloud-based Security-as-a-Service (SECaaS) offerings can reduce upfront costs and administrative burden, making advanced defenses more accessible to smaller enterprises.

Although a detailed comparison of technical controls is beyond the scope of this section, such an analysis would be valuable in evaluating their effectiveness based on criteria such as mitigation type, cost, integration complexity, usability, and scalability. In general, preventive controls (e.g., MFA, encryption) offer high scalability at lower cost, whereas detection and containment mechanisms (e.g., IDS/IPS, segmentation) provide stronger responsiveness but demand greater integration effort and maintenance resources.

These limitations reinforce the need to complement technical controls with user education, vendor diligence, and response planning to address social engineering threats comprehensively.

## 5.3 Incident Response and Business Continuity Planning

Incident response and business continuity planning are fundamental pillars of a robust security strategy for cloud computing environments. These processes help organizations prepare for, respond to, and recover from security incidents, including those stemming from social engineering attacks.

### 5.3.1 Creating an Incident Response Plan

An effective incident response plan (IRP) is essential for minimizing the damage caused by social engineering attacks, especially in cloud computing environments where traditional perimeter controls may be limited. While general IRPs provide broad guidelines for detecting, containing, and recovering from cybersecurity incidents, the IRP itself serves primarily as an operational and organizational strategy.

Importantly, an IRP should incorporate the technical and social measures previously described in Sections 5.1 and 5.2, such as security training, password best practices, identity-based forensics, and behavioral analytics, into a coordinated and actionable plan. The integration of these measures ensures that responses to social engineering threats are both timely and effective.

The specific composition of the IRP depends on factors, such as the organization's goals, threat landscape, resource availability, budget and internal expertise. It should also be shaped by a continuous risk management methodology to adapt to evolving threats, cloud configurations, and user behavior.

By embedding both general and SE-specific measures into the IRP, organizations can develop a responsive, resilient strategy that extends beyond detection and includes containment, recovery, and learning from incidents to inform future practices.

### 5.3.2 Regular Security Assessments and Testing

Although social engineering attacks typically target human weaknesses rather than technical system flaws, regular security evaluation, such as security assessments and penetration testing, still plays a valuable role in limiting the damage such attacks can cause.

More specifically, social engineering attacks often act as an entry point to broader system exploitation. An attacker who gains access to a user's credentials through phishing or pretexting may then attempt to exploit technical vulnerabilities within the system to escalate privileges, exfiltrate data, or disable critical services. In this context, vulnerability assessment does not directly prevent social engineering attacks but helps mitigate their potential impact by minimizing the available attack surface. This is achieved through its integration into the broader risk management process, where identified vulnerabilities are prioritized, remediated, and continuously monitored based on their potential exploitation likelihood and business impact, thereby reducing the opportunities an attacker can exploit following an initial social engineering breach.

**Security Assessment**

Security assessment refers to the systematic evaluation of an organization's technical, procedural, and human controls to identify weaknesses that could be exploited by attackers. It typically encompasses activities such as vulnerability scanning, penetration testing, configuration reviews, and compliance audits, all aimed at measuring the effectiveness of existing security measures.

According to the Cloud Security Alliance (CSA, 2017), the combination of regular security assessment and social engineering defenses can strengthen an organization's resilience against multi-stage attacks. Some concrete benefits of conducting regular security assessments in this context include:

- *Identifying post-compromise risks*: If a social engineering attack is successful, known vulnerabilities (e.g., unpatched services or excessive permissions) can be leveraged for lateral movement or privilege escalation.
- *Reducing system exposure*: Vulnerability assessment reduces exposure by systematically prioritizing and remediating weaknesses before they can be exploited. This includes enforcing

secure configurations, removing unnecessary services, and applying timely patches, thereby limiting the attack surface available to adversaries.

- *Strengthening defense-in-depth*: Security assessment complements non-technical defenses (e.g., training and awareness) by ensuring that the technical environment is robust, even when the human layer fails.

**Penetration Testing and Its Specialized Forms**

Penetration testing (or ethical hacking) simulates real-world attack scenarios to evaluate how well an organization can detect, prevent, or respond to intrusions. Unlike security assessment, penetration testing includes human-driven exploration, often extending to physical or social engineering vectors.

In the context of social engineering, specialized penetration tests can include:

- *Phishing Campaign Simulations:* Simulated phishing emails sent to employees to assess their response and awareness.
- *Vishing Exercises:* Simulated voice-based attacks that test whether employees will disclose sensitive information or grant access.
- *Physical Penetration Tests:* Attempts to access restricted areas using deception (e.g., impersonating staff or contractors).
- *Pretexting Scenarios:* Targeted engagement in which testers attempt to manipulate staff by posing as IT support or senior leadership.

These targeted simulations allow organizations to:

- Measure user susceptibility to specific types of manipulation
- Evaluate the effectiveness of awareness training programs
- Improve incident detection and escalation processes for human-origin threats

Penetration testing complements vulnerability assessment by actively simulating attack scenarios to validate the exploitability of discovered weaknesses. Cloud-specific penetration testing tools, such as Pacu for AWS environments, Google Cloud Platform (GCP) pentesting utilities, and host enumeration

frameworks like LinPEAS, WinPEAS, or Metasploit, enable security teams to test access controls, privilege escalation paths, and data exfiltration risks within virtualized and containerized infrastructures. These tools help organizations evaluate the real-world impact of potential breaches and refine their defensive configurations accordingly.

### 5.3.3 Recovery Planning

Planning for backups and recoveries is a critical component of business continuity in cloud computing environments, particularly in the aftermath of social engineering attacks. Attackers may delete, encrypt, or manipulate data after compromising user accounts, making effective backup and recovery processes vital for restoring data integrity and operational continuity.

The National Institute of Standards and Technology (NIST, 2018) recommends the following foundational practices for recovery:

- *Testing of Recovery Methods:* Conducting routine tests to validate the reliability of backup systems and ensure data can be restored quickly and accurately.
- *Documented Recovery Procedures:* Establishing detailed recovery playbooks outlining the exact steps for restoring services and minimizing downtime.

**Cloud-Specific and Automated Approaches**

In modern cloud environments, several automated tools and services exist to streamline and enhance backup and recovery efforts, tailored to the dynamic nature of cloud infrastructure:

- *Infrastructure as Code (IaC) for Recovery:* Cloud providers like AWS (CloudFormation), Microsoft Azure (ARM Templates), and Google Cloud (Deployment Manager) support declarative IaC scripts to automate the recreation of an infrastructure. These can act as a form of automated disaster recovery.
- *Automated Snapshot Management:* Services, such as AWS Backup, Azure Backup, and Google Cloud Backup and DR, offer scheduled and policy-driven backups of computers, storage, and database services, minimizing human error and enabling point-in-time recovery.
- *Automated Disaster Recovery (DR) Orchestration:* Solutions like Zerto, Veeam, or Azure Site Recovery support the automatic failover and recovery of entire environments across regions

or clouds. These platforms enable predefined DR workflows to be executed in response to an attack or incident.

- *Policy-based Data Retention:* Modern cloud platforms also offer automated data lifecycle policies (e.g., AWS S3 Lifecycle Rules, Azure Blob Lifecycle Management) to enforce backup retention strategies[16] without manual oversight.

These cloud-native and third-party solutions reduce the need for manual intervention, ensure fast response during incidents, and provide automated recovery workflows, all essential for minimizing the impact of social engineering attacks.

## 5.4 Vendor Management and Due Diligence

Vendor management and due diligence are critical components of a comprehensive security strategy for cloud computing environments.

### 5.4.1 Cloud Provider Evaluation

Selecting a cloud service provider (CSP) requires more than a checklist of best practices, it demands the application of structured methodologies that ensure the provider aligns with an organization's specific security, compliance, and operational needs. Several frameworks have been proposed to standardize and guide this selection process.

One of the most recognized frameworks is the Cloud Security Alliance's Cloud Controls Matrix (CSA CCM), which represents a detailed control framework aligned with industry standards, such as ISO/IEC 27001, NIST 800-53, and COBIT. Organizations can use the CCM to assess CSPs across 197 control objectives grouped under 17 domains, including identity and access management, application security, and threat and vulnerability management.

In practice, this evaluation is often conducted using the Consensus Assessments Initiative Questionnaire (CAIQ), which allows CSPs to perform a structured self-assessment of their security

[16] Backup retention strategies refer to predefined rules or policies that determine how long backup data is stored, when it should be transitioned to lower-cost storage tiers, and when it should be deleted. These strategies help organizations manage storage costs, ensure regulatory compliance, and maintain data availability over time.

posture. The CAIQ is directly mapped to the CCM and enables customers to review how the provider meets each control objective through standardized yes/no questions and explanatory fields. Some CSPs also publish their CAIQ responses publicly through the CSA's Security, Trust & Assurance Registry (STAR), enhancing transparency and comparability.

Another widely used guide is the NIST Special Publication 800-144, which outlines security and privacy considerations for public cloud computing. NIST suggests evaluating cloud providers based on their architecture, governance model, identity management practices, and data protection mechanisms.

In addition, the European Union Agency for Cybersecurity (ENISA) provides a Cloud Computing Risk Assessment methodology (ENISA, 2009). This approach identifies and categorizes 35 cloud-specific threats, linking them to 8 organizational assets and offering guidelines on how to evaluate whether a CSP has mitigation strategies in place for each threat.

A typical structured evaluation methodology, as recommended in cloud security best practices (CSA, 2019; NIST, 2012), typically includes the following stages:

- *Define Security and Compliance Requirements*: Based on industry regulations (e.g., GDPR, HIPAA), internal risk appetite, and operational needs.
- *Initial Vendor Screening*: Using predefined criteria or compliance questionnaires, such as CAIQ provided by CSA.
- *Detailed Security Assessment*: Apply tools, such as the CSA CCM, NIST 800-144 controls, or perform third-party audits to verify technical and procedural controls.
- *Risk Scoring and Comparison*: Assign quantitative or qualitative risk scores to each provider based on their ability to meet security and business needs.
- *Decision and Documentation*: Select the provider with the best alignment and maintain detailed records of the evaluation process for compliance and audit purposes.

Using such structured approaches not only improves the credibility of provider selection but also ensures transparency and accountability. These methods are particularly important in mitigating, and, where social engineering–aware controls are present, also preventing risks related to social

engineering, as they help verify whether CSPs have robust identity verification protocols, SE-aware security training for personnel, incident response readiness, and monitoring capabilities.

By adopting frameworks like CSA CCM, ENISA's Risk Assessment, or NIST SP 800-144, organizations can move beyond wishful thinking to a repeatable, defensible evaluation process grounded in the best global practices.

### 5.4.2 Security-Aware Service Level Agreements (SLAs)

Service Level Agreements (SLAs) are formal contracts between cloud service providers and their customers, specifying the terms under which services will be delivered, including the expected performance, responsibilities, and obligations of both parties. A crucial aspect of SLAs in cloud environments is the inclusion of security-related requirements, which are designed to protect confidentiality, integrity, and availability of data and services (Cloud Security Alliance, 2016).

These security requirements are not always direct countermeasures to social engineering attacks, but they can guide the design and implementation of cloud services toward meeting resilience goals. While a social engineering attack might not be directly prevented by an SLA clause, the damage such an attack can cause may be mitigated through predefined procedures and safeguards provided that these clauses are actively enforced by the provider(Huth & Cebula, 2011). Because enforcement ultimately depends on provider compliance, combining SLA evaluation with provider assessment processes, such as audits, independent certifications (e.g., ISO/IEC 27001, SOC 2), or third-party verifications, can help ensure that these obligations are both met and externally validated.

The following are examples of security-related SLA requirements, which may need to be fulfilled by either or both parties (provider and customer):

- *Encryption Standards:* The SLA can require the use of strong encryption protocols, such as AES-256 for data at rest and TLS for transit. These safeguards ensure that even if an attacker gains access to the system (potentially through social engineering), they may not be able to read or manipulate sensitive information (Cloud Security Alliance, 2017).
- *Regular Security Audits:* Although not always explicitly required in standard SLAs, cloud providers often conduct periodic internal or third-party audits to demonstrate compliance with

current security standards and best practices. These audits can help identify and resolve vulnerabilities that could be exploited following a successful social engineering breach (Mell, Grance, & NIST, 2011).

- *Data Breach Notification:* The SLA should outline strict timelines and procedures for notifying the customer in case of a data breach. This allows for faster response and damage control, especially important if a social engineer has already infiltrated the system (Cloud Security Alliance, 2017).
- *Data Ownership and Handling:* The SLA must clarify who owns the data and how it will be handled upon contract termination. Social engineering attacks often attempt to exploit unclear responsibilities to misappropriate data (Huth & Cebula, 2011).
- *Disaster Recovery (DR) and Business Continuity (BC) Planning:* The agreement should define recovery time objectives (RTOs) and recovery point objectives (RPOs) to ensure rapid (cloud) service restoration after an incident. Although these measures are also discussed separately (in Section 5.3), their inclusion here emphasizes the contractual obligation to uphold such strategies (Gartner, 2020).
- *Security monitoring and incident detection:* The SLA should define requirements for continuous monitoring and timely detection of anomalous activities that may indicate security breaches or social engineering–related exploits (e.g., insider threats, unusual access patterns). These objectives are often met through mechanisms such as Intrusion Detection and Prevention Systems (IDPS), but the agreement should emphasize the security goal rather than mandate a specific technical implementation (Cloud Security Alliance, 2016)
- *Data Privacy and Sovereignty:* The SLA must ensure that data is stored and processed in compliance with relevant regulations, such as GDPR or HIPAA. Social engineering attackers may try to exploit jurisdictions with weaker privacy enforcement, so location control and clarity are vital (Huth & Cebula, 2011).
- *Incident Response Time:* The SLA should define maximum response times for different types of security incidents. Quick containment is essential in minimizing the impact of breaches, including socially engineering ones (Mell et al., 2011).

While not all of these requirements are social engineering-specific, their enforcement helps reduce the attack surface and improve recovery posture, making it harder for attackers to succeed or cause

harm. Furthermore, as many social engineering attacks succeed by exploiting human and organizational weaknesses, having clear, enforceable contractual obligations improves accountability and ensures a proactive stance on security from both sides.

In summary, these requirements are security-related obligations that must be mutually agreed upon, monitored, and enforced. Their inclusion in SLAs enhances trust and contributes to a layered defense strategy that mitigates the risk and impact of social engineering attacks in cloud environments.

### 5.4.3 Regular Vendor Audits and Reviews

Regular vendor audits and reviews are critical components of effective cloud vendor management, supporting the overall security posture of cloud computing environments. These evaluations ensure that cloud providers adhere to their contractual obligations and comply with relevant security standards and regulations (Cloud Security Alliance, 2017).

This section complements Section 5.3.2, which addresses internal assessments conducted by the cloud customer. In contrast, this section focuses primarily on external evaluations of the cloud provider, conducted either by the customer (when permitted) or by specialized third-party auditors. It differs from the provider self-assessment processes discussed in Section 5.4.1, as it examines independent and externally verified audits that offer higher objectivity and assurance of compliance.

According to the Cloud Security Alliance (2017), such audits may include vulnerability assessments, penetration testing, security log analysis, and evaluations of incident response plans. These activities allow organizations to identify gaps in the provider's security framework, particularly vulnerabilities that could be exploited via social engineering techniques once the latter becomes successful.

**Customer Involvement in Audits.** While third-party auditors typically perform external assessments, customers may also be granted limited audit rights under specific conditions. These rights are often formalized within security-oriented SLAs or compliance-related clauses, allowing customers to verify that appropriate security controls are in place.

The Service Level Agreement (SLA) should clearly outline these audit rights, defining:

- The scope and depth of audits that customers may perform.

- Required notice periods and the acceptable time frames for audits to avoid disrupting cloud services.
- Obligations of both parties, including the provider's cooperation and the customer's duty to coordinate with the provider before launching assessments.

Unrestricted and uncoordinated security testing could impact service availability or stability. Therefore, SLAs should stipulate that audits initiated by customers occur only with the provider's prior approval and within designated time windows and restricted scopes.

**Responsibility and Follow-up.** The SLA should also define how security issues discovered during audits must be addressed. However, it is important to acknowledge that:

- Not all findings will result in mandatory remediation, especially if the issue is low-risk, already mitigated, or attributable to customer misconfiguration.
- The provider's responsibilities may vary depending on the cloud service model used (IaaS, PaaS, or SaaS).

As such, providers may only commit to resolving verified, significant vulnerabilities that fall under their domain of responsibility.

**Automated and Specialized Auditing Tools.** Currently, most audit processes are manual or semi-automated. However, there is growing interest in tools that can facilitate automated auditing of providers. Solutions leveraging machine learning, anomaly detection, or cloud configuration management (e.g., AWS Inspector, Azure Security Center) can:

- Continuously assess provider compliance.
- Detect configuration errors that could facilitate social engineering exploits.

Research in this area is ongoing, and more advanced automated frameworks tailored specifically for detecting and mitigating social engineering threats in cloud provider infrastructure remain limited (Suhonen & Martínez, 2024).

**Relevance to Social Engineering.** While many audit practices are general in nature, they can indirectly address social engineering risks. For instance:

- Penetration testing may simulate social engineering entry points (e.g., phishing simulations).
- Log reviews can uncover signs of insider manipulation or credential misuse due to social engineering.
- Incident response plan audits assess how providers are prepared to react to socially engineered intrusions.

## 5.5 Conclusions

In summary, regular vendor audits and reviews, when designed and executed with clarity, balance, and cooperation, play an essential role in reducing the risks of social engineering attacks. Security certifications can complement these efforts by providing externally verified assurance of a provider's adherence to recognized security standards. While such certifications are often the result of formal audit processes, they can also serve as independent indicators of trustworthiness, particularly when direct audit access is limited. However, like all countermeasures discussed in this chapter, audits alone are not sufficient. A layered and integrated defense strategy is essential, one that combines user education, technical controls, incident response capabilities, and rigorous vendor governance.

Each category of defense contributes uniquely to the organization's resilience: user training addresses human susceptibility; technical controls focus on detection and containment; incident response ensures rapid recovery; and vendor audits verify external assurance. The selection and implementation of specific measures within these categories must be tailored to the organization's risk profile, budget constraints, technical expertise, and the existing security posture. Organizations with mature internal controls may prioritize third-party assessments, while those with limited resources may initially focus on user awareness and basic technical safeguards.

Ultimately, an effective security strategy against social engineering is not built on a single technique, but on the synergistic application of multiple, mutually reinforcing measures that address both human and technical vectors of attack. Therefore, a risk-based and context-aware selection of methods, grounded in both internal evaluations and external obligations, ensures a more resilient and adaptive cloud security posture.

# 6. Challenges, Research Gaps and Future Directions

Despite the substantial progress made in preventing, detecting, and mitigating social engineering attacks in cloud computing systems, several critical challenges and open research gaps remain. These gaps limit the effectiveness of current defense mechanisms and highlight areas where further research and innovation are required.

This chapter identifies and discusses the key challenges that persist in the field, along with potential research directions and practical approaches for addressing them.
To ensure clarity and systematic presentation, each challenge and its corresponding future paths are discussed in separate sections that follow. These include challenges related to the human and psychological factors underlying social engineering, the need for adaptive and AI-enhanced training models, limitations of existing detection mechanisms, emerging vulnerabilities in edge and fog computing, privacy and compliance concerns, and the integration of regulatory and legal frameworks.

## 6.1 Lack of Focus on Psychological Components and Adaptive Training Tactics

The human component continues to be the weakest link in the security chain when it comes to defending against social engineering attempts or sophisticated attacks that begin with psychological manipulation. Numerous studies, such as the one conducted by Mitnick and Simon (2002), have emphasized that understanding the underlying psychological principles, such as authority bias, reciprocity, trust, and urgency, is crucial to designing more effective prevention strategies.

Future research should therefore focus on integrating psychological and behavioral science into cybersecurity awareness programs, exploring how specific cognitive biases can be counteracted through targeted interventions. For instance, incorporating psychological profiling or scenario-based simulations could help security teams anticipate user reactions and improve overall resilience against manipulation.

## 6.2 Adaptive Training Models

Another promising research direction concerns adaptive training models that dynamically adjust to user learning styles, behavior patterns, and evolving threat scenarios. Current awareness programs are often static and one-size-fits-all, limiting their long-term effectiveness.

Adaptive systems, possibly leveraging AI or machine learning, could personalize training frequency, difficulty, and content based on user performance or susceptibility indicators identified in prior simulations. Such approaches would enable continuous learning and provide organizations with actionable feedback loops, ensuring that awareness programs remain relevant against the ever-changing tactics of social engineering attacks.

Moreover, adaptive learning could be integrated with psychological profiling to align training methods with user personality traits or decision-making patterns, increasing engagement and retention rates.

## 6.3 Lack of Advanced Detection Techniques

As discussed by Heartfield and Loukas (2016), existing detection methods for social engineering attacks, such as anomaly detection, behavioral analysis, and heuristic-based systems, are still limited in their ability to detect highly sophisticated or multi-step attacks.

Most of these techniques have been primarily designed and evaluated for detecting single-step or well-defined attack scenarios, such as phishing emails or impersonation attempts, rather than complex, multi-phase social engineering campaigns. Even when they are conceptually capable of identifying broader attack chains, their performance often degrades in realistic, dynamic environments where attacker behavior evolves over time and lacks consistent patterns.

Although these detection methods were only briefly referenced in this study and not analyzed in depth, they highlight a critical research challenge, namely, the need for detection frameworks that can reliably identify multi-step, context-aware social engineering attacks in realistic cloud environments rather than under controlled or simplified conditions.

Future work should focus on developing more adaptive, context-sensitive, and explainable detection frameworks. In particular, machine learning and artificial intelligence techniques that incorporate natural language understanding, user behavior baselining, and real-time threat assessment could offer improved accuracy and responsiveness in identifying social engineering attempts across cloud environments.

## 6.4 Social Engineering in Edge and Fog Computing Environments

According to Alrawais et al. (2017), social engineering attacks are becoming more prevalent due to the widespread adoption of Internet of Things (IoT) devices and increased usage of mobile devices. In this context, edge devices are increasingly targeted by social engineering attacks. While there is limited research on the impact of social engineering attacks specifically on edge devices, this area represents an emerging field of study with significant implications for cloud computing, especially in fog and edge computing scenarios.

The connection between social engineering attacks and cloud computing lies in the extended ecosystem that includes both edge and fog computing. Edge computing refers to the distributed infrastructure that brings computation and data storage closer to the edge devices, reducing latency and enhancing real-time processing capabilities. Fog computing extends this concept further by introducing an intermediate layer of computation and storage between the edge and the centralized cloud. This intermediate layer, often composed of gateways, routers, or local servers, enables additional processing, coordination, and security functions before data reaches the cloud.

Given that edge devices are susceptible to social engineering attacks, securing the entire cloud computing ecosystem requires addressing all vulnerabilities at the edge and intermediate levels. In this context, the vulnerabilities primarily stem from human-related factors rather than the devices themselves. Social engineering attacks typically target administrators, developers, or maintenance personnel responsible for managing or configuring edge and fog systems.

By manipulating these individuals, through tactics such as phishing, pretexting, or fraudulent maintenance requests, attackers can obtain credentials or persuade administrators to alter configurations, install malicious updates, or disable security mechanisms. Technical vulnerabilities

such as weak authentication, insecure firmware update processes, and poor access segregation can then be exploited as a result of such human compromise.

While research in this area is limited, future work should focus on extending existing mechanisms, such as access control, trust management, and secure communication protocols, to become social engineering aware. This could include integrating behavioral anomaly detection for administrative actions, enhancing identity verification for remote maintenance and configuration tasks, and developing collaborative alert systems that correlate suspicious behavior between edge, fog, and cloud layers.

Such approaches would enable a more holistic and adaptive security posture, strengthening the resilience of distributed cloud environments against both technical and human-origin threats.

## 6.5 User Privacy Compromise

Jang-Jaccard and Nepal (2014) highlight that some detection approaches may involve monitoring user behavior, analyzing communication patterns, or examining personal data to identify indicators of social engineering attacks. In doing so, user privacy may be unintentionally compromised in several ways.

For example, sensitive data may be moved across jurisdictions or processed in external systems without proper safeguards, violating data sovereignty or compliance requirements. Additionally, explainable AI (XAI) models, which aim to provide transparency in detection outcomes, may inadvertently expose patterns or attributes that allow others to infer private user information such as login habits, location data, or communication contents.

To address these risks, researchers and practitioners should adopt privacy-by-design principle**s** in the development of social engineering detection systems. This includes employing privacy-preserving techniques such as anonymization, encryption, or differential privacy to minimize personal data exposure during detection processes.

By incorporating these measures, detection systems can strike a balance between effectively identifying social engineering attacks and safeguarding user privacy. The goal is to ensure that the

deployment of advanced behavioral analytics or AI-based systems does not compromise users' trust or data protection rights.

## 6.6 Missing Links Between Correlated SE Attacks

Attacks based on social engineering are frequently used as a gateway for other forms of cyberattacks. While the previous challenge emphasized the difficulty of detecting complex, multi-step attacks, this challenge focuses on the lack of coordination and data correlation between distinct detection systems.

The interplay between attack phases is often underexplored in current architectures, which tend to treat different types of attacks as isolated events. This lack of correlation can lead to detection gaps and delayed response, especially when the initial social engineering vector goes unnoticed.

For instance, if a phishing detection tool flags an email as suspicious but this information is not shared with an identity management or intrusion detection system, a subsequent privilege escalation attempt by the same compromised account may not be recognized as part of a broader attack chain.

Future research should therefore focus on cross-system awareness and inter-tool communication, for example, enabling partial confidence scores or anomaly signals to be shared between systems such as UEBA, EDR, and access control engines. This would allow dynamic policy adjustment (e.g., enforcing MFA or temporarily limiting data access) in response to suspicious patterns detected elsewhere.

## 6.7 Lack of Assurance of Regulation and Compliance

According to Power (2016), there is a need for greater understanding of the legal and regulatory elements associated with social engineering attacks. This includes examining how data protection laws (e.g., GDPR), cybersecurity directives (e.g., NIS2), and industry standards (e.g., PCI-DSS) can incentivize better security practices, as well as what legal remedies are available to victims.

Such research could adopt an interdisciplinary approach combining cybersecurity, legal studies, and behavioral science. It may include surveys, interviews, or case studies to assess how regulatory mechanisms influence awareness, accountability, and resilience.

Another critical direction concerns the lack of consistency and harmonization across international regulations. Differences in data protection laws, compliance standards, and enforcement mechanisms between countries or continents complicate incident reporting, cross-border investigations, and liability determination.

Although progress has been made toward international harmonization, explicit regulatory guidance addressing social engineering threats remains limited. Future research could explore how existing frameworks might be expanded to include social engineering–specific provisions for awareness programs, reporting obligations, and identity verification standards.

## 6.8 Summary

In conclusion, significant progress has been made in understanding and addressing social engineering attacks in cloud computing environments. However, several open research questions and practical challenges remain unresolved.

While this study primarily focused on technical, organizational, and measures that increase the overall user awareness regarding se attacks, future research should emphasize the integration of behavioral and legal approaches with existing technical controls. Behavioral techniques, such as psychological profiling, user behavior monitoring, and adaptive awareness training, can help address the human factors that social engineering exploits. Legal mechanisms, including stricter compliance frameworks, data protection regulations, and liability enforcement for cloud providers, can further enhance deterrence and accountability.

The combination of these approaches represents a promising direction for developing a holistic and resilient defense strategy against social engineering in the cloud.

# 7. Conclusions

In conclusion, this thesis report has made significant contributions in understanding the landscape of social engineering threats in cloud computing environments and strategies to mitigate such attacks. The exploration of different types of social engineering attacks, including phishing, pretexting, baiting, and tailgating, has revealed the intricate and multifaceted nature of these threats.

This study has also brought into light the importance of human factors in the security of cloud environments. It highlighted that despite the advancements in technology, the human element remains a vulnerable link in the security chain, susceptible to manipulation and exploitation. The experience gained during this review underscores the need for a holistic approach that integrates technological and human-focused strategies and measures in tackling social engineering threats.

Several categories of mitigation measures were reviewed, with a focus on their applicability to cloud computing environments. These included User Awareness and Education, Technical Controls, Incident Response and Business Continuity Planning, and Vendor Management and Due Diligence. Within these categories, specific measures, such as multi-factor authentication, access control, encryption, network segmentation, incident response planning, regular security assessments, and vendor audits were analyzed.

One of the key conclusions, outlined in Chapter 5, is that no single measure or category alone is sufficient to address the multifaceted nature of social engineering threats. Rather, the findings support the need for a multi-layered, defense-in-depth strategy that integrates these categories and adapts to the evolving tactics used by attackers.

User awareness and training emerged as a critical aspect of any security strategy. It is clear that educating users about the types of social engineering attacks, their indicators, and safe practices is an effective method to reduce the risk of successful attacks.

On the technological side, strategies like multi-factor authentication, access control, encryption, and network segmentation were found to be potent in securing cloud environments. However, more social engineering- and cloud-specific measures also emerged as critical. These include identity-based forensics (e.g., using IAM logs to detect credential abuse), behavioral analytics (e.g., UEBA systems

to flag anomalies), and cloud-native threat detection tools (e.g., AWS GuardDuty, Azure Defender) that can respond to suspicious activities linked to social engineering attempts.

Together, these technologies not only safeguard sensitive data but also improve detection and containment of social engineering-based breaches by restricting access and preventing lateral movement within the cloud environment.

Furthermore, the importance of incident response planning and regular security assessments was highlighted. These practices help organizations to quickly identify, respond to, and recover from social engineering attacks, thereby minimizing their impact.

Finally, the role of cloud service providers in the security of cloud environments was examined. It was concluded that organizations need to conduct due diligence in selecting their providers and ensure that security requirements are clearly defined in service level agreements and well respected by the respective providers.

While the strategies discussed in this review can significantly reduce the risk of social engineering attacks, it is essential to remember that the threat landscape is continually evolving. As such, regular reviews and updates of security strategies are necessary to ensure their effectiveness against new and emerging threats.

At the same time, this thesis identified a number of open challenges that warrant future investigation. These include the integration of social and technical measures that bridge human and technical defenses, the development of privacy-preserving detection systems, and the need to better link sequential phases of multi-stage attacks,e.g., correlating early signs of deception with follow-on technical intrusions. Addressing these challenges will require interdisciplinary research combining behavioral science, legal frameworks, cloud security, and artificial intelligence.

Lastly, from a personal and academic perspective, the **conduction of this thesis** provided valuable experience in critically evaluating complex security challenges at the intersection of human and technological domains. It deepened my understanding of real-world cloud architecture, threat modeling, and the nuanced role of human behavior in cybersecurity. The process also enhanced my

research, synthesis, and academic writing skills, equipping me with both theoretical insights and practical competencies that I will carry forward into future work in cloud security.

The insights gained and conclusions drawn through this analysis are expected to guide both future research and real-world practices for securing cloud environments against social engineering threats.

# Bibliography

Alrawais, A., Alhothaily, A., Hu, C. and Cheng, X., 2017. Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 21(2), pp.34-42.

Ammann, P., Wijesekera, D., Kaushik, S. (2002). Scalable, graph-based network vulnerability analysis. Proceedings of the 9th ACM conference on Computer and Communications Security.

Ana-Maria, D. & Sabina-Daniela, A. (2022). Security enhancements for cloud applications. Proceedings of the International Conference on Cybersecurity and Cybercrime, 9(38), 35-40.

Anshul, K., Mansi, C. & Nagresh, K. (2015). Social engineering threats and awareness: a survey. European Journal of Advances in Engineering and Technology, 9(11), 15-19.

Bautista, C. (2014) Apple denies icloud, find my iphone security breach: Only 'very targeted attacks', Tech Times. Available at: http://www.techtimes.com/articles/14717/20140907/apple-deniesicloud-find-my-iphone-security-breach-only-very-targetedattacks.htm

Cisco. (2020). Social Engineering. Retrieved from https://www.cisco.com/c/en/us/products/security/social-engineering.html

Cloud Security Alliance. (2016). Security Guidance for Critical Areas of Focus in Cloud Computing V3.0. Retrieved from https://cloudsecurityalliance.org/research/guidance/

Cloud Security Alliance. (2017). Security Guidance for Critical Areas of Focus in Cloud Computing V4.0.

Cloud Security Alliance. (2017). Top Threats to Cloud Computing: Egregious Eleven. Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/top-threats/TOP_THREATS_EGREGIOUS11.pdf

D. I. George, A. & S. Edel-Josephine, R. (2019). A survey on security challenges in cloud computing. Journal of Physical Sciences, 24(15), 133-141.

Fatima, S. & Naima, K. (2019). Social engineering attacks: a survey. Future Internet, 11(4). https://doi.org/10.3390/fi11040089

Federal Communications Commission. (2021). Robocalls. Retrieved from https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts

Federal Trade Commission. (2021). Phone Scams. Retrieved from https://www.consumer.ftc.gov/articles/0208-phone-scams

Gartner. (2020). Understand the Cloud Service-Level Agreement.

Gartner. (2021). Gartner Says Worldwide Public Cloud Service Market to Grow 23.1% in 2021. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2021-04-26-gartner-says-worldwide-public-cloud-service-market-to-grow-23-point-1-percent-in-2021

Gartner. (2021). The Five Most Common Cloud Security Threats. https://www.gartner.com/smarterwithgartner/the-5-most-common-cloud-security-threats/

Goyal, S. (2014). Public vs private vs hybrid vs community-cloud computing: A critical review. International Journal of Computer Network and Information Security, pp. 20–29. doi: 10.5815/ijcnis.2014.03.03

Gupta, B. B., Tewari, A., Jain, A. K. & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. Neural Computing and Applications, 28, 3629-3654. https://doi.org/10.1007/s00521-016-2275-y

Heartfield, R. and Loukas, G., 2016. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys (CSUR), 48(3), pp.1-39.

Huth, A., & Cebula, J. (2011). The Basics of Cloud Computing. US-CERT.

Jain, Preeti. (2012) "Reverse Social Engineering and its impact on Organization's Digital Data.", International Research journal of Management Science and Technology, Vol. 3, No.1, pp. 2250 - 1959 (ISSN)

Jang-Jaccard, J. and Nepal, S., 2014. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), pp.973-993.

Khatri, S., Cherukuri, A. K., & Kamalov, F. (2023). Global Pandemics Influence on Cyber Security and Cyber Crimes. Retrieved from https://arxiv.org/abs/2302.12462

KnowBe4. (2021). Simulated Phishing Attacks. Retrieved from https://www.knowbe4.com/phishing-simulator

Lee, M., Lee, S., Kim, S., & Kim, D. (2017). A survey on cloud security risk management. Journal of Internet Technology, 18(4), 777-786.

McGraw, G. (2006). Software security: Building security in. Addison-Wesley Professional.

McAfee. (2021). Social Engineering: What It Is, Why It Works, and How to Defend Against It. Retrieved from https://www.mcafee.com/blogs/consumer/social-engineering-what-it-is-why-it-works-and-how-to-defend-against-it/

Mell, P., Grance, T., & The National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145.

Mitnick, K. and Simon, W., 2002. The art of deception: Controlling the human element of security. Wiley Publishing.

Monjur Ahmed & Alan T. Litchfield (2018). Taxonomy for identification of security issues in cloud computing environments. Journal of Computer Information Systems, 58(1), 79-88. https://doi.org/10.1080/08874417.2016.1192520

National Cyber Security Centre. (2021). Password Guidance: Simplifying Your Approach. Retrieved from https://www.ncsc.gov.uk/collection/passwords

National Institute of Standards and Technology. (2011). The NIST Definition of Cloud Computing (Special Publication 800-145). Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

National Institute of Standards and Technology (NIST). (2018). Special Publication 800-146: Cloud Computing Synopsis and Recommendations. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-146/final

National Institute of Standards and Technology. (2017). Data Encryption Standard (DES). Retrieved from https://csrc.nist.gov/publications/detail/fips/46-3/final

National Institute of Standards and Technology. (2017). Multi-Factor Authentication. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-63/3/final

National Institute of Standards and Technology. (2018). Guidelines for Managing the Security of Information Systems. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Noor, O., Derar, E. & Amna, E. (2021). A survey of social engineering attacks: detection and prevention tools. Journal of Theoretical and Applied Information Technology, 99(18), 1817-3195.

Power, R., 2016. 2016 CSI/FBI Computer Crime and Security Survey. Computer Security Institute.

Rafat Ara, Md. Abdur Rahim, Sujit Roy, Dr. Uzzal Kumar Prodhan (2020) 'Cloud Computing: Architecture, Services, Deployment Models, Storage, Benefits and Challenges', International Journal of Trend in Scientific Research and Development, ISSN: 2456- 6470, Vol. 4, No. 4, pp.837-842.

Reason, J. (2016). Managing the risks of organizational accidents. Routledge.

Reza, A. & Shareeful, i. (2015). Human factors of social engineering attacks (SEAs) in hybrid cloud environment: threats and risks. Global Security, 534, 50-56.

Rosado, A., Rosado, D.G., Fernández-Medina, E., Piattini, M. (2012). Security analysis in the migration to cloud environments. Future Generation Computer Systems.

Røisland, P.B. (2019). Balancing product development and external contributions to open source projects: the case for open source project leadership. Journal of Systems and Software

Salahdine, F. and Kaabouch, N. (2019) Social Engineering Attacks: A Survey. Future Internet, 11, 89. https://doi.org/10.3390/fi11040089

Saleem, J. & Hammoudeh, M. (2018). Defense methods against social engineering attacks. In Computer and Network Security Essentials (pp. 603-618). Springer, Cham. https://doi.org/10.1007/978-3-319-58424-9_35

SANS Institute. (2020). Cloud Security Fundamentals. Retrieved from https://www.sans.org/white-papers/41186/

SANS Institute. (2020). Social Engineering. Retrieved from https://www.sans.org/security-awareness-training/resources/social-engineering

SANS Institute. (2021). Phishing: A Guide to Common Threats and Prevention. https://www.sans.org/security-awareness-training/resources/phishing/

Sharma, S., Shrivastava, A., & Nigam, S. (2019). User and Entity Behavior Analytics Using Machine Learning: A Review. Procedia Computer Science, 165, 502-509. doi: 10.1016/j.procs.2019.12.149

Srinivasan, A., Quadir, M.A. and Vijayakumar, V. (2015). Era of cloud computing: A new insight to hybrid cloud. Procedia Computer Science, 50, 42–51. https://doi.org/10.1016/j.procs.2015.04.059

Suryateja, Pericherla. (2018). Threats and vulnerabilities of cloud computing: a review. International Journal of Computer Sciences and Engineering, 6(3). DOI:10.26438/ijcse/v6i3.298303

Symantec. (2020). Ransomware. Retrieved from https://www.symantec.com/security-center/threat-report?tid=71181

Symantec. (2021). Security Awareness and Training. Retrieved from https://www.symantec.com/security-awareness/security-awareness-training

US-CERT. (2016). Access Control. Retrieved from https://us-cert.cisa.gov/bsi/articles/best-practices/access-control

US-CERT. (2016). Network Segmentation. Retrieved from https://us-cert.cisa.gov/bsi/articles/best-practices/network-segmentation

US-CERT. (2020). Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks. Retrieved from https://us-cert.cisa.gov/ncas/tips/ST04-014

Verizon. (2023). 2023 Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/2023/

Wang, S., Qin, X., & Gong, Y. (2017). Social engineering attacks and countermeasures in cloud computing. International Journal of Information Management, 37(1), 121-129. doi: 10.1016/j.ijinfomgt.2016.09.007

Zissis, D. and Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006.