Mohammad Ali

INFORMATION SECURITY THREATS IN CLOUD SERVICES
A COMPREHENSIVE OVERVIEW

Bachelor's thesis

Degree Bachelor of Engineering

Information Technology

2025

South-Eastern Finland
University of Applied Sciences

Degree title	Bachelor of Engineering
Author	Mohammad Ali
Thesis title	Information security threats in cloud services: a comprehensive overview
Year	2025
Pages	47 pages
Supervisor	Matti Juutilainen

ABSTRACT

Cloud computing has completely changed how individuals, companies, and organizations manage, store, and analyse data, enabling open and affordable solutions. However, switching to cloud services has resulted in major issues with information security.

Cloud security challenges include data breaches, software attacks, DoS attacks, and insider threats, while complex cloud settings can make data monitoring and management difficult for organizations. Cloud settings are prone to risks because they use shared technology, have multiple tenants, and depend on third-party sources. These factors can lead to data breaches, prohibited entry, and other security difficulties.

This study comprehensively examines the main security challenges that come with cloud settings, including data breaches, account theft, and APIs that may not be secure. Additionally, cloud platforms are extremely fascinating to hackers because they easily access and store data in one place.

This study combined insights from the previous study and a case study analysis from a practical perspective. It examined a real-life case to show how security issues in cloud services affect daily lives. This study provides security practitioners, IT professionals, and organizations with an understanding of the dynamic cloud threat environment and practical risk-reduction techniques. Organizations may fully use cloud computing while preserving a safe and reliable digital environment by coordinating cloud infrastructure and procedures with strong security standards.

Keywords: cloud security, cloud computing, cloud security challenges, insider threats, data privacy

Table of Contents

1 INTRODUCTION

The origin of cloud computing is the computer networking system dating back to 1960. John McCarthy, a pioneer of artificial intelligence, articulated his idea through network-based computers and said that information technology may eventually be structured as a service for everyone.

He imagined that multiple users would have simultaneous access to a central computing system and be able to share their work and activities (McCarthy 1961, 220-221).

Subsequently, this concept developed the foundation of cloud computing. Virtualization technologies developed in 1990 significantly influenced the evolution of cloud computing. An individual physical machine operates multiple operating systems and functions, creating better use of server resources. This technology was spread by corporations such as VMware, which facilitated the transformation of data centers into more cost-effective and dynamic environments. (VMware 2020.)

The contemporary idea of cloud computing, with the introduction of large internet platforms and development, required scalable infrastructure in the early 2000s (TechTarget 2025).

In 2006, Amazon introduced the Elastic Compute Cloud (EC2), the first commercial cloud. In 2008, Google was strongly followed by Amazon’s EC2 model and introduced a basic pricing model with a free-entry-level plan and low-cost computing and storage services. (AWS 2006.)

Microsoft, a software giant, launched Azure in the cloud market in 2010. This platform enables the quick expansion of mobile and web applications, by this means accelerating the growth of the mobile industry. (Microsoft Azure 2021.)

Currently, the cloud is the foundation of new emerging technology, such as composable business. It has provided resiliency, scalability, flexibility, and speed during periods of uncertainty. Multi-cloud, edge, and hybrid environments are

expanding, establishing the foundation for novel delivered cloud models. (TechTarget 2025.)

The key objective of this study will be to acknowledge ordinary weaknesses, measure the effectiveness of present mitigation approaches, and observe the improvement of advanced solutions to increase the security of the cloud environment. In order to enhance the reliability and security of cloud systems, this study intends to provide a thorough understanding of their progress.

2 INSIGHTS OF PREVIOUS STUDIES

Cloud computing performs a key role in contemporary information technology infrastructure, enabling scalable and easier services to people and organizations. However, the prompt adoption of cloud computing has renovated the information technology scenario, allowing companies to access scalable resources and decrease operational costs. This change poses numerous security challenges in information technology, which may compromise the data integrity, confidentiality, and availability of data stored in cloud environments. These insights section introduces the current studies on security challenges in cloud services, the classification of these challenges, and assesses their effects on businesses. The following observations emerged from previous study results.

Data breaches and privacy concerns

Data breaches are a significant threat in cloud computing because of the amount of stored data and potential misconfiguration. According to the Cloud Security Alliance (CSA), 90% of companies have suffered at least one misconfiguration-related breach in cloud computing (CSA 2023). The password compromise is a key factor in cloud data breaches (IBM Security 2022).

Insecure APIs and interfaces

The cloud service profoundly depends on the API for management and integration. However, when APIs are misconfigured and designs are not adequate, systems will be vulnerable to attacks (OWASP 2022).

Distributed denial of service (DDoS) attacks

DDoS attacks may cause cloud service availability issues by overloading resources with malicious traffic. Cloudflare claims that cloud systems are especially vulnerable to volumetric DDoS attacks, with bandwidth often topping terabytes per second (Cloudflare 2023).

In order to tackle this issue, public cloud providers such as AWS, Azure, and Google Cloud increasingly provide DDoS protection services such as traffic filtering and automated scaling (AWS Shield 2025).

Multi-tenancy vulnerabilities

Attackers can compromise “tenants” in multi-tenant cloud environments by exploiting resource-sharing mechanisms. In 2023, ENISA published a study that examines side-channel attacks in shared virtualized environments. The study demonstrates that attackers can infer sensitive data from nearby virtual machines. The adoption of hardware-based isolation techniques, such as Intel's SGX, is on the rise as a means of reducing multi-tenancy risks (Intel n.d).

Insider threats

Insider threats define the specific errors in the cloud system regardless of whether the consequences are due to incompetence or malicious intent. A study by Microsoft (2024) highlights that privilege misuse is one of the key reasons for insider threats. In order to decrease insider threats, non-stop monitoring, user behaviour analysis, and reduction of privileged access are suggested.

Misconfigurations and lack of compliance

The most common vulnerabilities in cloud computing are misconfigurations. This issue frequently occurs in breaches, data leaks, and noncompliance with regulations. According to the Gartner report from 2022, approximately 99% of cloud security issues until 2025 are due to customer responsibility for incorrect settings and poor control. There are several ways to avoid misconfiguration. For instance, using automatic configuration management tools such as Terraform and Pulumi. Additionally, real-time monitoring tools such as Azure policy assist to

enforce organizational policies and reduce non-compliance risk (Azure Policy Documentation).

Regulatory compliance and governance

When deploying a cloud service, it is required to comply with data protection laws, including GDPR, HIPAA, and CCPA. Achieving compliance can be challenging in a globally distributed cloud environment, so technologies such as AWS Config and Azure policy are recommended. (Microsoft Azure: Azure Policy 2025)

In summary, data breaches, misconfigured cloud resources, insecure APIs, DDoS attacks, and insider threats are the most significant risks that may expose sensitive data and destroy critical operations. Research organizations such as Cloud Security Alliance and Gartner have stated that 99% of cloud security issues result from human errors, such as misconfiguration and poor governance policies (Gartner 2022). The key features of the cloud environment, such as shared infrastructure and multi-tenancy, make vulnerabilities more likely, creating a complicated incident surface that is difficult to defend. Encryption, multi-factor authentication, and compliance tools are effective in avoiding threats, and the increase in attacks compels additional innovative and strong security measures. These security issues present a significant risk to organizations, administrations, and individual users that depend on cloud services for data storage, application hosting, and essential management.

3 CLASSIFICATION OF SECURITY ATTACKS AT VARIOUS LEVELS IN CLOUD

Cloud services come with several security challenges as they continue to provide new features and have increasing influence in the industries. Some risks are caused by the nature of cloud computing which involves the use of tools and services offered over the internet and stored on a shared server. The existing security challenges at several service levels, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), lead to multiple security issues, with potential attack directions present at each level. The following is a detailed description of the security challenges commonly linked to each cloud service model.

3.1 Infrastructure-level attacks

Attacks on the infrastructure level are fundamentally target at vulnerable hardware and virtual components. These attacks take advantage of vulnerabilities in multi-tenant architectures, hypervisors, and cloud data centers (Cloudflare 2023).

3.1.1 Denial of service (DoS) and distributed denial of service (DDoS) attacks

A Denial of Service (DoS) attack is a malicious attempt to disrupt the availability of a targeted system, such as a website or application, for legitimate end users. Usually, attackers create a significant number of packets or queries that eventually overwhelm the target system. DoS attacks commonly occur in two ways: buffer overflow attacks and flood attacks. (Cloudflare 2023.)

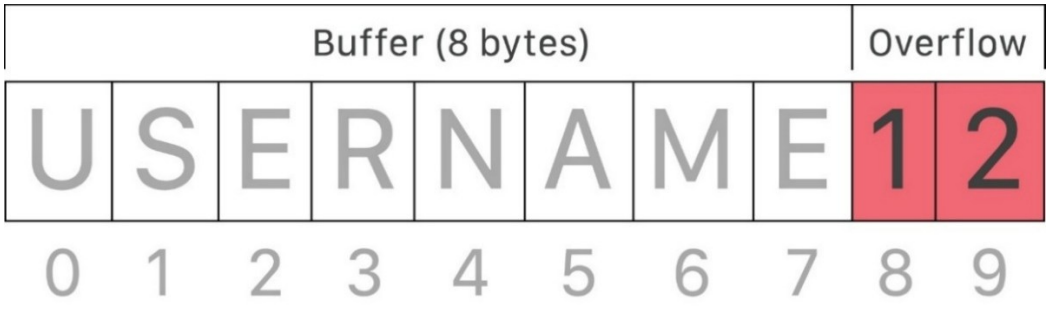

Figure 1. Buffer overflow (Cloudflare)

In a buffer overflow attack, a memory buffer overflow may be created in a device's hard disk space, memory, or CPU time. This type of attack regularly leads to denial-of-service which is characterized by inactive behavior, system failures, or other dangerous server behavior. (Cloudflare 2023.)

DoS flood attacks are defined as being able to overwhelm a target by exploiting a variety of network protocols and weaknesses in the system. An HTTP flood attack is designed to overwhelm a targeted server with HTTP requests. Once the target has been saturated with requests and is unable to respond to normal traffic, a denial-of-service will occur for additional requests from actual users .(Cloudflare 2023.)

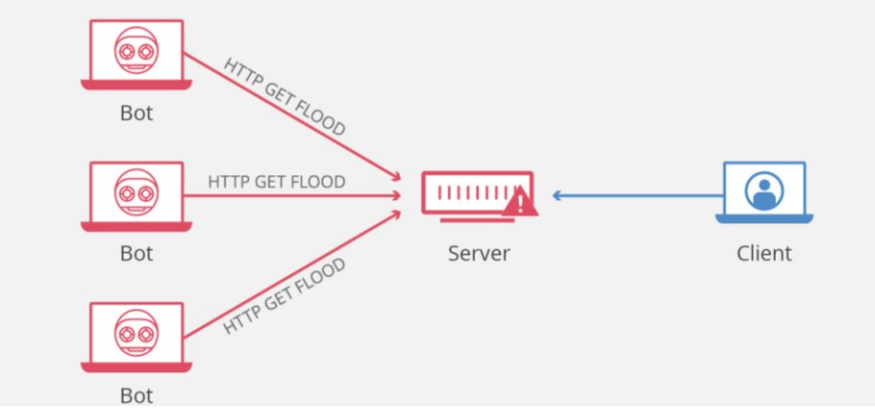

Figure 2. HTTP Flood attack (Cloudflare)

A UDP flood occurs when an immense quantity of UDP packets is sent to random ports, thereby diminishing the system's resources (Cloudflare 2023).

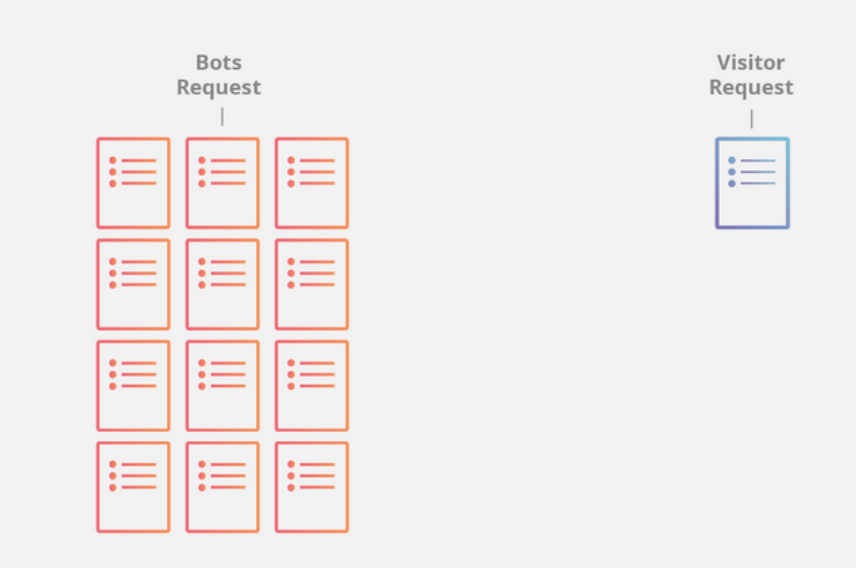

Figure 3. UDP Flood attack (Cloudflare)

TCP SYN flood attack exploits the handshake procedure by sending numerous SYN requests without finishing connections, resulting in server overload (Cloudflare 2023).

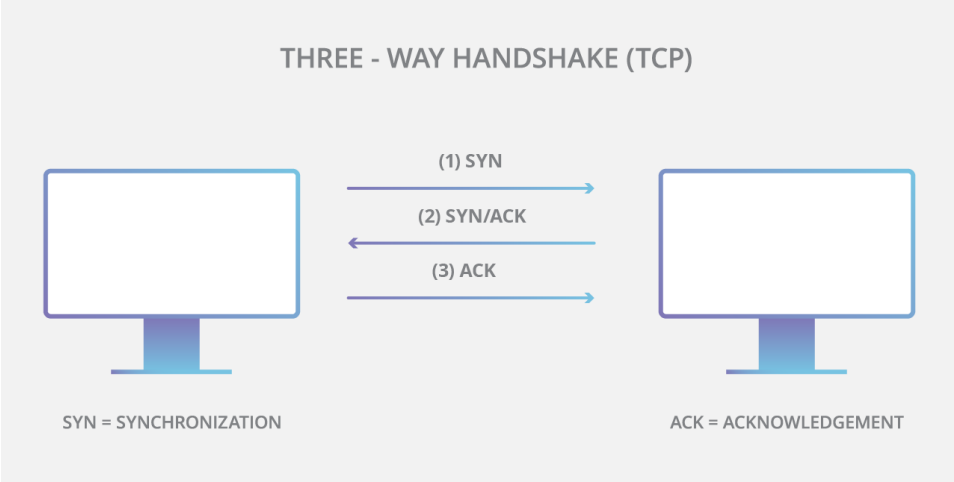

Figure 4: TCP SYN Flood attack (Cloudflare)

ICMP (ping) flood attacks overwhelm network bandwidth by attacking a system with excessive ICMP echo requests. By transmitting excessive GET or POST queries, HTTP flood attacks imitate legitimate user behaviours and affect web servers.

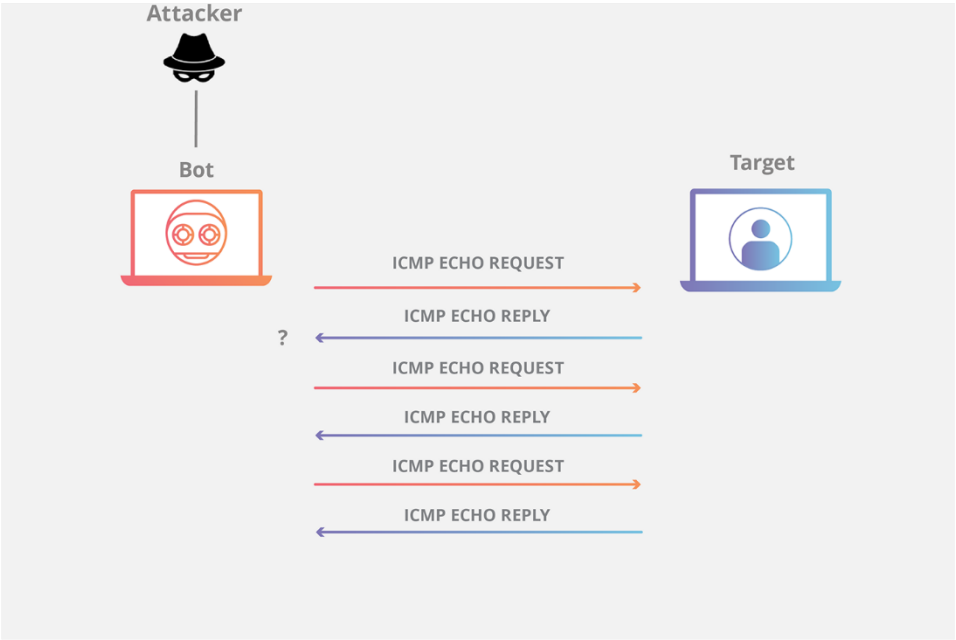

Figure 5. ICMP (ping) Flood attack (Cloudflare)

A smurf attack is a kind of distributed denial-of-service (DDoS) attack that overwhelms networks by using Internet Protocol (IP) broadcast addresses. The impact of smurf attacks is exacerbated by the flood of response messages that are triggered by ICMP requests. DNS flood attacks disrupt name resolution services by bombarding the domain name system (DNS) servers with an excessive number of queries. In the context of a Distributed Denial of Service (DDoS) attack, the attacker implements multiple hacked or manipulated sources to create the attack, while DoS attacks come from a single source. (Cloudflare 2023.)

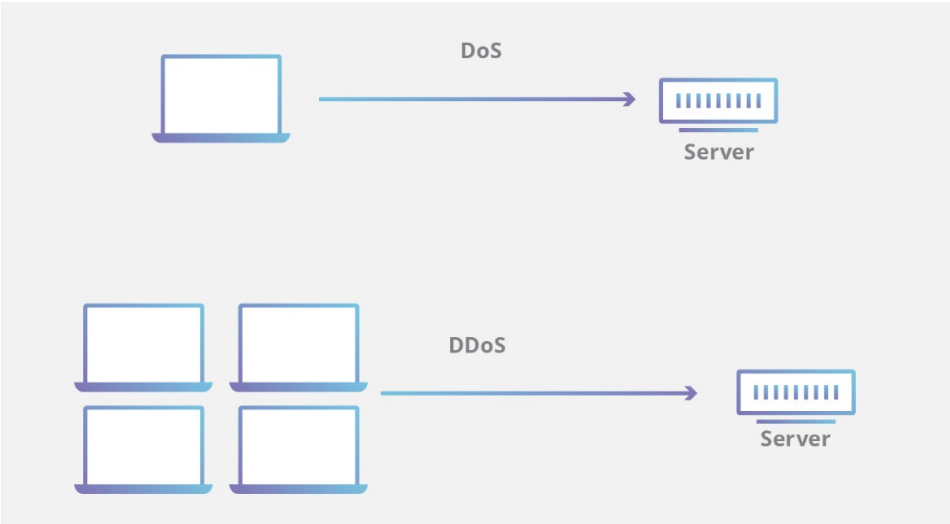

Figure 6. DoS Vs DDoS attack (Cloudflare)

Cloud servers become overwhelmed with a large quantity of traffic because of DoS and DDoS attacks which disrupt services. Cloudflare has reported that DDoS attacks increased by 60% in 2022, with a focus on cloud-hosted applications and infrastructure. (Cloudflare 2023.)

3.1.2 Side-channel attacks

These attacks separate sensitive data by exploiting shared physical resources in multi-tenant environments. These attacks can reveal the most recent activities of a legitimate user by exploiting resource sharing, such as cache memory. Side-channel attacks can be executed effectively using various techniques and factors. Consequently, multi-tenancy remains a risk factor in cloud computing, despite the numerous benefits it provides. If not sufficiently prevented, this security risk could become the primary fear that hampers the cloud system. (IEEE Xplore 2022.)

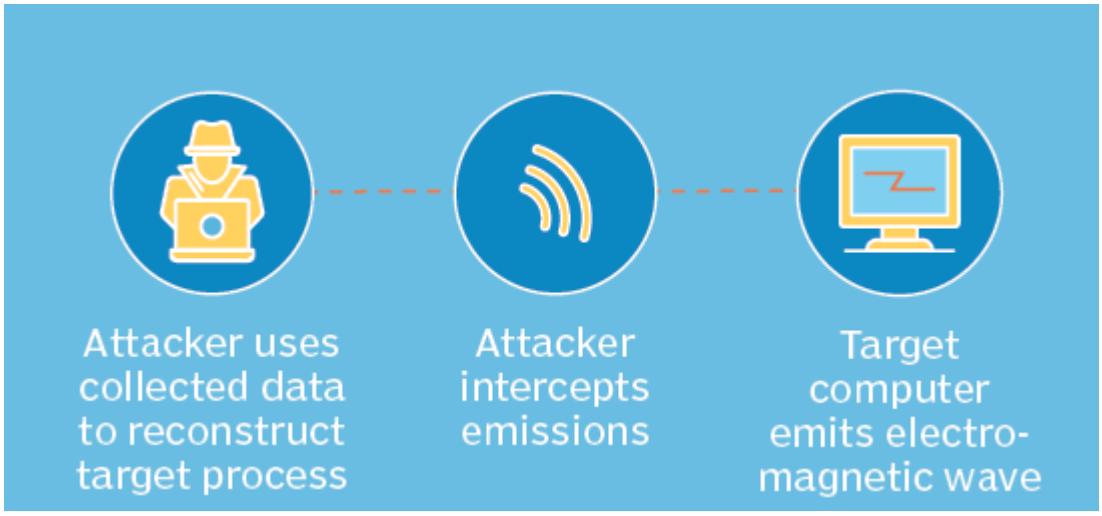

Figure 7. How a side-channel attack works (TechTarget)

There are different types of side-channel attacks, such as electromagnetic, acoustic, power, optical, timing, and memory cache attacks.
An electromagnetic (EM) attack exploits electromagnetic radiation emitted by electronic components, such as CPUs or cryptographic chips. These emissions can be captured and analyzed to extract sensitive data. Attackers use specialized antennas and sensors to capture electromagnetic signals. Analyzing the signal techniques helps reconstruct secret information. (TechTarget 2021.)

Acoustic cryptanalysis exploits sound emissions from computer components, such as keystrokes, CPU operations, or hard disk movements. These sounds are recorded and analyzed to extract confidential information. Attackers use highly sensitive microphones to capture sound signals, and the machine learning algorithms or frequency analysis techniques extract patterns. (IEEE Xplore 2022.)

Power analysis attacks exploit power consumption variations of a device while performing cryptographic operations to extract sensitive data. Attackers measure power consumption while a system processes encrypted data. Small variations in power usage reveal cryptographic key patterns. Attackers analyse the power consumption and attacks twice ways: either directly analyze power traces to extract data or use statistical techniques to correlate power variations with encryption keys. (TechTarget 2021.)

Optical attacks analyze light emissions from electronic components, such as LEDs, to infer internal processing states and extract secret information. Attackers use high-speed cameras or optical sensors to monitor light variations, and LED signals leaking CPU activity or encryption processes can be decoded. (TechTarget 2021.)

Timing attacks analyze how long a system requires to perform specific operations to infer sensitive data. Cryptographic algorithms often process different inputs in varying amounts of time, allowing attackers to extract key information. Attackers measure execution time for encryption processes, and variations in timing reveal patterns in cryptographic key calculations. (TechTarget 2021.)

Cache-based side-channel attacks exploit CPU cache behavior, such as memory access patterns, to infer secret information. Since processors store frequently accessed data in the cache, attackers can measure cache hit or miss timing to recover sensitive data. They execute code on the same system, such as a shared cloud server, and analyse cache access times to detect data usage patterns. (TechTarget 2021.)

3.1.3 Hypervisor attacks

A software layer known as a hypervisor is responsible for the deployment and management of virtual machines (VMs), which is the foundation of virtualization. It serves as a bridge between the physical hardware and the virtualized environment. Each virtual machine (VM) may operate independently of the others due to the hypervisor's provision of a virtual environment and the separation of the main physical hardware. This boosts resource performance and reduces expenditures for both the cloud provider and the end user by allowing a variety of virtual machines (VMs) to share actual resources, including CPU, memory, and storage. Hypervisor incidents may result in calamitous consequences for the organization when an adversary targets the virtualization layer of the system. (Cyber Insight 2023.)

Attacks at the hypervisor level present significant security threats, as hypervisors are indispensable for the administration of virtual environments. These attacks are particularly harmful in cloud computing and data centers due to the fact that hypervisors facilitate server virtualization which allows for the operation of numerous virtual machines (VMs) on a single physical server. By concentrating on the hypervisor, attackers may be able to seize control of all hosted virtual machines (VMs), potentially leading to data breaches, service disruptions, and compromised system integrity. (Cyber Insight 2023.)

Based on their architecture and vulnerability to attacks, hypervisors are divided into two categories. Type 1 hypervisors are referred to as bare-metal hypervisors; they operate directly on the host's hardware, managing guest operating systems and controlling them. Common examples of these comprise VMware ESXi, Microsoft Hyper-V, and Xen. Type 1 hypervisors are highly efficient due to their direct access to actual hardware. However, they require robust security measures to avert potential attacks. (ITU 2024.)

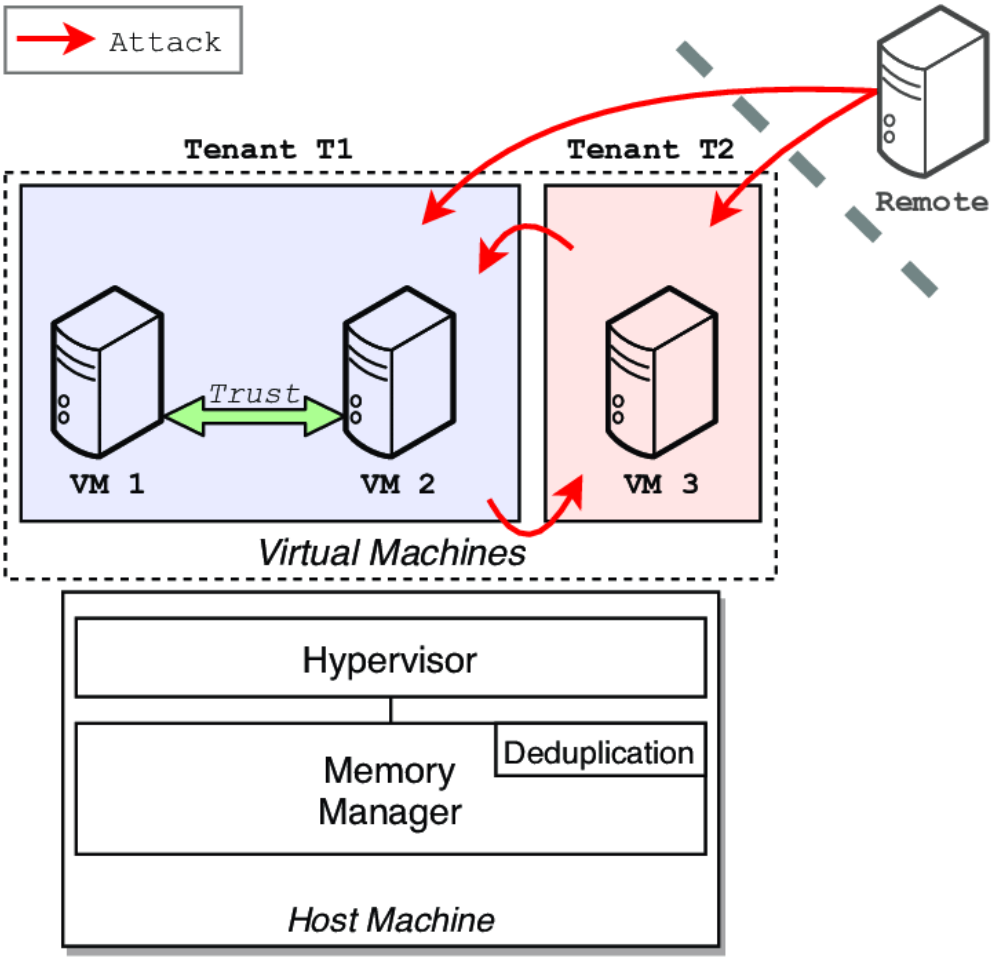

Figure 8. A hypervisor running three virtual machines. (Researchgate)

The figure (8) illustrates a hypervisor running three VMs, where two of them (VM-1 and VM-2) belong to one tenant (T1), while the third one (VM-3) belongs to another tenant (T2). Attacks from remote machines. (Researchgate 2017.)

Type 2 hypervisors operate on a standard operating system, similar to other computer applications. Oracle VirtualBox and VMware Workstation are two examples of this type. Type 2 hypervisors are simpler to operate than Type 1 hypervisors. However, they are considered less secure due to the possibility of a compromise in the event of a host operating system attack.
Attacks at the hypervisor level may use several strategies, such as arbitrary code, increased privileges, or the utilization of security measures by taking advantage of known security holes in the hypervisor software. By escaping the virtual machine, an attacker may be able to take control of the whole virtualized environment and acquire access to the host hypervisor or additional virtual

machines. The act of installing malware or a rogue hypervisor at the hypervisor level to gain total control of the host system is known as "hyperjacking." When too many requests or actions overwhelm the hypervisor, it exhausts its resources and causes service degradation or even shutdown. (ITU 2024.)

3.2 Network-level attacks

The network-level attacks aim to exploit vulnerabilities in the cloud network, interrupt data transmission, or network configuration. The key attack is Man-in-the-Middle (MITM) at the network level. The following is an in-depth discourse on this issue.

Man-in-the-Middle (MITM)

In a man-in-the-middle attack, an attacker may access the data between the user and the cloud. Such an attack occurs when a hacker silently captures and perhaps manipulates the network between two groups who trust they are communicating directly. The attacker may compromise data, disrupt networks, stalk users, or steal sensitive information. Interception and decryption are the two individual stages of successful MITM execution. (IBM 2024.)

Interception

The first step of an interception attack involves intercepting user traffic passing via the attacker's network before it reaches the target. The most popular and straightforward method for doing this is via passive assaults. In these incidents, attackers provide free but malicious WiFi connections to the public. These connections usually have names that reflect their locality and are not password-protected. Immediately after a victim connects to a hotspot, the attacker has full insight into any online data exchange. (IMPERVA 2025.)

Attackers who desire to implement a more proactive approach to interception may initiate the subsequent incidents. The act of a malicious entity impersonating an application by changing the packet information in an IP address is known as IP hijacking. (IMPERVA 2025.)

IP hijacking refers to the illegitimate appropriation of an IP address for malicious objectives, including executing cyber attacks, stealing confidential information, or impersonating a genuine user or device inside a network. (LARK 2024.) Consequently, users are diverted to the attacker's website when they try to visit a URL linked to the program (IMPERVA 2025).

ARP spoofing is the practice of using fictitious ARP packets to link an attacker's MAC address to a genuine user's IP address on a local area network. The data that the user intended to send to the host IP address is, therefore, obtained by the criminal. (IMPERVA 2025.)

The technique of changing a website's address record by breaching a DNS server is called DNS spoofing, or DNS cache poisoning. Consequently, visitors who try to access the website are redirected to the attacker's website via the altered DNS record. (IMPERVA 2025.)

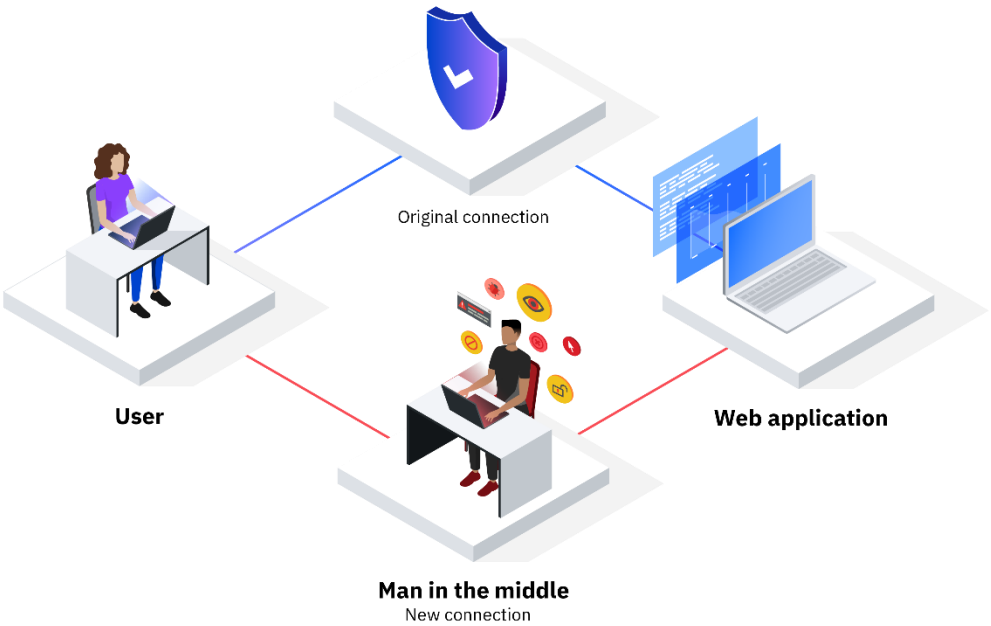

Figure 9. Man-in-the-middle attack (IBM)

Decryption

Any two-way SSL communication that is found must be decrypted without informing the user or program. Several matters can be done to make this occur.

When someone tries to connect to a safe site for the first time, an HTTPS deceit can be used to send a fake certificate to their computer. In order to make sure that the digital fingerprint of a compromised app is genuine, the browser checks it against a list of known safe websites. As a consequence of this, the attacker may look at any information the target sends before it is sent to the application. (IMPERVA 2025.)

SSL BEAST is a computer attack on SSL/TLS. The SSL BEAST which takes advantage of an error in SSL version 1.0 by installing a harmful JavaScript on the victim's computer to intercept private cookies sent by a web application. Subsequently, a hacker is able to break into the app's cipher block chaining (CBC) which allows them to decrypt its login keys and cookies.

SSL theft occurs during a TCP handshake when an attacker sends fake authentication keys to both the user and the program. This results in an apparently safe link, but it effectively provides the person in the middle with a full power over the session. SSL stripping is a means to steal the TLS authentication that the app sends to the user, thus reducing turns an HTTPS link into an HTTP link. The attacker provides the user a version of the app's website that is not secure while in a safe session on the app. Consequently, the attacker is aware of the user’s complete procedure. (IMPERVA 2025.)

3.3 Application-level attacks

Application layer attacks are initiatives to obtain unauthorized access to an organization's cloud-hosted systems by exploiting software vulnerabilities.

3.3.1 Injection attacks

When hackers take advantage of injection errors, they can use user data that has not been observed to add harmful parts to the application code. This is called an injection attack. According to OWASP, these attacks are among the worst threats to application security, ranked as the third most dangerous threat to web apps generally (THE ACUNETIX 2025).

There are different injection attacks, but they all have one thing in common: the attacker changes the way the application manages data, which may entail changing database queries, or running JavaScript, system commands, or even native application code. This attack can lead to consequences ranging from small data leaks to significant security breaches, such as denial of service (DoS), bypassing identification, gaining more privileges, running code remotely (RCE), or compromising the whole system. (THE ACUNETIX 2025.)

In injection attacks, malicious code is inserted into a program, causing illegal command execution or data access. Injection attacks come in a variety of forms, and below are the primary types.

SQL Injection: Affects data integrity and availability by exploiting database vulnerabilities through malicious SQL statements.

Command Injection: Executes of unknown commands on the host operating system, which has the possibility to gain access to the system.

XML Injection: Manipulates the processing of XML data or documents to harm XML applications.

Here is figure 10 illustrates an example of a SQL injection attack . A registration form for a web application that validates user credentials by querying a database. The web form contains two input sections: `USERNAME` and `PASSWORD`.

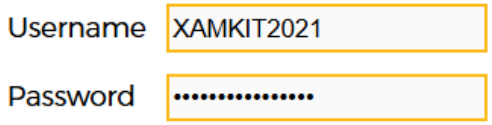

Figure 10. Example of SQL Injection attack (a Screenshot of the logging page of the learn page)

In this example, it is reasonable to anticipate that the server-side script will verify the credentials using a SQL query similar to the following:

```
SELECT *<p>FROM users</p>WHERE
username='${request.body.username}' AND</p>
<p>passworrd='${request.body.password}'</p>
```

The script would substitute the specified value for `request.body.username` with `XAMKIT2021` and the value for `request.body.password` with the provided password.

If the username and password combination do not match an existing record as below in the `USERS` table, the query will fail to retrieve any rows.

```
SELECT *<p>FROM users</p>WHERE
username='XAMKIT2021' AND</p>
<p>passworrd='2Study#0with@2fuN1!'</p>
```

Nevertheless, if the web form inputs are not cleansed, it is important to consider the potential consequences if the end user submits a form with these values. rather than:

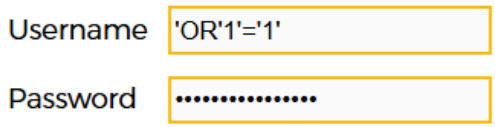

Figure 11. Example of SQL Injection attack

Figure 11 illustrates that the values for username and password are the same as unclear.

This is the SQL query that would be generated if the inputs were not purified:

```
SELECT *<p>FROM users</p>WHERE username=''
OR '1'= '1' AND</p><p>password='' OR '1' ='1'</p>
```

This query would return every row from the `users` table, therefore enabling the malicious attacker to log in as the first user returned.

At a primary phase, attackers may implement straightforward strategies, such as SQL injection which involves exploiting unsanitized input fields. Nevertheless, attackers may also develop sophisticated tools to automate vulnerability discovery and implement intricate injection attacks in order to circumvent stronger defences. More recently, attackers have started employing AI-powered tools to identify effective attack vectors, adapt to protocols, and analyse security patterns. The weapons race between cybersecurity measures and attackers' tactics is intensifying as attack techniques become more efficient and rapid. This highlights the necessity of ongoing updates and attentive security practices. (CROWDSTRIKE 2024.)

Injection attacks have the potential of consequences. Attackers can gain control of sensitive data, including personal information, financial records, and proprietary business data, by effectively exploiting vulnerabilities. This illegitimate access to sensitive data not only undermines trust but also presents a direct threat to individuals and organizations. The compromised data can be exploited through criminal, controlled targeted sites distributed on the dark web, or utilized for further data breaches.

In addition to data breaches, an injection attack can result in a system outage by corrupting or overwhelming the operations of the targeted system. The repercussions of service disruptions can be extensive as they necessitate time-consuming data restoration efforts and operations, and occasionally lead to disruptions in business activities. The consequences include potential long-term reputational harm, reduced consumer satisfaction, and financial losses. (CROWDSTRIKE 2024.)

3.3.2 Cross-site scripting (XSS)

In cross-site scripting (XSS) attacks, malicious scripts are put into websites that are supposed to be safe and secure. In other words, an individual uses a web app to send harmful code, usually as a browser-side script. Quite a few web applications have bugs that facilitate these hacks which may occur whenever the

app uses user input in its output without verifying it or encoding it. XSS allows an attacker to send a harmful script to an unsuspecting user, and there is no way for the user's computer to know that the script is unsafe; it will run the script. Because the computer assumes the script came from a reliable source, it obtains access malicious script can get to cookies, session tokens, and other private data the browser stores for that site. In this way, the hacker can even change the content of an HTML page. (OWASP 2025.)

The following script shows how cross-site scripting (XSS) operates.

```
<script>
i=new/**/Image();isrc=http://evilwebsite.com/log.php?'+document.cookie+' '+document.location
</script>
```

Cross-site-scripting (XSS) can use any client-side language, although the payload is typically JavaScript. Changing a request is another method attackers can employ in this context. If the web application is susceptible to XSS attacks, the user-supplied input is executed as code. For instance, in the request below, the script displays a message box containing the text "xss."

```
http://www.site.com/page.php?var=<script>alert('xss');</script>
```

An XSS attack can be initiated in a variety of ways, and even either upon the page's loading or when a user hovers over specified elements of the page, such as hyperlinks. The possible implications of cross-site scripting attacks include obtaining the user's keystrokes, sending the user to a malicious website, executing web browser-based exploits, or accessing the user's account by collecting the cookie information while they are logged onto a website. In some instances, the victim's account is entirely compromised, and attackers may mislead them into inputting their credentials into a fraudulent form which subsequently discloses all pertinent information to the assailant. (BLACKDUCK 2025)

3.3.3 API attacks

The objective of API attacks is to exploit the application programming interfaces that facilitate communication between a variety of software systems. Such assaults exploit API vulnerabilities to disrupt services, take data, or gain illegitimate access to sensitive data. APIs facilitate communication between applications but they also expose endpoints to potential adversaries. APIs are perceived by attackers as a potential route for system infiltration, inadequate authentication, or authorization circumvention. Their primary goal is to exploit these interfaces in order to achieve malicious objectives. (Palo Alto 2025.)

The transmission of malicious code or queries by attackers to control servers is a common technique in API attacks. This is known as injection, but SQL injection and cross-site scripting are frequently methods. The absence of updates, weak security practices, and misconfigurations are frequently the causes of API vulnerabilities. These assaults have the potential to have a substantial impact on both enterprises and consumers, leading to data breaches and interruptions. In order to mitigate hazards, organizations must prioritize the protection of their APIs. (CloudTweaks 2024.)

Authentication and authorization bypass attacks arise when attackers use Application Programming Interface (API) errors to acquire unauthorized access to systems. Inadequately implemented authentication procedures or absence of approval checks are prevalent weaknesses exploited in these attacks. This poses considerable security concerns by enabling attackers to impersonate genuine users or access sensitive data without the necessary authorizations. (CloudTweaks 2024.)

Distributed Denial-of-Service (DDoS) attacks against APIs include overflowing the target service with an excessive volume of requests, so incapacitating it for legitimate users. Attackers often use botnets to propagate requests, resulting in significant network traffic. Such mistakes may significantly impact internet

services, leading to financial losses and brand harm. APIs devoid of rate restriction are especially susceptible to DDoS assaults. (CloudTweaks 2024.)

In man-in-the-middle (MitM) attacks, an adversary intercepts API connections to alter or observe data transmission. These assaults exploit susceptible channels, enabling perpetrators to appropriate sensitive information, including secret data and authentication credentials. Man-in-the-Middle attacks offer significant risks to APIs that either lack encryption or use insufficient encryption, compromising the security and integrity of data. (CloudTweaks 2024.)

API abuse and exploitation, which occur when APIs are misused beyond the intended purpose, frequently result in wasted resources or unlawful activity. Attackers may reverse-engineer APIs to implement unauthorized actions, such as manipulating service behaviors or accumulating data. Inadequate access constraints and unmonitored API usage exacerbate these risks. (CloudTweaks 2024.)

Organizations depend on APIs for simplifying their operations, which is why attackers are perpetually on the lookout for API vulnerabilities to exploit (Palo Alto 2025). The simplicity with which threat actors can access valuable data is illustrated in Figure 12.

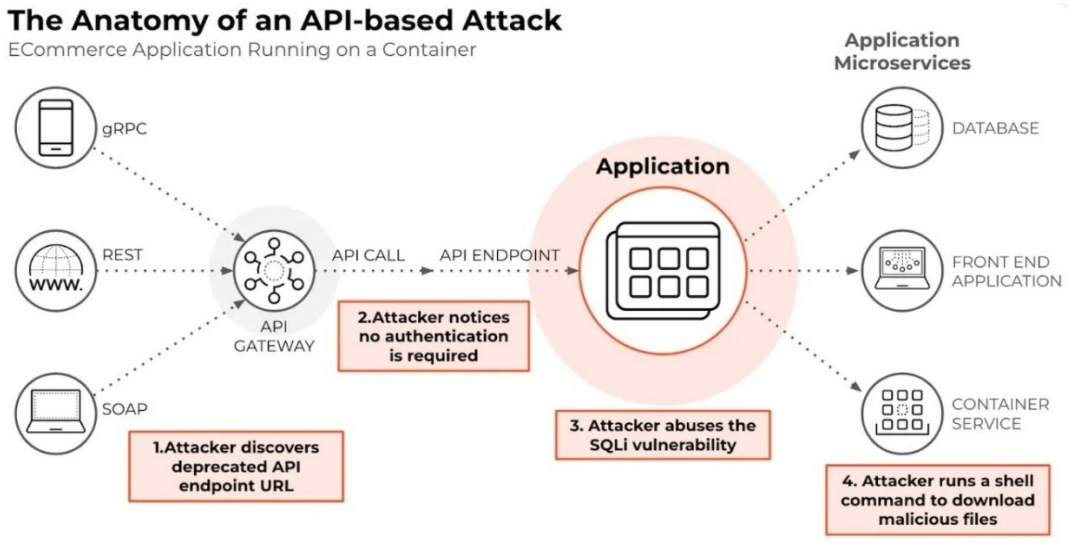

Figure 12. API attack anatomy (Paloalto)

In order to find an expired API endpoint URL that is being used to obtain data from a backend microservice, an attacker reverse-engineers the mobile application and investigates whether sending API queries to this endpoint requires permission or authentication. The attacker aims to exploit the SQLi vulnerability and determine if the input field can be used to successfully carry out a SQLi attack, they run a series of machine-learning tests. A distinct product identification in the form of a numeric identifier is provided by the API endpoint URL. Most likely, the perpetrator prefers to exploit the SQLi vulnerability by initiating a shell command in the microservice that hosts the SQL database, rather than utilizing it for data manipulation. The shell command downloads and executes a malicious executable which contains bitcoin mining software. (Palo Alto 2025.)

3.4 Data-level attacks

In the cloud system, the major objective of attackers is to access the data stored in order to steal, corrupt, or blackmail important information.
The following sections present several data-level attack methodologies utilized by attackers.

3.4.1 Data breaches

A data breach is the unauthorized disclosure of sensitive, confidential, or private information into an unprotected environment. It may happen either accidentally or as a consequence of a targeted attack. Every year, data breaches affect millions of people (IBM 2024). They can be rather insignificant such as a doctor looking at the wrong patient's chart by accident, or very serious such as someone trying to access into government computers to find private information.

Data breaches are a significant security concern due to the continuous transmission of sensitive data over the Internet. Attackers can try to break into the data of almost any person or company, from anywhere (Cloud Flare 2025).

An IBM report from 2024 stated that the average cost of a data breach around the world is USD 4.88 million. Businesses of all kinds and sizes may be affected by a data breach, but the damage they cause and the costs of repair vary, and the average cost in recent years of a data breach in the US was USD 9.36 million which extremely large about four times the average cost of a data breach in India USD 2.35 million. Organizations in heavily controlled fields, such as finance and healthcare, may be hit especially hard by a data breach. The costs may even increase due to heavy fines and penalties (IBM 2024). According to a study by IBM, in 2023 the average cost of a healthcare data breach was USD 9.77 million which is twice the average cost of all breaches. (IBM 2024.)

Most people who break into data systems do so to earn money. Hackers obtain credit card numbers, bank account information, and other financial details to extort money from people and businesses. Some hackers try to steal people's identities by obtaining personally identifiable information (PII), such as social security, and phone numbers, to obtain loans and credit cards in their names. On the dark web, cybercriminals sell stolen PII and account information. For individual bank login data, they may obtain as much as USD 500. (NASD 2023.) A data breach may signify the beginning of a more extensive attack. For instance, hackers may acquire the email credentials of senior executives inside a corporation and use them to execute schemes that compromise corporate communications. Data breaches may pursue goals beyond personal gain. Unethical organizations may acquire trade secrets from opponents, while state-sponsored individuals might infiltrate governmental networks to acquire knowledge about sensitive political affairs, military activities, or national infrastructure. (IBM 2025.)

Typically, an attacker causes data breaches through the four steps illustrated in Figure 13.

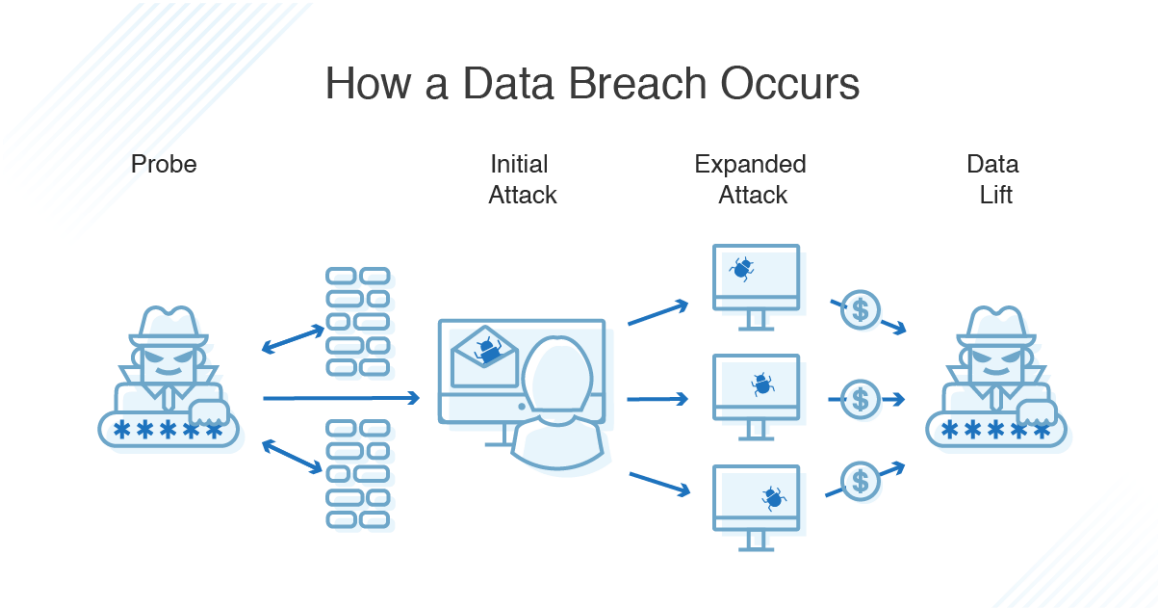

Figure 13. Occurrence of data breach (DNS Stuff)

The following steps define the occurrence of a data breach.

Probe

The first phase of a data breach involves acquiring knowledge about the network and the broader digital environment. The attackers may seek outdated software lacking the latest security updates, assess passwords, evaluate cybersecurity measures, or investigate the probability of a phishing attack. (DNS Stuff 2020.)

Initial attack

Upon discovering the most efficient approach for executing their attack, the attackers will commence the second phase. This may be launching an email designed to mislead workers into clicking a link to a harmful website or compromising a critical program necessary for employee activities. (DNS Stuff 2020.)

Expanded attack

Upon successfully exploiting a vulnerability, hackers will assess their subsequent actions. Typically, they use any advantage to infiltrate the network to acquire significant personal data. (DNS Stuff 2020.)

Data lift

As several security incidents occur across distinct timeframes, malicious individuals may either attempt to transfer substantial volumes of data simultaneously or remain invisible until they feel sufficiently safe to escape investigation. (DNS Stuff 2020.)

3.4.2 Ransomware

Ransomware is a type of malware that compromises a computer, restricting the user's access to the affected system or targeted files in order to extort payment. The target system generally terminates most operations and presents an on-screen notification upon its compromise. This notification frequently signifies that the system is secured or that all its data has been encrypted. A significant payment is required before the release of the system or the decryption of data. Ransomware will use the weaknesses or vulnerabilities in an organization's IT systems or infrastructure. The incidents are so evident that conducting a comprehensive investigation to ascertain if the company has been compromised or whether an occurrence requires reporting is redundant. (Learn Microsoft 2024.)

Cloud-based ransomware attacks which compromise the synchronized file sharing service, and ransomware incidents, such as encrypting data and demanding a ransom for its release. This type of an assault frequently commences with a compromised device that disseminates malware to a synchronized cloud service. Cloud ransomware attacks create access to corporate email communications, the network, and cloud-stored information and apps may be blocked for hours or even days. (Learn Microsoft 2024.)

Figure 14 illustrates the process of ransomware being initiated by an attacker.

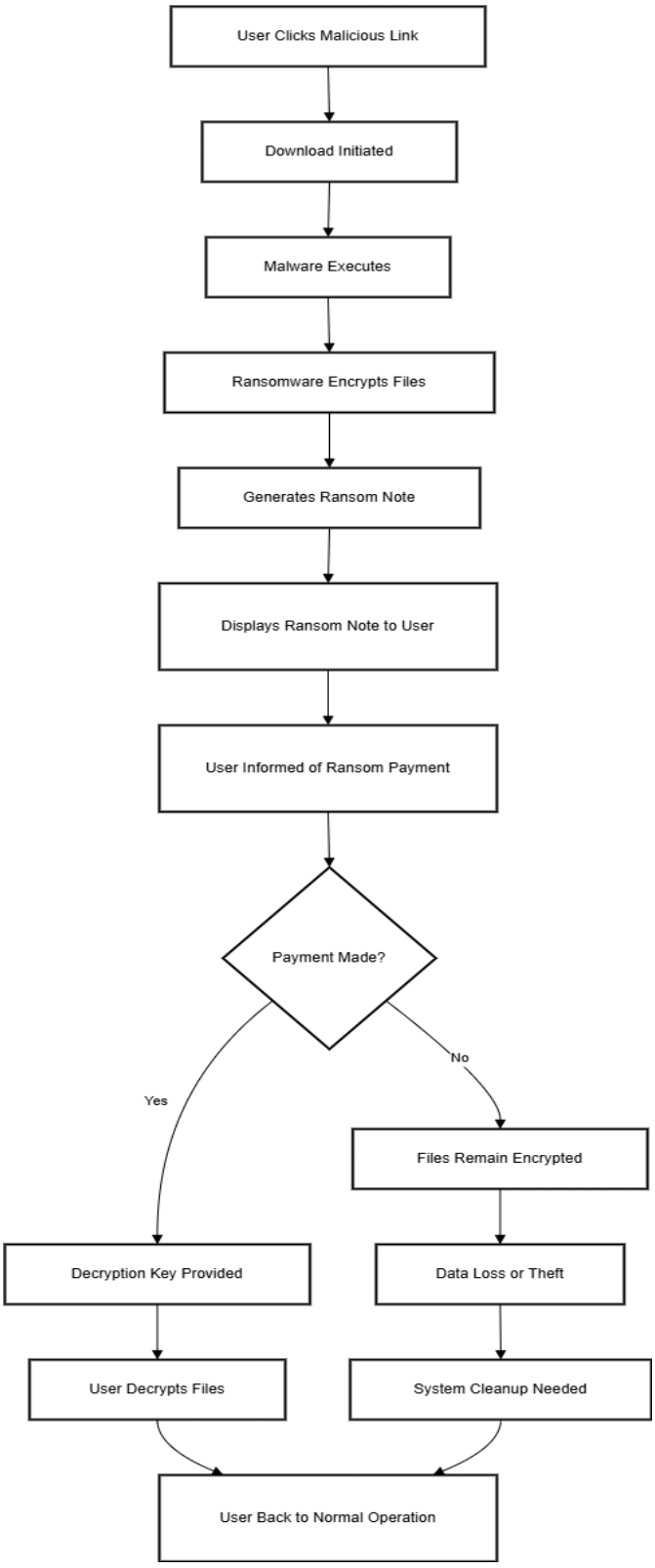

Figure 14. Process of a ransomware attack

According to a report by Seagate, in recent years, a Los Angeles hospital was requested to pay a ransom of $3.4 million, which resulted in the hospital being unable to operate its system for ten days. The average compensation for ransom demands is $541,010, with a range of $50,000 to $2.2 million, contingent upon the target. Over the past few years, 130 distinct ransomware families have been identified. (Seagate 2025.)

3.4.3 Data Integrity Attacks

Data integrity refers to an assessment of the accuracy, precision, and consistency of a company's data throughout the lifecycle. Data integrity protects an organization's data against breaches, loss, and negative consequences. Organizations require accurate data to make informed choices, predict customer behavior, evaluate market trends, and protect against data breaches. (IBM 2024.)

Organizations must have adequate security protocols to ensure the integrity and reliability of data and prevent unauthorized access. Data integrity errors may lead to inaccurate reports, evaluations, and insights. These errors may have significant consequences, including the loss of a competitive advantage, involvement in unproductive activities, and the making of harmful choices. Inaccurate sales forecasts may result in either an excess or deficiency of inventory, thereby escalating expenses and diminishing sales prospects. If data integrity issues persist, both employees and customers may lose confidence in the organization's performance and its ability to provide accurate and reliable information. (IBM 2023.)

3.5 User-level attacks

In user-level attacks, perpetrators can encrypt data stored in the cloud or restrict user access to cloud services. This assault swiftly disseminates throughout the organization's cloud infrastructure due to the interconnected characteristics of the cloud. Below most typical forms of user-level attacks are described.

3.5.1 Phishing attacks

Phishing emails, messages, or phone calls may include virus links appearing as legitimate links or direct visitors to seem reputable websites, consequently misleading individuals or personnel into disclosing their credentials. Phishing attacks may manifest in several forms. A fundamental phishing campaign may include the collection of several email addresses, along with a harshly crafted message and a link to a malicious website. This strategy may provide some outcomes, even if the majority of people will not be fooled by it. (SYSDIG 2025).

In a spear-phishing attack, the perpetrator gathers information on a specific target, such as name, location, job title, and organizational role. In order to enhance the authenticity of the fraudulent communication, these details help to the attackers (SYSDIG 2025).

Whaling is a sophisticated phishing assault that specifically targets an organization's senior executives. These activities are meticulously studied and crafted to use their leadership positions, access to key data, and dedication to the organization's welfare. Perpetrators often pose as questions about legal issues or consumer complaints, compelling the executive into prompt action against reputational or operational loss. (SYSDIG 2025.)

Smishing, or SMS phishing, is an effective technique used by hackers to confuse individuals into taking action. It entails sending a gentle text message containing an urgent request and a clickable hyperlink. These messages often exploit common worries or aspirations, such as alerts about a hacked bank account, notifications of an unforeseen reward, or updates concerning a postponed parcel. The risk is in activating the embedded link, which may result in the covert installation of malware or drive the user to a fake website intended to extract personal information, login passwords, or even validate phone numbers for malicious purposes. (SYSDIG 2025).

3.5.2 Credential stuffing

Credential stuffing is a hacking technique in which attackers use databases of compromised user credentials to gain unauthorized access to a system. Machines are used to automate and amplify an attack, predicated on the idea that several individuals utilize identical addresses and passwords across multiple websites. Basic security protocols, such as blocking IP addresses with an excessive frequency of failed login attempts, are often bypassed using these algorithms. (IMPERVA 2024.) Figure 15 illustrates the process of credential stuffing.

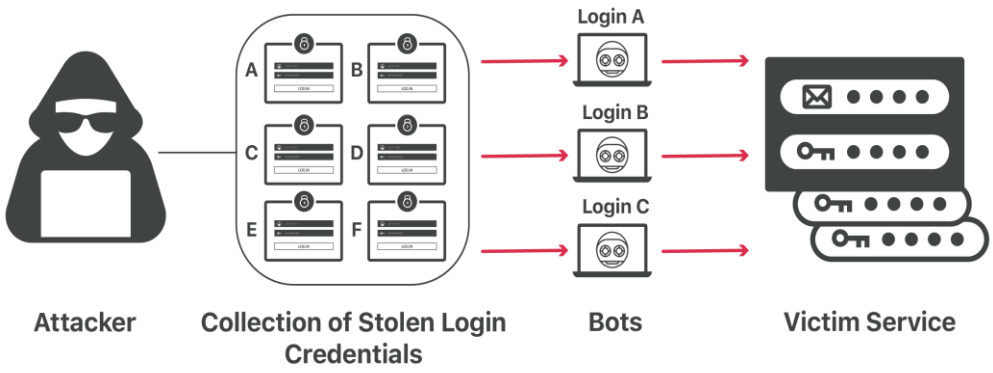

Figure 15. Credential Stuffing (CLOUDFLARE)

The SpyCloud Identity Exposure Report found that 74% of individuals use identical passwords across several accounts. This indicates that individuals often use identical login credentials across many websites. If an individual appropriates credentials from one website and subsequently utilizes them on other sites that express valuable information or satisfy to particular demographics, malicious actors are more likely to successfully acquire personal or financial data, fraudulent activity such as identity theft, initiate DDoS attacks, or disseminate malware. (SPYCLOUD 2025.)

The 2022 PayPal credential stuffing incidents highlight a significant instance of a credential stuffing attack. Cybercriminals acquired approximately 35,000 PayPal users' personally identifiable information (PII) during two days. This information included full names, social security numbers, tax identification numbers, and credit and debit card information. Following the identification of the attack, PayPal

swiftly implemented actions to rectify the security issue and advised all impacted customers to update their passwords and activate two-factor authentication (2FA). However, it is conceivable that the obtained credentials were used on other services unrelated to PayPal, possibly compromising some of accounts. (WIZ 2024.)

3.5.3 Insider threats

Organizations encounter a substantial cybersecurity risk resulting from the sophisticated problem of insider threats. Individuals can act as harmful insiders, attempting to undermine the operation or disseminate disinformation. Employees who commit accidental mistakes or fall victim to forceful hostility are considered undesirable insiders. The significance of identifying insider threats is growing. Malicious insiders often use methods that obscure their activities while executing their operations incrementally. This complicates the identification and mitigation of related hazards. Frequently, malevolent insider threat activities go undetected and unreported. Insiders may also disclose confidential information, modify data, lose portable devices, misconfigure systems, or violate security procedures. Potential consequences include data breaches, financial losses, brand deterioration, and regulatory violations. Any of these could compromise an organization. (Google Cloud 2023.)

Cloud configurations provide remote access, enabling employees to execute activities from any location, hence complicating the identification and mitigation of insider threats. The flexibility and scalability of cloud services, albeit for corporate operations, may expand the potential attack surface. (Cybersecurity-Magazine 2024.)

4 CLOUD SECURITY BREACH PREVENTION METHODS ACROSS MULTIPLE LEVELS

As organizations progressively transition to cloud environments, the security of cloud infrastructure becomes multifaceted, with attacks targeting

infrastructure, data, networks, applications, and user access points. Each level exhibits distinct weaknesses requiring customized protection measures. Implementing appropriate breach prevention measures may mitigate potential risks, protect personal data, and maintain the integrity, confidentiality, and availability of cloud services. Some of these measures are introduced below.

4.1 Breach prevention at the infrastructure Level

At the infrastructure level, security methods must be in place to the hardware, virtualization platforms, and physical data centers housing data. In order to avert unwanted access, cloud providers use surveillance systems, biometric entrance restrictions, and on-site security staff. In order to prevent assaults such as VM escape and side-channel exploitation, it is essential to defend the hypervisor inside a virtualized system. DDoS mitigation strategies, such as anomaly detection, auto-scaling, and rate limitation, are used to prevent the cloud infrastructure from being overwhelmed with traffic. Intel Software Guard Extensions (SGX) and AMD safe Encrypted Virtualization (SEV) are technologies that enable private computing by partitioning distinct duties into safe zones. Cloud security posture management (CSPM) systems provide the identification of vulnerabilities in Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS) models, allowing for the implementation of preventive measures. These technologies continuously evaluate the protection of multi-cloud environments by maintaining a current inventory of cloud assets that may be scrutinized and appraised for risks to identify any errors. (Cloudflare 2023.)

Figure 16 illustrates the recommended process to prevent security threats at the infrastructure level.

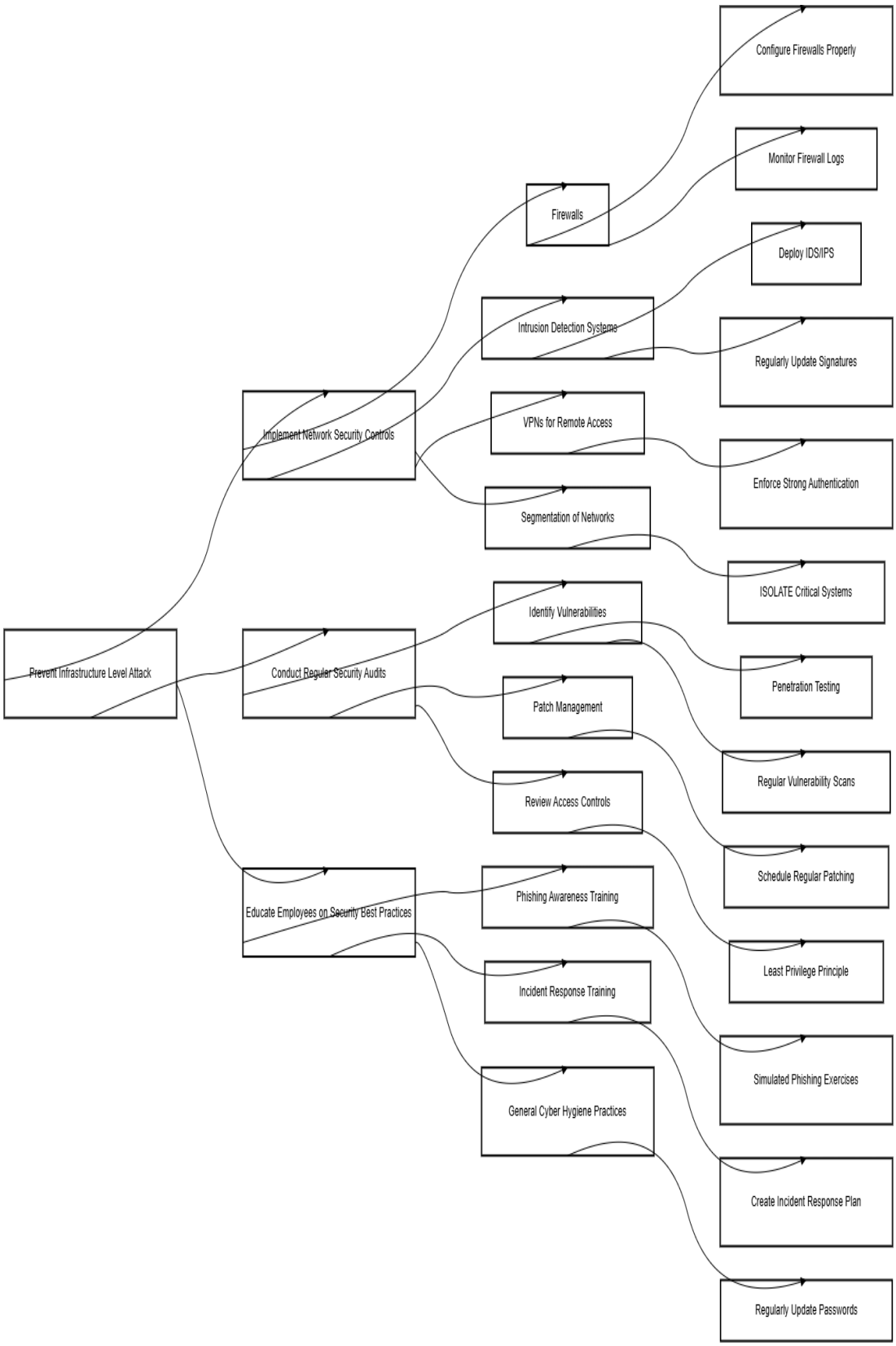

Figure 16. Prevention methods of infrastructure-level attacks

Prominent CSPM products include Prisma Cloud, Microsoft Cloud Defender, AWS Security Hub, Wiz, and Check Point CloudGuard. Cloudflare reports that machine learning based anomaly detection has significantly improved DDoS attack identification in recent years. (Cloudflare 2023.)

4.2 Prevention method at the Network Level

In order to protect the communication pathway and prevent illegal access, efficient defense measures at the network level are essential. IPSec VPN and Transport Layer Security (TLS) 1.3 are frequently utilized to safeguard data during transmission. This guarantees the secrecy of data sent between cloud services and clients. Numerous companies use a zero-trust architecture (ZTA) that authenticates all access requests, irrespective of their origin. This complicates the process of malware infiltration. Organizations must implement end-to-end encryption, such as SSL/TLS for data in transit, deploy intrusion detection and prevention systems (IDPS) like Palo Alto Networks' Prisma Cloud, monitor network data patterns to detect and mitigate anomalies, and establish stringent network segmentation utilizing virtual private clouds (VPCs) and security groups to mitigate these risks. Minimizing network-level risk in cloud systems entails deploying DDoS protection services, upkeep of detailed access control lists (ACLs), and continuously auditing network configurations.
OWASP recommends DNSSEC (Domain Name System Security Extensions) and certificate anchoring as critical measures against DNS spoofing and Man-in-the-Middle (MITM) attacks. (OWASP 2023.)
Figure 17 illustrates the suggested process to prevent security threats at the network level.

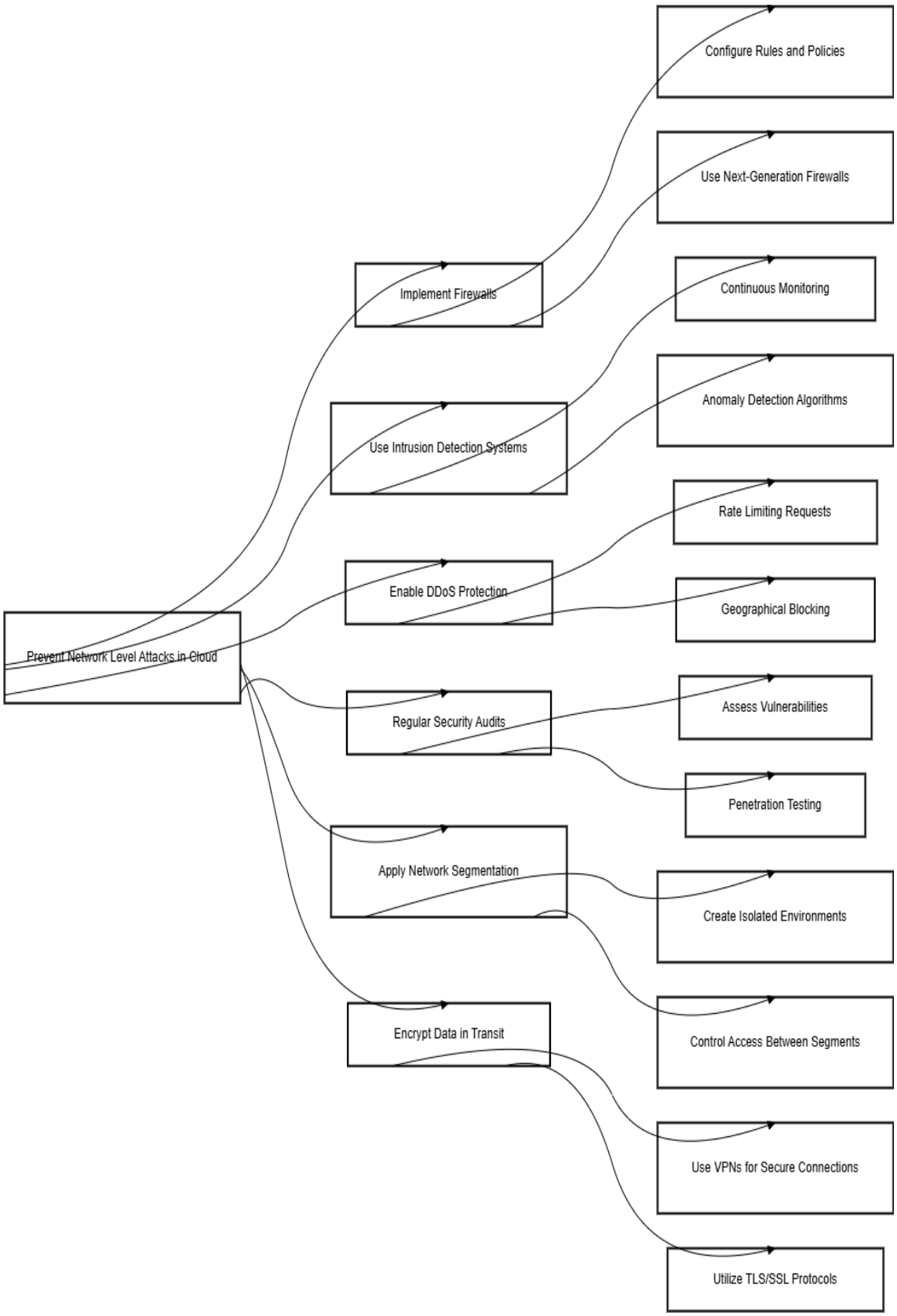

Figure 17. Prevention methods against Network-level attacks in the cloud

4.3 Prevention method at the Application level

Security protocols at the application layer primarily focus on cloud-based applications and the vulnerabilities within application programming interfaces (API). Comprehensive API design strategies, such as OAuth 2.0, OpenID Connect, and API ports, support the regulation and monitoring of user access to cloud services. Managing the input rate is vital to ensure its uniqueness, thereby protecting against brute-force attacks and injection vulnerabilities. (Cloud Security Alliance 2023.)

AWS WAF and Cloudflare WAF are two web application firewalls that protect applications against SQL injection, cross-site scripting (XSS), and other prevalent threats. Implementing DevSecOps to integrate security across the development lifecycle, conducting frequent code assessments, and adhering to stringent authentication and authorization protocols such as role-based access control (RBAC) and multi factor authentication (MFA) are effective strategies for safeguarding against attacks. The Cloud Security Alliance (CSA) emphasizes the need to test API security and use secure coding practices to mitigate the risks associated with cloud-native applications. (Cloud Security Alliance 2023.) Figure 18 illustrates a prevention method in cloud computing at the application level.

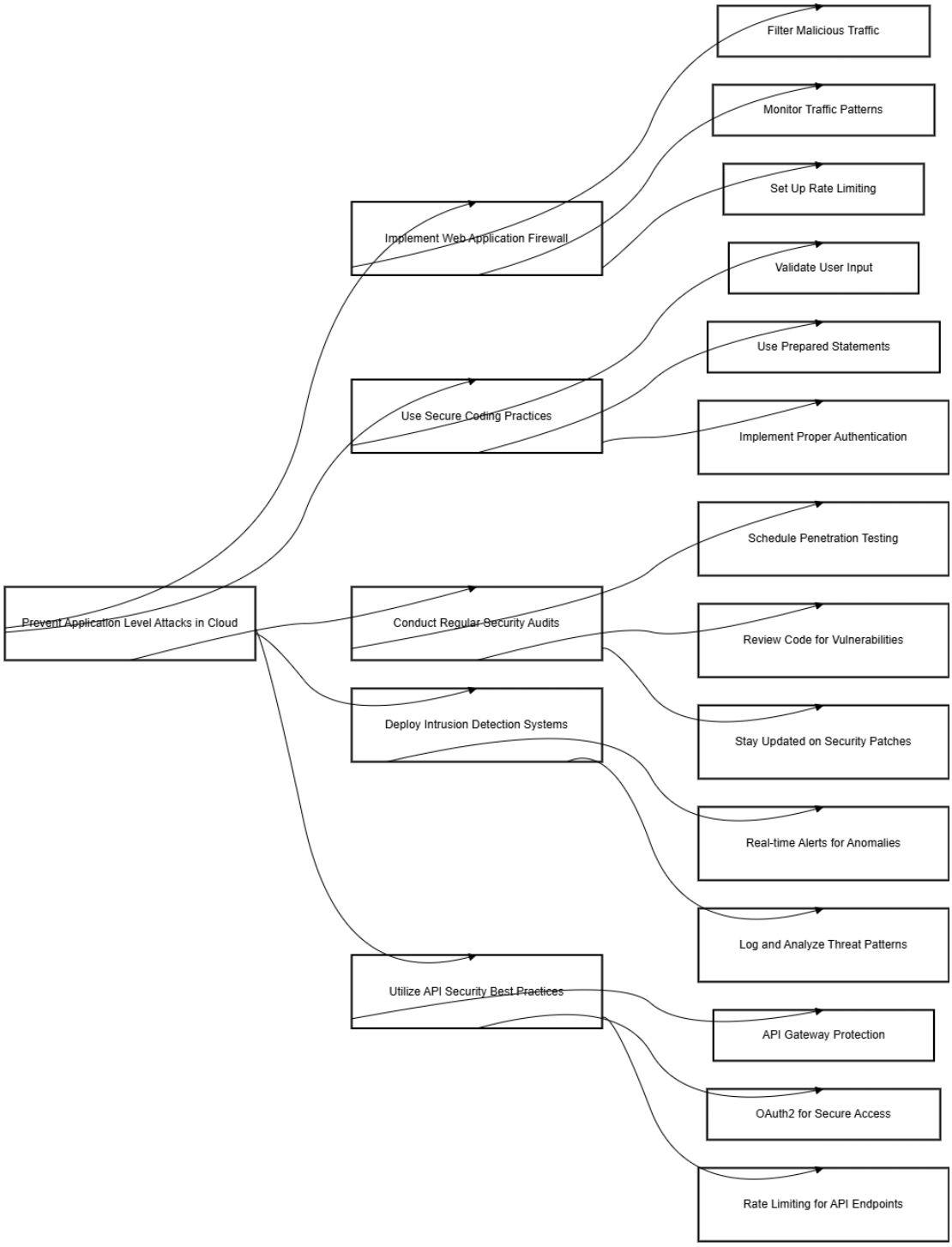

Figure 18. Prevention methods of Application-level attacks in the cloud

4.4 Preventing method at the Data level

Data breaches and ransomware attacks have become widespread, emphasizing the necessity of securely safeguarding cloud data. Figure 19 demonstrates the prevention method at the data level.

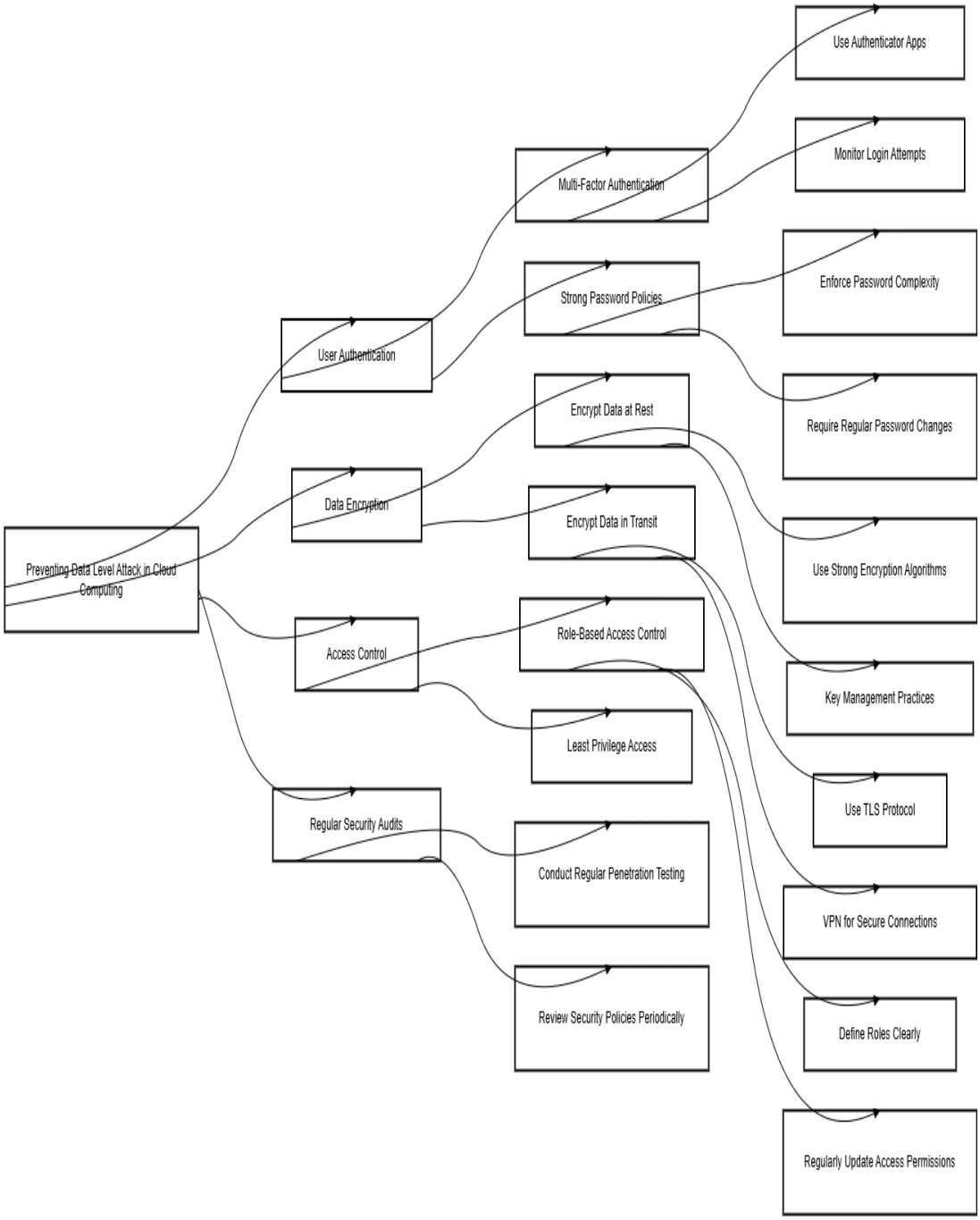

Figure 19. Prevention methods of Data-level attacks in the cloud

Encrypting private data, both at rest and in transit, makes its protection extremely simple. AES-256 encryption is mostly used to safeguard stored data, whilst TLS 1.3 encryption is utilized to protect data sent over a secure network. Certain secure computing solutions, such as Google Cloud Confidential VM, guarantee the safety of ongoing operations, preventing unauthorized access even in the event of infrastructure compromise. (IBM Security 2024.)

Personally identifiable information (PII) is safeguarded by data screening and tokenization. This assists enterprises in adhering to regulations such as GDPR and HIPAA. Immutable backups and geo-redundant storage (GRS) facilitate disaster recovery by safeguarding data from ransomware assaults. (IBM Security 2024.)

4.5 Prevention method at the User level

User level security measures are implemented to ensure the protection of user activities and the right to use credentials. Users may access cloud services with limited authorization through Identity and Access Management (IAM) systems such as Microsoft Entra ID and Okta IAM. Multi-factor authentication (MFA) is an additional security measure that employs biometric data, SMS codes, and passwords to verify identification. Behavioural analytics technologies, such as User and Entity Activity Analysis (UEBA), assist in detecting anomalous activity that may suggest account breach. The Verizon data breach investigation report (DBIR) reveals that security awareness training equips users to recognize hacking attempts and social engineering tactics which remain the predominant methods used by hackers to infiltrate networks (Verizon 2024).
Figure 20 illustrates a method to protect users against user-level attacks in the cloud.

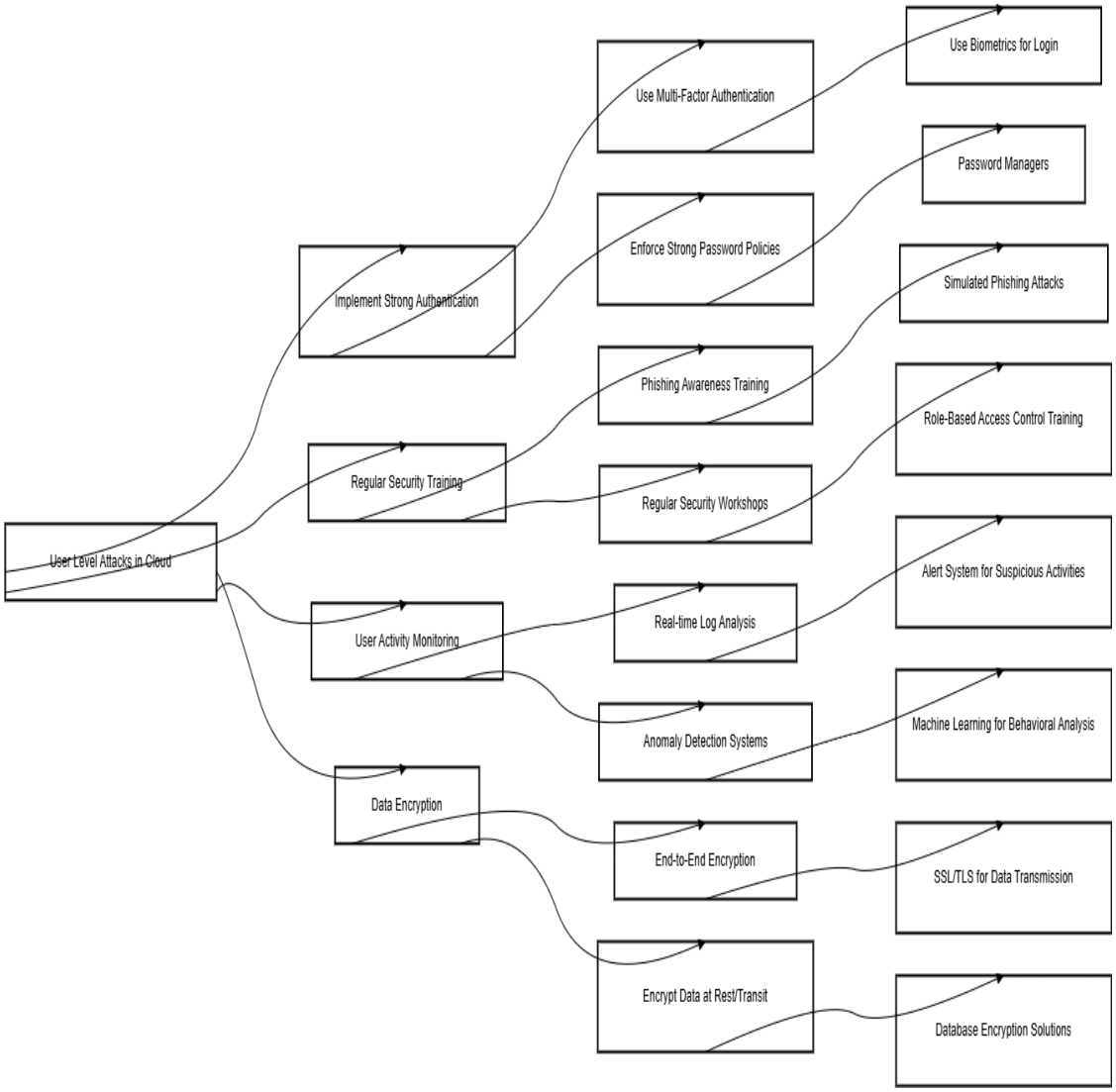

Figure 20. Prevention methods of User-level attacks in the cloud

The security of the cloud requires a thorough, tiered strategy. Organizations can significantly mitigate their security challenges by rectifying infrastructure deficiencies, ensuring the protection of network communications, securing APIs and applications, adequately safeguarding data, and equipping users with essential knowledge and resources. As cloud technologies evolve, the implementation of flexible security frameworks, such as a zero-trust model will be crucial for safeguarding against cloud-related security threats.

5 CASE STUDY: US TREASURY DEPARTMENT BREACH BY CHINESE STATE-SPONSORED HACKERS IN DECEMBER 2024

5.1 Incident Overview

A notable case study analyzed in the study involves the 2024 cyberattack on the U.S. Treasury Department by Chinese state-sponsored hackers. By exploiting a vulnerability in a third-party cloud service provider, the attackers accessed sensitive government documents. This incident highlighted the importance of securing supply chains, improving detection capabilities, and developing robust incident response strategies. (Reuters 2024.)

On December 8, 2024, BeyondTrust informed the Treasury Department of a security concern about their online assistance service. The attackers acquired a digital key used by BeyondTrust to secure a cloud-based service. This enabled them to circumvent security protocols and remotely access user computers inside the Treasury Department. This breach allows unauthorized individuals to see the public documents that users were maintaining. (Reuters 2024.)

Attack Vector

The incident was facilitated through a supply chain assault, whereby the threat actors focused on BeyondTrust's cybersecurity services used by the Treasury. The hackers may circumvent security safeguards and gain unauthorized access to the Treasury's network by compromising a critical key used for securing a cloud-based service. (POLITICO 2024.)

Response and Mitigation

The Treasury Department, in collaboration with the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), assessed the consequences and fortified the systems upon identifying the breach. The compromised service was discontinued, and there was no indication of continued access to Treasury systems or data. (NYPost 2024.)

5.2 Discussion: The Consequences and Lessons Acquired

Supply Chain Vulnerabilities

This event highlights the risks associated with third-party providers. In order to avoid indirect risks, firms must ensure that their associates adhere to strong security measures.

Advanced Persistent Threats (APTs)

This incident underscores the requirement for enhanced threat detection competencies and ongoing surveillance, considering the complex strategies used by state-sponsored APT groups.

Incident Response Preparedness

The Treasury's immediate response in collaborating with federal agencies and deactivating corrupted services emphasizes the significance of a comprehensive incident response plan. The online attack by the U.S. Treasury Department serves as a significant reminder of the evolving landscape of cyber threats, especially those originating from state-sponsored entities. In order to successfully minimize these risks, organizations must adopt comprehensive security policies that include supply chain protection, enhancement of threat detection techniques, and maintenance of strong incident response plans.

6 CONCLUSION

Cloud computing is acknowledged as a transformative technology that offers enterprises affordable, scalable, and adaptable options for data storage, computational power, and application hosting. The transition to cloud-based infrastructure has introduced an innovative variety of complex and ever-evolving security threats. The vulnerabilities exist at multiple layers of the cloud architecture, including infrastructure, network, application, data, and user access. Each layer has unique vulnerabilities that require specific preventative strategies.

Hypervisor vulnerabilities represent a significant threat, and if attackers acquire control of the hypervisor, they may access all virtual machines (VMs) on a host. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are prevalent and capable of overwhelming cloud servers and interrupting services. Threat exposure is exacerbated by improperly configured network security settings, permissive firewalls, or unprotected ports. In order to prevent such assaults, organizations require cloud security posture management (CSPM) technologies to continuously monitor setups, install DDoS mitigation solutions, and routinely update hypervisors.

At the network level, the intricately connected and shared framework of cloud computing creates several significant security concerns. Unauthorized access via unprotected terminals is a significant risk, potentially arising from misconfigured firewalls, unsecured ports, or susceptible virtual private networks (VPNs). Cloud infrastructures are vulnerable to man-in-the-middle (MITM) attacks, whereby outsiders intercept and manipulate data during transmission. Organizations must adopt end-to-end encryption, including SSL/TLS for data in transit, deploy intrusion detection and prevention systems (IDPS) to monitor traffic abnormalities, and establish strong network segmentation using virtual private clouds (VPCs) and security groups to mitigate these risks.

Application-level security in the cloud is crucial since most cloud-hosted applications are accessible over the internet, which may be vulnerable to attacks such as SQL injection, cross-site scripting (XSS), and insecure application

programming interfaces (APIs). The use of outdated software libraries may enable software supply chain assaults. Conducting frequent code assessments and implementing stringent authentication and authorization protocols, including role-based access control (RBAC) and multi-factor authentication (MFA), are effective defences.

Considering the quantity and sensitivity of the stored data, data-level security is paramount in the cloud where data breaches may occur due to insufficient access restrictions, improperly built databases, or poor encryption measures. Organizations require that all data be secured using strong cryptographic techniques, both in transit and at rest. Key management systems (KMS) must be established to guarantee the safe storage and processing of keys. In order to prevent data loss or corruption, it is essential to establish automatic backups and data upgrades.

Identity and access management (IAM) is crucial at the user access level to avert illegal access. In cloud systems, account hijacking is a common threat, sometimes arising from phishing assaults or compromised credentials. Insider dangers emerge when workers or contractors use their privileges. A fully operational IAM system is essential, including user behavior monitoring, regular access assessments, and well-defined rules. Efficient security measures include the immediate deactivation of dormant accounts, use of multifactor authentication (MFA), and limitation of access exclusively to absolutely necessary resources.

REFERENCES

Amazon Web Services. n.d. AWS Config: Continuous compliance for cloud resources. Available at https://aws.amazon.com/config/ [Accessed 7 October 2024].

AWS Shield. 2025. AWS Shield: Managed DDoS protection. Available at https://aws.amazon.com/shield/ [Accessed 25 February 2025].

BLACKDUCK. 2024. Cross-Site Scripting (XSS). Available at https://www.blackduck.com/glossary/what-is-cross-site-scripting.html [Accessed 6 October 2024].

Cloud Security Alliance. 2023. Security guidance for critical areas of focus in cloud computing v4.0. Available at https://cloudsecurityalliance.org/research/security-guidance [Accessed 5 October 2024].

CLOUDFLARE. 2024. Phishing attack. Available at https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack/ [Accessed 6 October 2024].

CLOUDFLARE. 2025. What is data breach. Available at https://www.cloudflare.com/en-gb/learning/security/what-is-a-data-breach/ [Accessed 8 October 2024].

Cloudflare. 2023. DDoS attack trends report 2023. Available at https://www.cloudflare.com/learning/ddos/ [Accessed 25 September 2024].

CLOUDSTRIKE. 2024. Bart Lenaerts-Bergmans. 03 May 2024. Injection Attack. Available at https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/injection-attack/ [Accessed 23 September 2024].

CloudTweaks. 2024. Why API Attacks Threaten Your Cloud, Available at https://cloudtweaks.com/2024/09/why-api-attacks-threaten-your-cloud/ [Accessed 15 October 2024].

Cyber Insight. 2023. Adcyber what are Hypervisor Attacks? Securing Virtualized Environments, available at https://cyberinsight.co/what-are-hypervisor-attacks/ [Accessed 10 October 2024].

CYBERSECURITY-MAGAZINE. 2024. Why the Cloud Is So Vulnerable to Insider Threats. Available at https://cybersecurity-magazine.com/why-the-cloud-is-so-vulnerable-to-insider-threats/ [Accessed 12 October 2024].

DNSstuff. 2020. What is a Data Breach? Ultimate Guide to Cyber Security Breaches. Available at: https://www.dnsstuff.com/data-breach-101 [Accessed 27 September 2024].

Gartner. 2022. Top security and risk trends in cloud computing. Available at https://www.gartner.com [Accessed 20 October 2024].

Gartner. 2022. Top security and risk trends in cloud computing. Available at https://www.gartner.com [Accessed 15 October 2024].

Google Cloud Platform. 2022. "History of Google Cloud." Google Cloud Blog. Available at https://cloud.google.com. [Accessed 8 October 2024].

GOOGLE CLOUD. 2023. Muhammad Muneer, Chris Madge, Arjun Bhardwaj; Insider Threat: Hunting and Detecting. Available at https://cloud.google.com/blog/topics/threat-intelligence/insider-threat-hunting-detecting/ [Accessed 25 September 2024].

IBM. 2023. Data Integrity Issues: Examples, Impact, and 5 Preventive Measures. Available at https://www.ibm.com/think/insights/data-integrity-strategy [Accessed 8 October 2024].

IBM. 2024. Cost of data breach report 2024. Available at https://www.ibm.com/reports/data-breach [Accessed 8 January 2025].

IBM. 2025. Matthew Kosinski. What is a data breach? Available at https://www.ibm.com/think/topics/data-breach [Accessed 18 February 2024].

IBM Security. 2024. Cost of a data breach report 2024. Available at https://www.ibm.com/security/data-breach [Accessed 15 October 2024].

IBM. 2024. Tim Mucci and Cole Stryker. What is data Integrity and why is data Integrity important. Available at https://www.ibm.com/think/topics/data-integrity [Accessed 15 October 2024].

IBM. 2024. Gregg Lindemulder and Matthew Kosinski What is man-in-the-middle (MITM) attack. Available at https://www.ibm.com/think/topics/man-in-the-middle [Accessed 7 October 2024].

IEEE Xplore. 2022. Abdullah Albalawi, Vassilios Vassilakis, Radu Calinescu. Side-channel Attacks and Countermeasures in Cloud Services and Infrastructures. Available at https://cyberinsight.co/what-are-hypervisor-attacks/ [Accessed 29 October 2024].

IMPERVA. 2025. Man in the Middle (MITM) Attack. Available at https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ [Accessed 15 February 2025].

IMPERVA. 2025. What is *DNS Spoofing?* Available at: https://www.imperva.com/learn/application-security/dns-spoofing/ [Accessed 18 February 2025].

IMPERVA. 2024. Credential stuffing. Available at https://www.imperva.com/learn/application-security/credential-stuffing/ [Accessed 5 October 2024].

Intel. n.d. Intel Software Guard Extensions (SGX) overview. Available at https://software.intel.com/content/www/us/en/develop/topics/software-guard-extensions.html [Accessed 13 February 2025].

ISO. 2022. ISO/IEC 27001: Information security management systems. Retrieved from https://www.iso.org/obp/ui/en/#iso:std:73906:en [Accessed 28 February 2025].

ITU. n.d. What is a hypervisor-level attack. Available at https://www.ituonline.com/tech-definitions/what-is-a-hypervisor-level-attack/ [Accessed 20 February 2025].

Lark. 2024. IP Hijacking. Available at https://www.larksuite.com/en_us/topics/cybersecurity-glossary/ip-hijacking [Accessed 22 February 2025].

LEARN MICROSOFT. 2024. Ransomware protection in Azure. Available at https://learn.microsoft.com/en-us/azure/security/fundamentals/ransomware-protection [Accessed 20 November 2024].

McCarthy, J. 1961. "Speech at the MIT Centennial: Time-sharing computer systems." Available at https://archive.org/details/managementcomput00gree/page/220/mode/2up?view=theater () [Accessed 2 October 2025].

Microsoft Azure. 2025. Azure Policy: Simplified cloud compliance. Available at https://learn.microsoft.com/en-us/azure/governance/policy/ [Accessed 2 March 2025].

Microsoft Azure. 2021. "The History of Microsoft Cloud." Microsoft Azure Blog. Available at https://azure.microsoft.com. [Accessed 6 October 2024].

Microsoft Azure. n.d. Azure Policy documentation. Available at https://learn.microsoft.com/en-us/azure/governance/policy/ [Accessed 20 January 2025].

Microsoft. 2024. Microsoft Digital Protection Report 2024. Available at https://www.microsoft.com/fi-fi/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024 [Accessed 20 November 2024].

NASDAQ. 2023. Heather Taylor. How Much Do Hackers Make From Stealing Your Data? Available at https://www.nasdaq.com/articles/how-much-do-hackers-make-from-stealing-your-data [Accessed 12 November 2024].

NORTON. 2025. Oliver Buxton. IP spoofing: What is it and how does it work. Available at https://us.norton.com/blog/malware/what-is-ip-spoofing [Accessed 20 January 2025].

NYPost. 2024. Ryan King, Chinese hackers infiltrate US Treasury in major cyberattack, officials tell Congress. Available at https://nypost.com/2024/12/30/us-news/chinese-hackers-infiltrate-us-treasury-in-major-cyberattack-officials-tell-congress/ [Accessed 20 February 2025].

OWASP. 2025. KirstenS. Cross-site scripting (XSS), Available at https://owasp.org/www-community/attacks/xss/ [Accessed 13 January 2025].

OWASP. 2022. OWASP API security project: Top 10 vulnerabilities. Available at https://owasp.org/www-project-api-security/ [Accessed 20 December 2024].

PALOALTO Networks. 2025. What is API security? Available at https://www.paloaltonetworks.com/cyberpedia/what-is-api-security [Accessed 1 March 2025].

POLITICO. 2024. Sam Sutton, Treasury breached by Chinese hackers in ‘major’ cybersecurity incident, Available at https://www.politico.com/news/2024/12/30/treasury-breached-chinese-hackers-cybersecurity-00196140 [Accessed 3 March 2025].

Researchgate. 2017. Nayeem Ahmed Khan. Hypervisor attack on VM. Available at: https://www.researchgate.net/figure/Hypervisor-attack-on-VM_fig1_329937281 [Accessed 28 February 2025].

Reuters. 2024. Raphael Satter and A.J. Vicens, US Treasury says Chinese hackers stole documents in 'major incident'. Available at https://www.reuters.com/technology/cybersecurity/us-treasurys-workstations-hacked-cyberattack-by-china-afp-reports-2024-12-30/ [Accessed 1 March 2025].

SEAGATE. 2025. Ransomware's Impact on Cloud Security. Available at https://www.seagate.com/blog/ransomware-impact-on-cloud-security/ [Accessed 2 March 2025].

SECURITY. 2023. Over half of organizations experienced an insider threat in 2022. Available at https://www.securitymagazine.com/articles/98879-over-half-of-organizations-experienced-an-insider-threat-in-2022 [Accessed 8 December 2024].

SPYCLOUD. 2025. Credential stuffing attack. Available at https://spycloud.com/glossary/credential-stuffing-attack/ [Accessed 3 March 2025].

SYSGIG. 2025. What is phishing? Available at https://sysdig.com/learn-cloud-native/what-is-phishing/ [Accessed 2 March 2025].

TechTarget. 2025. Stephen J. Bigelow. The history of cloud computing explained. Available at https://www.techtarget.com/whatis/feature/The-history-of-cloud-computing-explained [Accessed 26 February 2025].

TechTarget. 2021. Gavin Wright, Alexander S. Gillis. How a side-channel attack works. Available at https://www.techtarget.com/searchsecurity/definition/side-channel-attack [Accessed 17 December 2024].

THE ACUNETIX. 2025. Understanding Injection Attacks in Application Security: Types, Tools, and Examples. Available at https://www.acunetix.com/blog/articles/injection-attacks-application-security/ [Accessed 1 March 2025].

ThreatDown. 2021. Peater Arntz. What is sniffing. Available at https://www.threatdown.com/blog/what-is-ip-sniffing/#:~:text=A%20sniffing%20attack%20involves%20the%20illegal%20extraction%20of,to%20steal%20customer%20data%20and%20compromise%20network%20security. [Accessed 12 November 2024].

Verizon. 2024. Data breach investigations report (DBIR). Available at https://www.verizon.com/business/resources/T870/reports/2024-dbir-data-breach-investigations-report.pdf [Accessed 14 January 2025].

VMware. 2020. "The Evolution of Virtualization: From Hardware to the Cloud." VMware Official Blog. Available at https://www.vmware.com. [Accessed 1 October 2024].

WIZ 2024. 2024. Credential Stuffing Explained. Available at https://www.wiz.io/academy/credential-stuffing [Accessed 8 October 2024].

LISTS OF FIGURES

Figure 9. Hypervisor attack on VM.Researchgate. Nayeem Ahmed Khan. December 2017. Available at https://www.researchgate.net/figure/Hypervisor-attack-on-VM_fig1_329937281 [Accessed 9 March 2025]

Figure 10: Example of SQL Injection attack. A Screenshot of the logging page. Available at https://xidp.xamk.fi/idp/profile/SAML2/Redirect/SSO?execution=e1s2 [Accessed 9 March 2025]

Figure 12: API attack anatomy. Paloalto. Available at https://www.paloaltonetworks.com/cyberpedia/what-is-api-security [Accessed 9 March 2025]

Figure 13: How a data breach occurs.DNSstuff. 23 August 2020. Available at https://www.dnsstuff.com/data-breach-101 [Accessed 9 March 2025]

Figure 15: Common indicators of phishing attacks. Technology Solution. Available at https://www.technologysolutions.net/blog/common-indicators-of-phishing-attacks/ [Accessed 9 March 2025]

Figure 16: What is credential stuffing? CLOUDFLARE. Available at https://www.cloudflare.com/en-gb/learning/bots/what-is-credential-stuffing/ [Accessed 8 March 2025]