جامعة بيرزيت

BIRZEIT UNIVERSITY

لن يستطيعوا كسر إرادتنا، كلنا غزة

OUR WILL IS UNBREAKABLE... WE ARE ALL GAZA

Cloud Computing Project

1220783

AbdAl-rheem Yaseen

Proposal for Migrating TechSolutions Inc. to Google Cloud Platform:

This proposal outlines a migration plan to Google Cloud Platform (GCP), addressing TechSolutions Inc.'s goals and security concerns, where it seeks to migrate its on-premises IT infrastructure to the cloud to achieve improved scalability, accessibility, and cost-effectiveness.

Understanding Cloud Computing and Google Cloud Platform:

Google Cloud Platform (GCP) offers a set of cloud computing services that leverage the same infrastructure that Google uses internally for its products like Google Search and YouTube. Google Cloud Platform provides various services including computing power, storage, databases, and machine learning.

Critical characteristics of cloud computing:

Cloud computing is defined by several important characteristics:

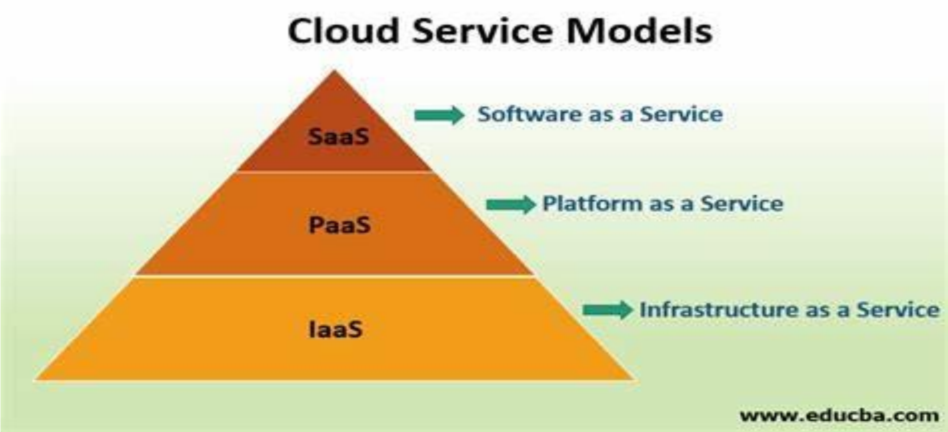
- On-demand self-service: Users can automatically provision computing power as needed.
- Cloud services can be accessed over the Internet through a variety of devices, which allows users to access applications and data from anywhere with an Internet connection.
- Flexibility: Capacity can be provided flexibly to expand quickly to match demand.

For More: Click Here

Cloud service models:

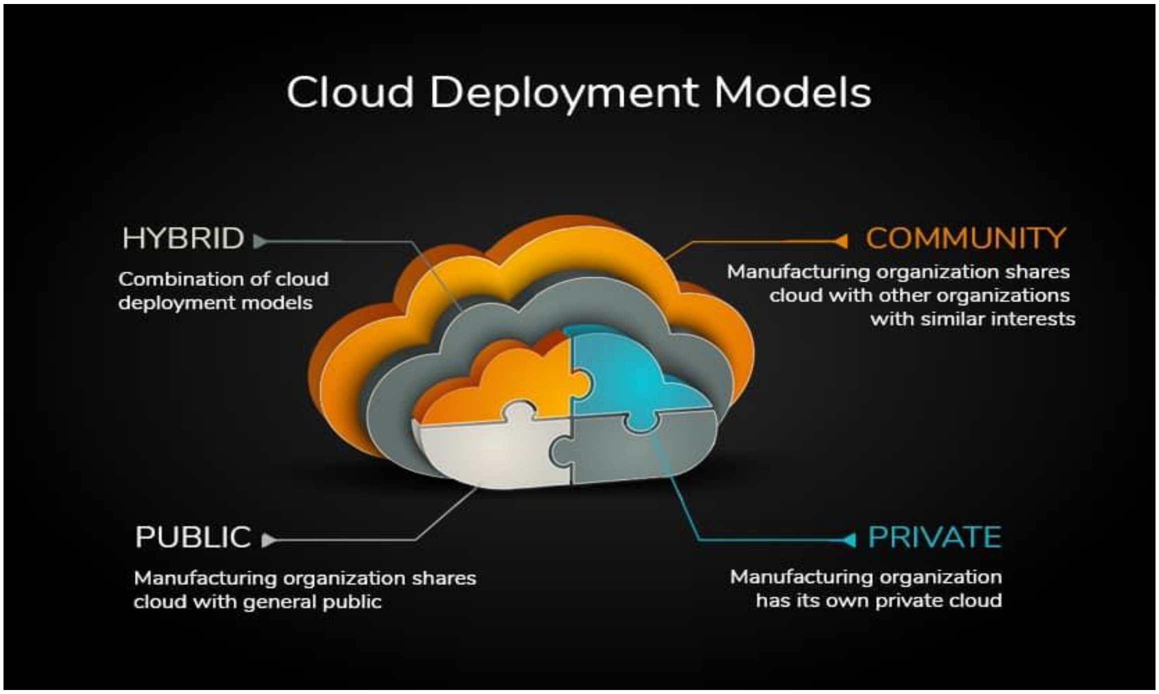
Google Cloud Platform offers multiple service models such as:

- Infrastructure as a Service (IaaS): Provides virtual computing resources over the Internet. Compute Engine on Google Cloud Platform provides scalable virtual machines. Click here
- Platform as a Service (PaaS): Provides a platform that allows customers to develop, run, and manage applications without dealing with the underlying infrastructure. Google App Engine is a PaaS component of Google Cloud Platform. Click here
- Software as a Service (SaaS): Offers software applications over the Internet on a subscription basis. Google Workspace provides productivity and collaboration tools. Click here



Cloud deployment models:

- Public Cloud: Services are delivered over the public Internet and shared across organizations. GCP is a public cloud provider. Click here
- Private Cloud: Services are maintained on a private network, which provide greater control and security. Click here
- Hybrid cloud: Combines public and private clouds, allowing data and applications to be shared between them, also providing flexibility and optimization of existing infrastructure, security and compliance. Click here


Cloud Deployment Models
HYBRID
Combination of cloud deployment models
COMMUNITY
Manufacturing organization shares cloud with other organizations with similar interests
PUBLIC
Manufacturing organization shares cloud with general public
PRIVATE
Manufacturing organization has its own private cloud

Alignment with TechSolutions Inc.'s goals:

Migrating to Google Cloud Platform aligns with TechSolutions Inc.'s business goals by providing:

- Scalability: You can easily scale resources up or down based on your demand.
- Accessibility: You can access resources from anywhere.
- Cost-effective: Pay only for what you use.
- Innovation: Leverage advanced services such as machine learning and data analytics.

Cloud computing security assessment:

Security risks and challenges:

Cloud computing could have a security risks and challenges:

Cloud computing risks can be summarized in four

management areas:

- ❖ Governance management risk.
- ❖ Enterprise management risk.
- ❖ Information management risk.
- ❖ Information security.

- Data breaches: Access sensitive data stored in the cloud by unauthorized people without your knowledge or permission, a data breach may occur due to a targeted attack, human mistake, or insufficient security measures. So, any material not intended for public access is deemed a data breach.

Data breach threats lead to three main violations:

- Data privacy violations.
- Data confidentiality violations.
- Data integrity violations.

Data Breaches Associated Vulnerabilities:

A vulnerability is any weakness in an information system, system security operations, central administration, or application that could be misused or controlled by a remote attacker.

Data breach threats lead to three main violations:

- Data Privacy Violations: Data privacy violations occur when personal or sensitive information is accessed or used.
- Data Confidentiality Violations: Data confidentiality violations occur when sensitive information is accessed or disclosed to unauthorized entities, compromising the secrecy of the data.
- Data Integrity Violations: Data integrity violations occur when information is altered, deleted, or otherwise corrupted in unauthorized ways, leading to inaccurate or incomplete data.

Shared responsibility model:

Both the cloud provider (Google) and the customer (TechSolutions Inc.) play roles in ensuring security:

Google Cloud Responsibilities:

Network and device security:

Google is responsible for the security of the physical infrastructure, including the network and hardware devices. This includes:

- Network Security: Google implements measures to protect its network, such as firewalls, virtual private networks (VPNs), and secure access points.

- Device Security: Physical devices and infrastructure are protected in Google data centers through robust security measures. Google ensures that hardware is regularly updated and patched to protect against vulnerabilities.

Cloud infrastructure security:

- Physical Security: Google's data centers are equipped with layered security measures to prevent unauthorized access. This includes restricted access areas, security cameras, and controlled access points.
- Data Encryption: Google encrypts data both at rest and in transit using strong encryption protocols.
- Operational Security: Google employs advanced operational security practices to protect data.

Client Responsibilities:

Identity and access management:

Clients are responsible for managing who can access their cloud resources and what actions they can perform. This involves:

- User Authentication: Implementing strong authentication mechanisms, such as multi-factor authentication (MFA), to verify user identities
- Security in the cloud (data and applications):
  - Data Security: Encrypting sensitive data before storing it in the cloud.
  - Application Security: Ensuring that applications running on GCP are secure by following secure development practices.

Security measures by Google Cloud

Google Cloud Platform provides robust security measures suitable for TechSolutions Inc.:

- Encryption: Data is encrypted at rest and in transit.
- Network security: Google Cloud Platform offers network security features such as Virtual Private Cloud (VPC) and firewall rules to help TechSolutions Inc. To create secure network environments.
- DDoS Protection: GCP provides built-in DDoS (Distributed Denial of Service) protection to help mitigate the impact of DDoS attacks on TechSolutions Inc.'s applications and services.

Data security requirements:

This issue must be addressed by TechSolutions Inc. Several data security requirements:

- **Privacy:**

Privacy in cloud computing refers to the protection of personal and sensitive information from unauthorized access, use, or disclosure.

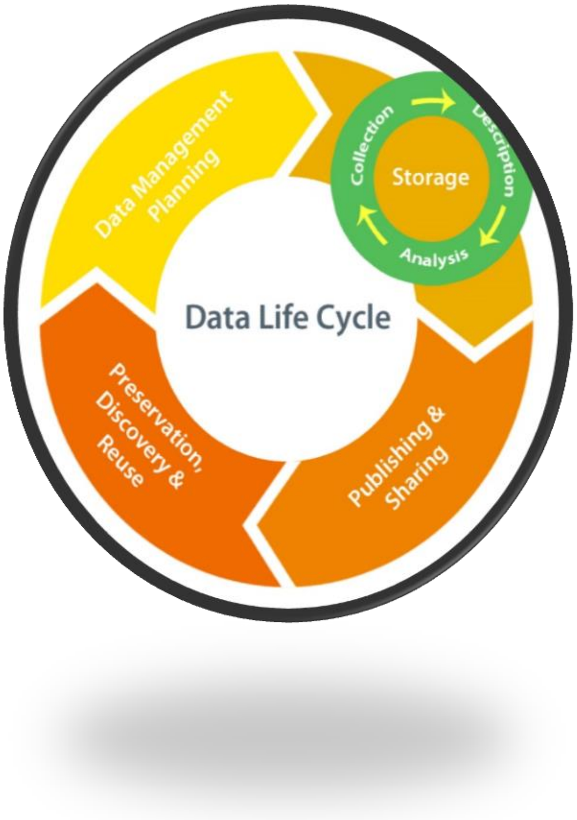
- **Confidentiality:**

Confidentiality in cloud computing is a crucial part of keeping information secure. It focuses on protecting data from being accessed or shared without permission. This is especially important because cloud environments involve storing and processing data on shared servers managed by third-party providers.

- Integrity:

Data integrity is the assurance that digital information is uncorrupted and can only be accessed or modified by those authorized to do so.

Data classification and lifecycle management



Data classification and lifecycle management play essential roles in maintaining data security within cloud computing Data classification based on its sensitivity is foundational to data security. By assigning classification levels: Organizations can efficiently manage, protect, and handle their data assets. While lifecycle management works on data from its creation until its disposal. Thus, the company reduces the risk of unauthorized access to data. Together, these practices protect and secure data.

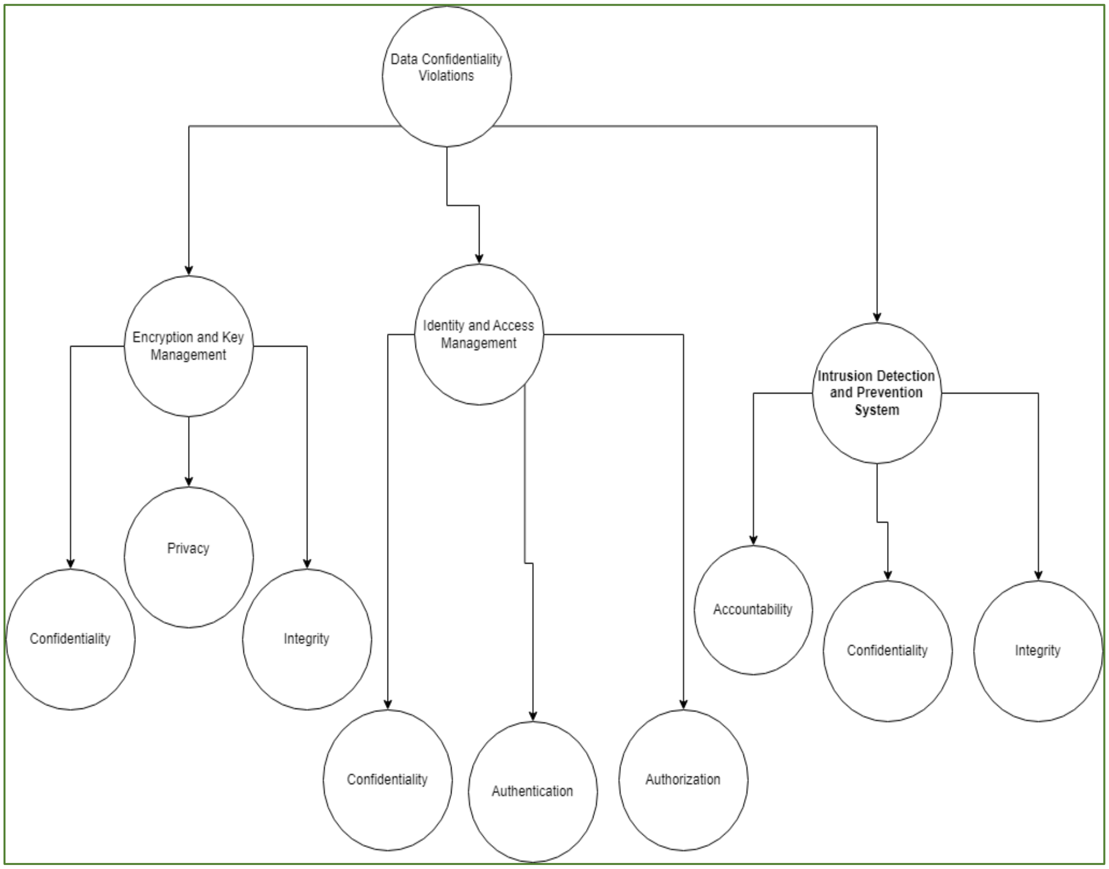
Data can be classified into three levels:

- Primary (non-sensitive data).
- Confidential (personal information).
- Highly confidential, stored data (financial, political, Health).

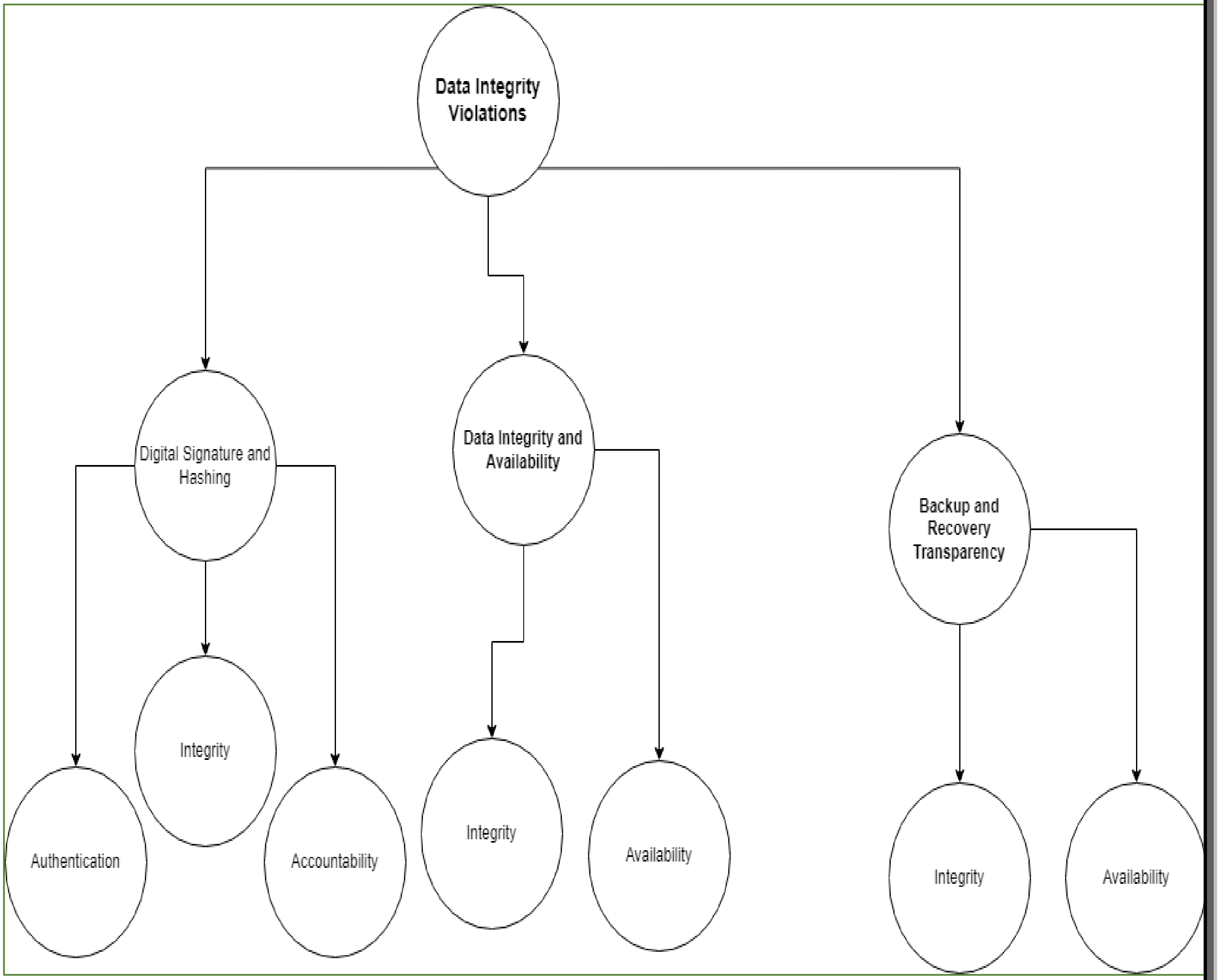
Cloud native security services and tools:

Google Cloud Platform (GCP) offers a set of cloud-native security services and tools designed to efficiently secure data in the cloud. Identity and Access Management (IAM) is defined as the security discipline that permits the appropriate users to access the right resources at the correct time for the proper purposes., while key management service (KMS) allows management of cryptographic keys to encrypt data. Cloud Data Loss Prevention (DLP) helps discover and protect sensitive data. Together, these tools mitigate risks.

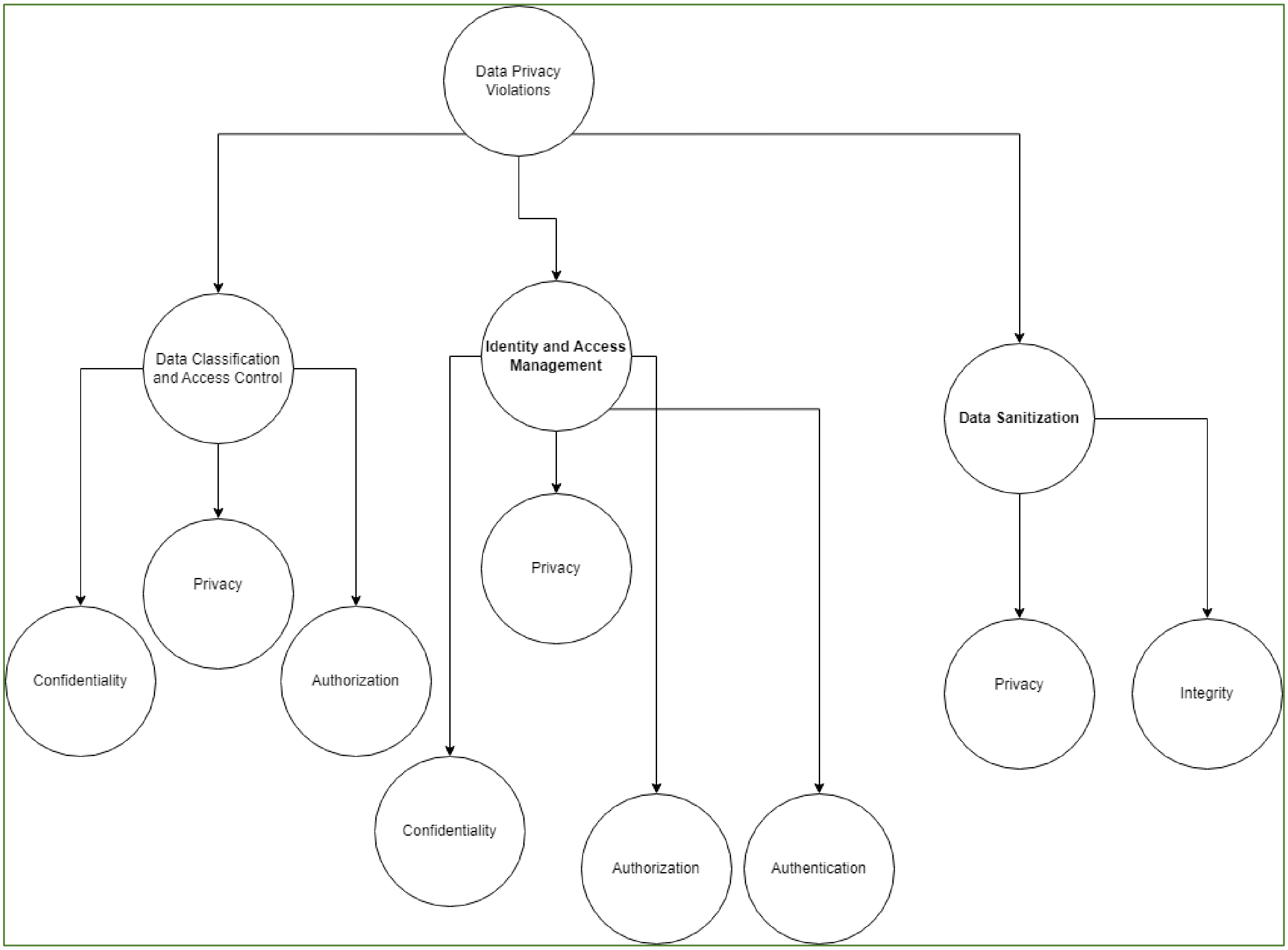
Address data breaches, vulnerabilities, and security requirements:


Data Confidentiality Violations
Encryption and Key Management
Identity and Access Management
Intrusion Detection and Prevention System
Privacy
Confidentiality
Integrity
Accountability
Confidentiality
Integrity
Confidentiality
Authentication
Authorization

Data confidentiality Violations


Data Integrity Violations
Digital Signature and Hashing
Data Integrity and Availability
Backup and Recovery Transparency
Authentication
Integrity
Accountability
Integrity
Availability
Integrity
Availability

Data integrity Violations



Data privacy Violations

Encryption and keys Management are essential, for protecting the privacy of data while methods like data classification and access control help in managing data based on its sensitivity. To ensure the integrity and authenticity of data, digital signatures and hashing techniques are recommended. User access control mechanisms play a role in maintaining confidentiality and enforcing authorization procedures. Furthermore, systems for detecting and preventing intrusions work towards monitoring and mitigating access strengthening both confidentiality and integrity. Emphasis is placed on measures to preserve data integrity and availability including backup processes. Building trust frameworks and implementing data sanitization practices further enhance security measures. These efforts are complemented by a set of requirements covering privacy protection, This framework provides an approach to understanding. Addressing the diverse security challenges present, in cloud computing environments.