Secure Cloud Migration Strategy for TechSolutions Inc.: Leveraging Microsoft Azure for Enhanced Scalability and Data Protection

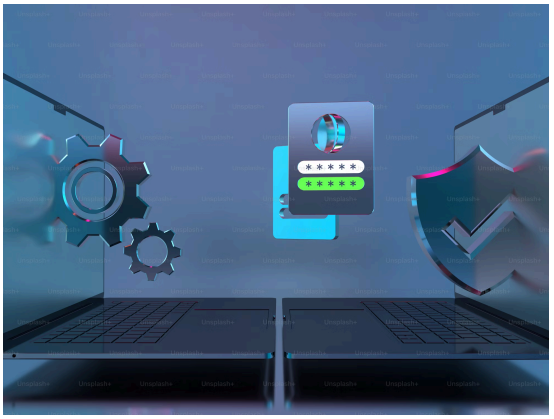
Yuna Nawahda[1]
[1]Faculty of Computer Science, Birzeit University, Palestine,1211524

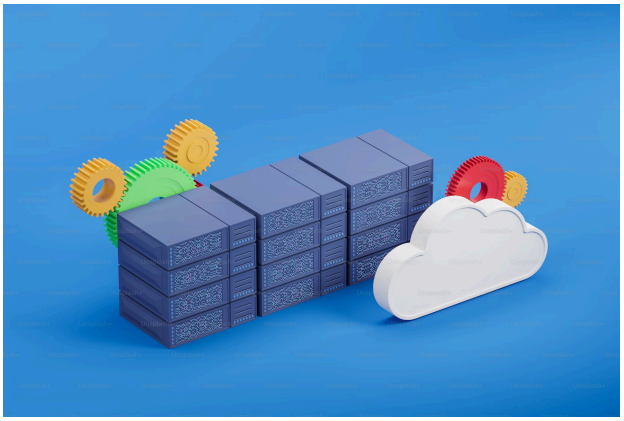
Introduction:

This paper explores the security challenges faced by cloud computing. It discusses the prevailing protection tactics to secure the cloud infrastructure, programs, and drawbacks[2]. Cloud computing started in the mid 90's and one of its earlier users are Amazon and Ali Baba. It is growing fast in the field of computer science. People nowadays use cloud computing at a vast level. Cloud computing is based on the Internet and has the most powerful computation architecture. After a particular has deployed his/her cloud-based platform, the biggest fear is its security.[2] As mentioned earlier, a cloud is all web-based, meaning retrieving data from a particular cloud isn't impossible. As the use of cloud computing grows, so do the security challenges. More people are becoming aware of the technology making it easier for them to break into different clouds and retrieve their desired information.[2] Many organizations have started offering cloud-based solutions to their customers, making security a major aim of their projects. On the other hand, many security experts are working on finding better security solutions. Even though security is getting better daily, hackers are still finding ways to exploit a particular cloud. The Cloud security concern becomes more complex below the cloud model as many other fields continuously enter the Cloud computing industry.[2]

The present study outlines a deliberate approach to migrating centralized systems to the cloud, given the emergence of cloud computing as a prevailing trend in organizational operations.[1] This technological advancement has facilitated innovation and competition among businesses by enabling the adoption of novel and inventive business models. The increasing prevalence and efficacy of cloud technology have led to the development of cloud-based Infrastructure-as-a-Service (IaaS) systems, thereby providing an alternative to conventional on-premise systems.[1] Cloud-based systems offer numerous advantages for enterprises. Infrastructure engineers must attend to data security concerns before migrating their enterprise applications to the cloud. [1]The utilization of cloud-based systems gives rise to particular apprehensions regarding the preservation of confidentiality and integrity of the data that is stored in the cloud.

We will investigate moving TechSolutions Inc.'s IT infrastructure to the cloud as part of our proposal for (Microsoft Azure), with an emphasis on finding security flaws and creating a strong security plan specifically for TechSolutions Inc. The objective of this proposal is to investigate the features and services provided by our cloud platform to address any security concerns and suit the demands of TechSolutions Inc.





Keywords:

Cloud Migration, Security, TechSolutions Inc., Data Encryption, Access Controls, Microsoft Azure, Data breach, vulnerabilities, shared responsibility model.

So I will start by introducing Microsoft Azure,

What is Microsoft Azure?

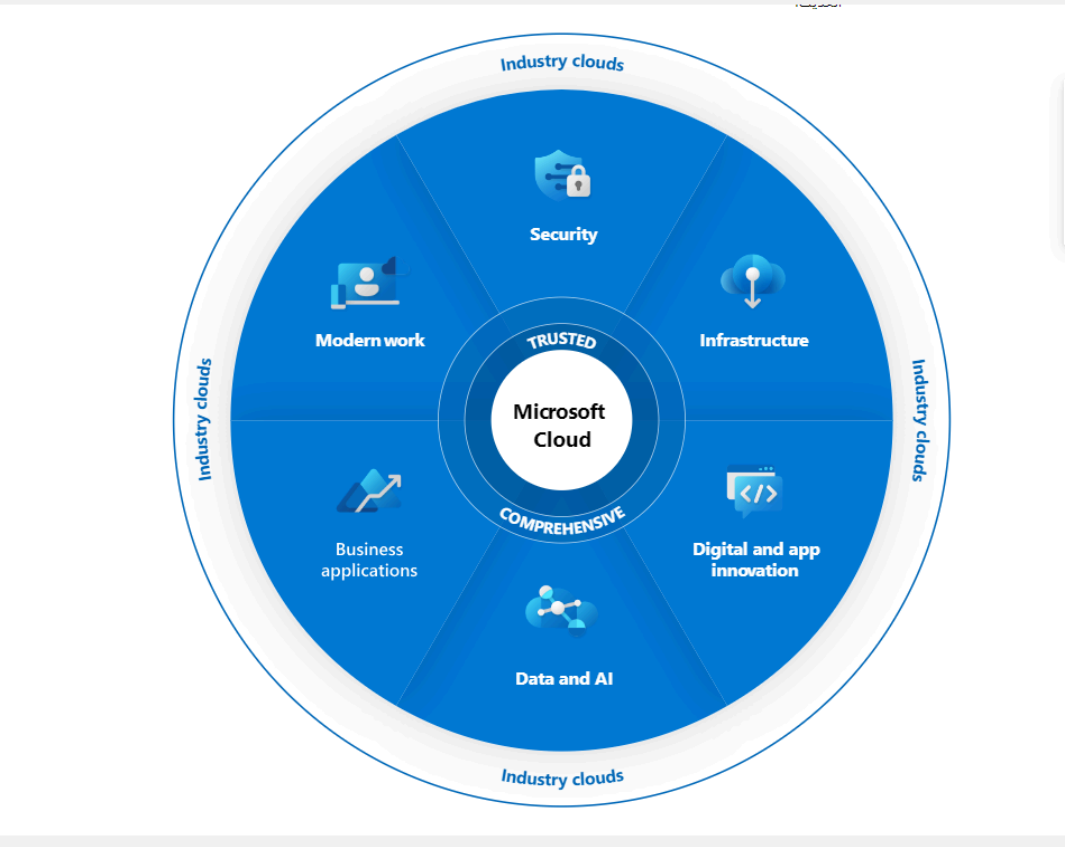
Azure is a cloud computing platform [3] and web portal that lets you use and control Microsoft's cloud resources and services. These resources and services include storing and changing your data according to your needs[3]. All that's required to access these resources and services is the ability to connect to the Azure portal and an active internet connection.[3]

Things that you should know about Azure:

- It was launched on February 1, 2010, significantly later than its main competitor, AWS.[3]
- It’s free to start and follows a pay-per-use model, which means you pay only for the services you opt for.[3]

- Interestingly, 80 percent of Fortune 500 companies use Azure services for their cloud computing needs.[3]
- Azure supports multiple programming languages, including Java, Node Js, and C#.[3]
- The quantity of data centers Azure has all across the globe is another advantage. The most data centers of any cloud platform are found on Azure, which has 42 data centers worldwide. Additionally, Azure plans to add 12 more data centers, bringing the total number of data centers to 54 shortly.[3]

Methodology : (For Microsoft Azure)



*part1:Understanding Cloud Computing Definitions

1. What is cloud computing??

The cloud computing is the delivery services of computing including servers, storage, databases, networking, software, analytics, and intelligence over the internet that offer faster innovation, flexible resources, and economies of scale.[4] You just pay only for cloud services you use pay-per-use,by helping you reduce your operating costs, run your infrastructure more efficiently way, and scale as your business needs change.[4]

2. Benefits and characteristics :

Cloud computing is a big shift from the traditional way businesses think about IT resources.[4] Here are seven common reasons organizations are turning to cloud computing services:

- **Cost:**
  - Businesses can reduce their IT expenses by migrating to the cloud [4]. This is because cloud computing reduces the capital cost of purchasing hardware and software as well as the setup and maintenance of on-site data centers, which include the need for IT specialists to manage the infrastructure, servers arranged in racks, and continuous electricity for power and cooling. It quickly accumulates.[4]

- **Speed:**
    - Because most services for the cloud computing are self-service and also on-demand too, large amounts of resources of the computer can be delivered in minutes, typically with just only a few mouse clicks. Businesses can make their stress less related to the capacity planning because to this flexibility. [4]

- **Global scale:**
    - One advantage of cloud computing services is their elastic scalability. This means, in terms of cloud terminology, that the right amount of IT resources like different processing, storage, and bandwidth capacities are made available at the correct time from the right place.[4]

- **Productivity:**
    - Onsite data centers typically require a lot of “racking and stacking”—hardware setup, software patching, and other time-consuming IT management chores. Cloud computing removes the need for many of these tasks, so IT teams can spend time on achieving more important business goals.[4]

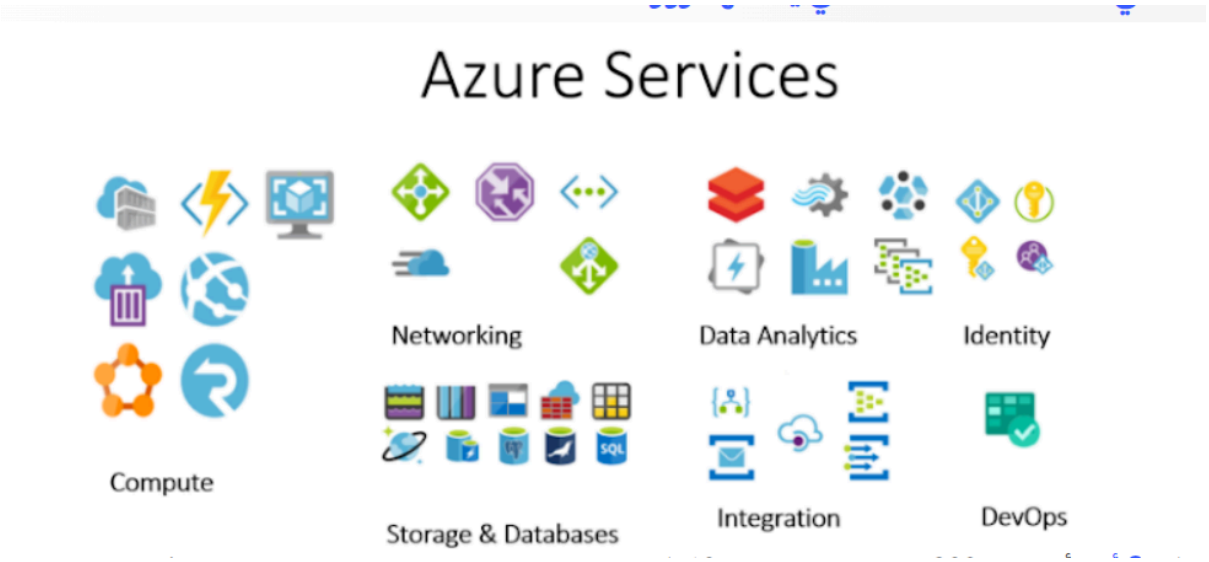
- **Performance:**
    - The largest cloud computing services are powered by a global network of safe data centers that are updated frequently with the newest models of quick and powerful computer gear. Compared to a single corporate data center, this provides a number of advantages, including increased economies of scale and decreased network latency for applications.[4]

- **Reliability:**

- Cloud computing reduces costs and helps data backup, disaster recovery, and business continuity by allowing data to be duplicated at several redundant sites on the network of the cloud provider.[4]

- **Security:**
  - Several cloud service providers provide a wide range of technologies, rules, and controls that improve your overall security posture [4] and shield your infrastructure, data, and apps from dangers.[4]

3. Cloud services: IaaS, PaaS, and SaaS, serverless:



The mostost cloud computing services specified in 4 categories in Microsoft Azure: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), serverless. These services sometimes called the cloud computing "stack" because they build on the top of one of each other.[4] Knowing what they are and how they're different makes it easier to achieve your business goals.[4]

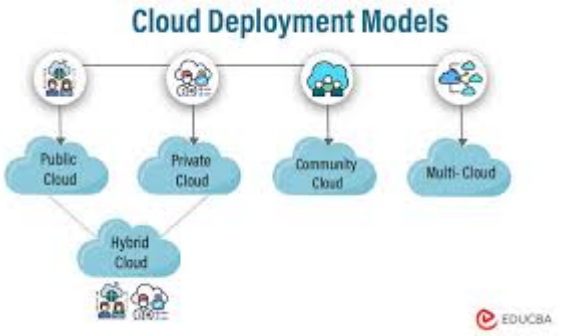
- **IaaS:**
  - The most important and basic category of the cloud computing services. With infrastructure as a service (IaaS) [4], you rent IT infrastructure servers and virtual machines (VMs), storage, networks, and operating systems(OS) from a cloud service provider(CSP) on a pay-as-you-go or pay-per-use basis.[4]

- **PaaS:**
  - The (PaaS) Platform as a service [4] is called to the cloud computing services that it provides the on-demand environment for improving, developing,upgrading, testing, delivering, and managing software applications. its designed to make it simple and easier for the developers to create the web or mobile apps quickly and without being worried about set up or manage the underlying infrastructure of servers, storage, network, and databases needs for the development.[4]

- **SaaS:**
  - Software as a service (SaaS) [4] is the method for delivering software applications through the Internet, on-demand, and typically on subscription basis. With it the cloud service providers(CSP) host and manage the software application and underlying infrastructure, and handle any maintenance or improvement, like software upgrades, updates and security patching. Users connect to the application throught the internet, that it always with a web browser on their phone, tablet, or PC.[4]

- **Serverless computing:**
    - Interfere with PaaS,the serverless computing focuses on building applvation functionality without spending or wasting time continually managing the servers and infrastructure required to do so. The cloud services provider(CSP) handles the setup, capacity planning, and server management for the users. Serverless architectures are highly scalable and event-driven, its only using resources when a specific function or trigger occurs.[4]

4. Deployment Model:



There are three different ways to deploy the cloud services: on a public cloud, private cloud, or hybrid cloud.[4]

- **Public cloud:**
  Third-party cloud service providers, who supply computing resources such servers and storage via the Internet, own and run public clouds [4]. One instance of a public cloud is Microsoft Azure.[4] The cloud provider owns and manages all of the hardware, software, and other supporting infrastructure in a public cloud. A web browser is used to manage your account and access these services. [4]

- **Private cloud:**
  A single company or organization's exclusive use of cloud computing resources is referred to as a private cloud [4]. The on-site data center of the business may house a private cloud. Additionally, some

businesses pay outside service providers to host their private clouds.[4] A private cloud is one where the infrastructure and services are kept up to date on a private network.[4]

- **Hybrid cloud**
  Public and private clouds are combined in hybrid clouds [4], which are connected by a system that permits data and applications to be exchanged between them.[4] A hybrid cloud allows your company more deployment options and flexibility by enabling data and apps to migrate between private and public clouds. It also helps to optimize your current infrastructure, security, and compliance.[4]

5. **how cloud computing aligns with TechSolutions Inc.'s business objectives and IT requirements.**

   business objectives and IT requirements that cloud computing aligns with :

   - **Accessibility:**

     A technical requirement known as accessibility aims to provide technology, software, or services that are usable and accessible to all users.[6] One type of accessibility technical requirement is the addition of closed captions for users who are deaf or hard of hearing in tutorial videos.[6]

   - **Authentication and authorization:**

     This is a technical specification that demands an authentication and authorization policy to be followed by a system.[6] Authorization gives

people permission to access data, whereas authentication evaluates the validity of the data.[6]

- **Availability:**

  A technical requirement that works more like a metric is availability.[6] This measure confirms how long a program or resource is accessible to users and measures time as a percentage.[6]

- **Data quality:**

  A technical required known as "data quality" describes information and data that meet specific standards.[6] High-quality data that you can utilize for operational and decision-making procedures is what you want ideally.[6]

- **Human error:**

  It is technically necessary for software to be able to recognize when users have entered false information.[6] The software alerts the user and suggests that they correct the disparity if it finds this problem.[6]

- **Information security:**

  The encryption and security of user credentials and private information within an online storage base or transit system are the subject of this technical requirement.[6] Highly classified material would also need to be encrypted in order to maintain this level of security.[6]

- **Internal controls:**

Due to technical internal controls, only specific users are able to access the decryption keys for highly classified and encrypted user data.[6] These people, known as data stewards, are only able to access the data with permission from a higher authority.[6]

- **Interoperability:**

  According to the technical criteria for interoperability, software must provide complete compatibility.[6] This implies that it must function on all popular web browsers, operating systems, and gadgets. Customers' technological needs may determine how these criteria are implemented.[6]

- **Maintainability:**

  Software must, in essence, be maintainable in terms of its integrity.To put it another way, a system must recognize and address technical issues within a predetermined amount of time. The majority of repairs may be finished in an hour or less.[6]

- **Performance:**

  The average wait times and page or program loading times are set by the performance technical requirement.[6] Setting a technical requirement that load times not exceed two seconds, for instance, is recommended practice.[6]

- **Privacy:**

  Protecting sensitive customer data from internal data experts and staff is referred to as privacy.[6] Employees might not be able to see a customer's social security number that is kept in a customer database, for instance, due to privacy technical requirements.[6]

- **Productivity:**

  The processes that enable users to be more productive are referred to as productivity technical requirements.[6] One way to avoid having users enter data repeatedly is to develop a system that creates data automatically.[6]

- **Reliability:**

  The average amount of time that a software or system functions between malfunctions or outages is referred to as reliability.[6] This statistic calculates the average time for services and apps that are essential to business operations.[6]

- **Serviceability:**

  Because most software and systems experience frequent upgrades or modifications, serviceability is a crucial technical need.[6] According to this technological requirement, when software is updated or changed, systems cannot be completely shut down.[6]

- **Standards:**

  Because most software and systems experience frequent upgrades or modifications, serviceability is a crucial technical need.[6] According to this technological requirement, when software is updated or changed, systems cannot be completely shut down.[6]

- **System errors:**

  This technical requirement results in an error code that alerts the user to a disparity in the system.[6] The error code is recorded in a help database, assisting the user in quickly resolving the issue.[6]

- **Vendor lock-in:**

  A technical prerequisite for open-sourced software or systems is vendor lock-in.[6] Open-sourced software is available for any user to modify using their own custom code and is not owned by a proprietary or private corporation.[6]

So to Empowering Businesses and IT requirements with Azure:
Because Azure enables businesses of all sizes to avoid the capital and operating costs associated with maintaining physical servers, the platform is having a significant influence on business.[5] Here's how to do it:

- **Flexibility & Scalability:**

  Applications can be scaled by Azure to meet customer demand.[5] Without incurring any capital costs, businesses may quickly scale up and down their resource usage and just pay for what they use.[5]

- **Speed & Efficiency:**

  Azure is incredibly flexible, which enables rapid application deployment and shorter time to market.[5] Businesses can adopt a software delivery strategy that is quicker, more effective, and more iterative by utilizing platform services such as Azure DevOps.[5]

- **Analytics & Intelligence:**

  Azure enables enterprises to get meaningful insights from vast amounts of data. They provide a range of intelligence services, including stream analytics, data lake analytics, and machine learning.[5] Disaster Recovery: To avoid data loss and downtime, Azure comes with built-in disaster recovery features. It makes sure companies don't need to make large capital expenditures to have a dependable disaster recovery solution.[5]

Also Microsoft Azure offers AI solutions services ：

Service	Description
Anomaly Detector (retired)	Identify potential problems early on.[7]
Azure AI Search	Bring AI-powered cloud search to your mobile and web apps.[8]
Azure OpenAI	Perform a wide variety of natural language tasks.[9]
Bot Service	Create bots and connect them across channels.[10]
Content Moderator (retired)	Detect potentially offensive or unwanted content.[11]
Content Safety	An AI service that detects unwanted content.[12]
Custom Vision	Customize image recognition for your business.[13]

Document Intelligence	Turn documents into intelligent data-driven solutions.[14]
Face	Detect and identify people and emotions in images.[15]
Immersive Reader	Help users read and comprehend text.[16]
Language	Build apps with industry-leading natural language understanding capabilities.[17]
Language understanding (retired)	Understand natural language in your apps.[18]
Metrics Advisor (retired)	An AI service that detects unwanted content.[19]
Personalizer (retired)	Create rich, personalized experiences for each user.[20]
QnA maker (retired)	Distill information into easy-to-navigate questions and answers.[21]

Speech	Speech-to-text, text-to-speech, translation, and speaker recognition.[22]
Translator	Use AI-powered translation technology to translate more than 100 in-use, at-risk, and endangered languages and dialects.[23]
Video Indexer	Extract actionable insights from your videos.[24]
Vision	Analyze content in images and videos.[25]

---

*part2:Assessing Cloud Computing Security

Security challenges and concerns:

There are the following security challenges and concerns:

- Cloud computing is a collection of different technologies which make client data vulnerable to threats. [26]
- Threats often happen because of legal and regulatory issues and the involvement of a third party. [26]
- The benefits of cloud computing must be weighed against the security concerns through a risk management approach. [26]

The 7 Security Risks of the Cloud Computing are:

1. Malicious malware [36]
2. Limited visibility into network
3. Compliance issues[36]
4. Data loss[36]
5. Data breaches[36]
6. Account hijacking[36]
7. Insider threats[36]

Cloud Computing Risks:

The responsibilities and methods for putting governance into practice and monitoring it are altered by cloud computing.[26] Four management domains can be used to sum up cloud computing risks:

1. **Governance management risk.[26]**

- Inadequate cloud system integration, even throughout the same company.[27]
- redundant work or information across many organizational divisions.[27]
- incompatibility of cloud systems with organizational objectives.[27]
- Novel security concerns: the possibility of utilizing cloud systems with inadequate or nonexistent access control.[27]

2. **Enterprise management risk.[26]**

   It can include things like[28]:
   - protecting confidential information,
   - adhering to legal requirements,
   - preventing financial fraud, and
   - guaranteeing worker safety.

   Risk might come from external sources like natural disasters or internal ones like equipment failures.[28]

3. **Information management risk.[26]**

- **hardware and software failures** you may need IT expert assistance or to purchase a new computer to continue business operations[29]
- **Malware** malicious software designed to disrupt computer operation[29]
- **Viruses** codes that can spread from 1 computer to another, disrupting computer operations (e.g. sent through emails)[29]
- **spam, scams, and phishing** unsolicited contact that fool people into giving personal details or buying fake goods[29]
- **human error** accidentally opening an email containing viruses, incorrect data processing, or careless data disposal[29]
- **natural disasters** floods, storms, and bush fires may interrupt service within the business or to external suppliers (e.g. NBN, electricity).[29]

4. **Information security.[26]**

- The purpose of confidentiality measures is to stop information from being disclosed without authorization(id and passwor).[30] The confidentiality principle is to protect the privacy of personal information and guarantee that only those individuals have visibility and access to it who require it to carry out their job duties.[30]
- Protection against illegal data changes (additions, deletions, revisions, etc.) is a component of integrity consistency. The integrity principle guarantees that information is correct and trustworthy and is not altered inadvertently or intentionally into error.[30]
- The safeguarding of a system's capacity to provide data and software systems at a user's request (or at a predetermined time) is known as availability.[30] Making technological infrastructure, applications, and data accessible when needed for internal business operations or for external clients is the aim of availability.[30]

Data Breaches :

82% of data breaches are cloud based!!!!

For businesses using the cloud, data breaches are still a major worry.[33] Sensitive information may be stolen, gained illegal access to, or exposed due to a data breach, which could have disastrous effects on one's finances and reputation.[33] To reduce the risks associated with data breaches, organizations must prioritize data security by putting in place robust access controls, encryption, and data loss prevention measures.[33]

What is a data breach?

A cyberattack in which illegal access to or disclosure of private, sensitive, or otherwise protected data occurs is known as a data breach. [34] Any type of organization, from small startups to large conglomerates, is susceptible to data breaches.[34] They could include trade secrets, personally identifiable information (PII), personally health information (PHI), or other private information.[34]Personal data, such as credit card numbers, driver's license numbers, Social Security numbers, and medical records, as well as company data, including client lists and source codes, are frequently exposed in data breaches.[34]

- The current technological environment causes data owners to remain concerned about their data, even in spite of the CSP's best efforts to establish a comparatively solid security foundation. [26]

- The CSA study collected the most critical cloud computing security flaws or issues that result in various attacks:
    - ○ Identity spoofing
    - ○ Data repudiation
    - ○ Information leakage
    - ○ Denial of service
    - ○ Privilege elevation. [26]

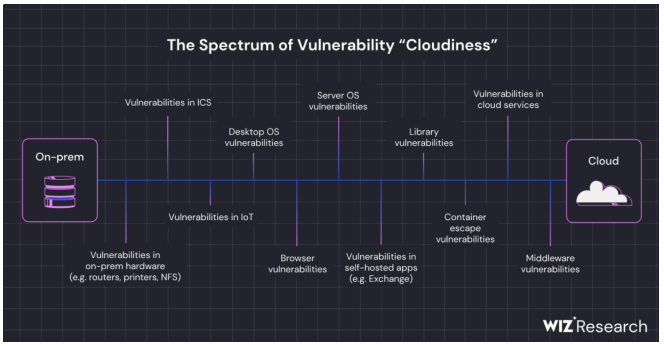
- Data breaches are the most prevalent in cloud computing.[26]
- Data breach threats lead to three main violations:

    - ○ **Data privacy violations:**
      A privacy breach happens when someone accesses another person’s personal information without his or her permission.[41] It is very similar to a data breach, which happens when someone accesses information without authorization. Many people use the two terms interchangeably, but there is a difference in terms of what information is illegally accessed. [41]
      A *privacy breach* specifically refers to breaches that target information about people.[41]

    - ○ **Data confidentiality violations:**

    - ○ Data integrity violations[26]

Vulnerability:



Cloud vulnerabilities are openings or flaws in a cloud computing system that hackers can use to obtain illegal access, steal information, or interfere with operations[35]. any weakness in an information system, system security operations, central administration,[26] or application that could be misused or controlled by a remote attacker.

There are four types of vulnerabilities linked to data breaches:

- **Data Storage Cryptography Vulnerabilities.[26]**
  When an application uses outdated, poorly designed cryptographic algorithms to encrypt data or fails to encrypt important data,[37] it creates an insecure cryptographic storage vulnerability.[37] Inadequate cryptographic algorithm design can involve using the wrong ciphers, using a shoddy encryption technique, and managing keys badly.[37]

    - Poor key management [26]
    - Faulty, insecure encryption technique [26]

- **Data Access Vulnerabilities.[26]**
  Vulnerabilities or weaknesses in a system's implementation, configuration, or design that permit unauthorized users to access, alter, or exfiltrate data are referred to as data access vulnerabilities.[38] These weaknesses can occur in a number of an information system's constituent parts, such as hardware, apps, databases, and network infrastructure.[38]

    - Unauthorized access to insiders and outsiders

- **Data Storage Location, Backup, and Recovery Vulnerabilities [26]**
  The process of backing up and recovering data involves making duplicate copies of it, keeping it safely in case of loss or damage[39], and then restoring it to either the original location or a secure backup copy so that it can be utilized for operations once more.[39]

    - Data integrity and availability
    - Information disclosure and data loss
    - Loss of control, data locality, and multi-location.[26]

- **Data Sanitization Vulnerabilities.[26]**

  Purposefully erasing or destroying data from a storage device in order to assure that it cannot be recovered is known as data sanitization.[40] Data deletions from storage media typically leave the media unintentionally unerased, leaving it vulnerable to recovery by an attacker with physical access to the device.[40]

    - Information disclosure [26]

CSA Ensuring general security: shared responsibility model

The Clery Act classifies a person as a campus security authority, or CSA.[32] A crucial component of gathering information for the yearly safety and security report is CSAs.[32]

For cloud clients and CSPs alike, the nonprofit Cloud Security Alliance (CSA) develops a shared responsibility paradigm. [26]

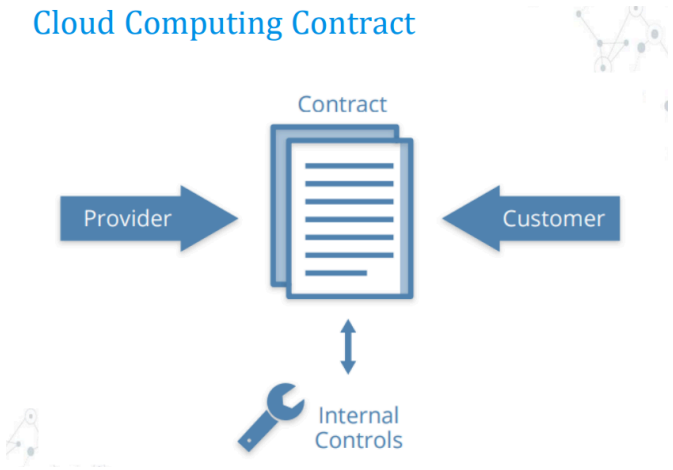
The shared responsibility model is a fundamental aspect of cloud security.[42] While CSPs secure the cloud infrastructure, customers must ensure the security of their workloads, applications, and data.[42] Tools like Tufin can help manage these responsibilities effectively, ensuring a robust security posture in the cloud.[42]

The CSP is in charge of:

- Maintaining records of client and internal security measures Developing and implementing such policies via the Consensus Assessments Initiative Questionnaire (CAIQ) instrument.[26]

The cloud client is responsible for:

- Documenting who implements controls.[26]
- Using the Cloud Controls Matrix (CCM) tool to track duties.[26]



CSA creates a process model for cloud security management.

Despite the notable variations that may arise when developing a cloud project, as illustrated in Figure 1, CSA has created a rather straightforward and high-level process model for cloud security management[31]. Finding the needs first, creating the architecture design next, and determining the gaps based on the capabilities of the underlying cloud platforms are the keys to successfully implementing the model.[31]

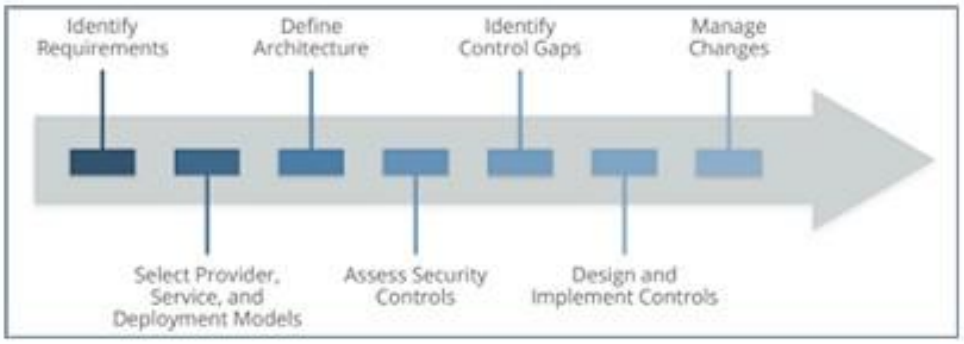


Fig. 1. CSA Process Model for Cloud Security Management [7]

The security measures the cloud computing provides:

Security Countermeasures

are methods, actions, devices, procedures, or techniques that reduce or prevent threat, vulnerability, or attack by minimizing the harm it can cause. [26]

Such as:

1. Encryption and Key Management [26] (privacy and confidentiality).
2. Data Classification and Access Control [26](authentication, authorization and confidentiality).
3. Digital Signature and hashing[26]
4. Trust Framework [26]
5. Data Integrity and Availability[26](integration)
6. Identity and Access Management [26]
7. Intrusion Detection and Prevention System [26]
8. Location, Backup and Recovery Transparency [26]
9. Data Sanitization[26]

For me as Azure service provider i have (R&D) research and department wich always explore the best available technology (BAT) in different security schemes and algorithm .

Evaluation toAzure Security Measures for TechSolutions Inc.

1. Azure Active Directory (AAD)

The security measures for Azure Active Directory (AAD) are:

- Strong user identity and access authorization control is offered by Identity and Access control (IAM).[43]
- Using a single set of login credentials, users can access various applications through Single Sign-On (SSO).[43]
- By demanding additional verification processes, Multi-Factor Authentication (MFA) provides an additional layer of protection.[43]

Suitability for TechSolutions Inc.:

- Strong access controls are required, and AAD's IAM features guarantee that only authorized individuals may access sensitive data.[43]
- SSO enhances user experience without sacrificing security, which makes it appropriate for the operational effectiveness of the business.[43]
- By enhancing security against unauthorized access, MFA reduces the possibility of a data breach.[43]

2. Azure Security Center

Azure Security Center Security Measures:

- Real-time security status monitoring of cloud resources through continuous security assessment.[43]
- Advanced Threat Protection: Makes use of analytics and machine learning to identify and neutralize threats.[43]
- Compliance management: Offers resources and analyses to guarantee adherence to rules and guidelines in the sector.[43]

Suitability for TechSolutions Inc.:

- Maintaining the security posture of the organization's cloud infrastructure depends on the timely identification of vulnerabilities made possible by continuous security assessment.[43]
- TechSolutions Inc.'s data and applications must be protected against sophisticated cyber threats, and this requires advanced threat protection.[43]
- By lowering legal risks, compliance management solutions assist the business in meeting regulatory and industry standards.[43]

3. Encryption and Key Management

Security Measures for Key Management and Encryption:

- Azure Key Vault: Safely keeps and organizes certificates, secrets, and cryptographic keys.[43]
- Encryption: Using industry-standard protocols, encryption is provided for data both in transit and at rest.[43]

Suitability for TechSolutions Inc.:

- The company's need for strong key management procedures is met by Azure Key Vault, which guarantees the secure management of encryption keys.[43]
- Sensitive information is shielded from unwanted access via encryption of data while it is in transit and at rest, satisfying the company's requirements for privacy and confidentiality.[43]

4. Data Classification and Access Control

Security Measures for Data Classification and Access Control

- Role-Based Access Control (RBAC): This technique enforces least privilege access by allocating permissions according to user roles.[43]
- Tools for classifying data according to its sensitivity levels are known as data classification.[43]

Suitability for TechSolutions Inc.:

- Strict access restrictions can be implemented with the use of RBAC, guaranteeing that users have access to the data required for their responsibilities and boosting security.[43]
- Effective data governance requires the organization to manage and safeguard data based on its level of sensitivity, which is made possible by data classification technologies.[43]

5. Intrusion Detection and Prevention

Security Measures for Intrusion Detection and Prevention:

- Azure Sentinel uses SIEM capabilities to provide threat detection and incident response.[43]
- Defense against Distributed Denial of Service (DDoS) attacks is provided by Azure DDoS Protection.[43]

Suitability for TechSolutions Inc.:

- The powerful threat detection capabilities of Azure Sentinel aid in the identification and response to security problems, guaranteeing that the business can quickly reduce possible threats.[43]
- In line with the demand for high availability and dependability by the organization, DDoS defense safeguards services from attacks that could interfere with regular business operations.[43]

6. Compliance and Legal Considerations

Security Measures for Compliance Issues and Legal

- Compliance Certifications: HIPAA, GDPR, ISO/IEC 27001, and other important industry standards are all met by Azure.[43]
- Tools for Compliance: offers instruments and resources to assist companies in staying in compliance with applicable laws.[43]

Suitability for TechSolutions Inc.:

- The platform satisfies strict security and privacy standards thanks to Azure's numerous compliance certifications, which is essential for preserving stakeholder and client trust.[43]
- TechSolutions Inc. uses compliance technologies to improve overall governance, lower the risk of non-compliance penalties, and comply with legal and regulatory obligations.[43]

---

*part3:Implementing Data Security in Cloud Computing

Data Security Strategy for TechSolutions Inc.'s Cloud Data Processing

I will create a strong data security plan as an Azure team member for TechSolutions Inc.'s cloud data processing. Taking into account the particular requirements specified in the project requirements, this strategy will fulfill the three main requirements for data security: integrity, confidentiality, and privacy.

1. Privacy

Goal: Ensure that client's critical data is not disclosed to unauthorized individuals or processes.[26]

Azure Solutions:

- Use industry-standard encryption techniques (AES-256) to safeguard virtual machine disks with Azure Disk Encryption. By doing this, data that is at rest is shielded from unwanted access.[44, 43]
- Azure Key Vault: With hardware security modules (HSMs) in place to protect them, store and manage cryptographic keys, secrets, and certificates. Access control and secure key management are therefore guaranteed..[44, 43]
- Azure Information Protection: Use Azure Information Protection to label, categorize, and safeguard confidential data. Applying policies that stop data loss and unlawful sharing is made easier with the use of this tool..[44, 43]

2. Confidentiality

Goal: Ensure that client data is used only for authorized purposes and is not accessed by unauthorized entities.[26]

Azure Solutions:

- Manage who has access to Azure resources by using role-based access control, or RBAC. RBAC makes sure that, according to their positions within the company, only authorized individuals can see and edit data.[44, 43]
- Utilize Azure Active Directory (AAD) to provide thorough identity and access control, guaranteeing safe and legal access to data and applications. To improve user authentication, use AAD to provide multi-factor authentication (MFA).[44, 43]

- Utilize Azure Confidential Computing to process data in secure, isolated settings while maintaining data confidentiality throughout the processing process.[44, 43]

3. Integrity

Goal: Ensure that client's critical data is not altered or destroyed without authorization.[26]

Azure Solutions:

- Azure SQL Database and Azure Storage Integrity Checks: To protect data integrity in Azure SQL Databases and storage accounts, activate capabilities like Advanced Threat Protection and Transparent Data Encryption (TDE).[44, 43]
- Utilize Azure Monitor and Log Analytics to set up alarms and logs for ongoing resource activity monitoring. Data integrity can be ensured by tracking and analyzing changes to the data using Log Analytics.[44, 43]
- Azure Security Center: Make use of Azure Security Center to evaluate and track security posture over time, offering suggestions and automated reactions to integrity breaches.[44, 43]

TechSolutions Inc. may successfully secure its data in the Azure cloud environment by concentrating on these three crucial factors: integrity, confidentiality, and privacy. By protecting data against unwanted access and manipulation, this approach complies with IT regulations and the business goals of the organization.

Data Classification and Lifecycle Management

Importance:

- **Data Classification:** Data classification in cloud security assists an organization in understanding the value of its data, determining if the data is under threat, and implementing measures to limit risks.[46] It serves as the foundation for an organization's effective data security and data management programs. [46]
- Data classification allows organizations to properly manage, secure, and control their data resources by providing classification levels, which we will

discuss in detail later.[46] These levels allow businesses to implement security measures that are specific to the needs of each data type.[46]

(it enables the company to publish open data and closed data)

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. [26]

○ Organizations can prioritize resources and apply security measures to each data category's requirements.[26]

Data can be classified into three levels:

○ Primary (non-sensitive data) [26]

○ Confidential (personal information) [26]

○ Highly confidential, stored data (financial, political, Health).[26]

Data classified using:

1. Advanced algorithms to scan and analyze data, matching it to the defined categories based on data attributes. [26]

2. Manual classification[26]

- **Lifecycle Management:** Data lifecycle management has several important benefits which include:

- **Process improvement:** Data plays a crucial role in driving the strategic initiatives of an organization. DLM helps maintain data quality throughout its

lifecycle, which in turn enables process improvement and increases efficiency. [47]A good DLM strategy ensures that the data available to users is accurate and reliable, enabling businesses to maximize the value of their data.[47]

- **Controlling costs:** A DLM process places value on data at each stage of its lifecycle. Once data is no longer useful for production environments, organizations can leverage a range of solutions to reduce costs such as data backup, replication and archiving. [47]For example, it can be moved to less-costly storage located on-premises, in the cloud, or in network attached storage.[47]

- **Data usability:** With a DLM strategy, IT teams can develop policies and procedures that ensure all metadata is tagged consistently so it can improve accessibility when needed.[47] Establishing enforceable governance policies ensures the value of data for as long as it needs to be retained. The availability of clean and useful data increases the agility and efficiency of company processes.[47]

- **Compliance and governance:** Each industry sector has its own rules and regulations for data retention, and a sound DLM strategy helps businesses remain compliant. DLM lets organizations handle data with increased efficiency and security, while maintaining compliance with data privacy laws regarding personal data and organizational records.[47]

Cloud-Native Security Services and Tools

Azure Native Services:

For more tools please check the link below:

https://learn.microsoft.com/en-us/azure/security/fundamentals/overview[45]

- **Microsoft Sentinel** [45]

Microsoft Sentinel is a cloud-native, scalable solution for security orchestration, automation, and response (SOAR) and security information and event management (SIEM).[45] Offering a unified solution for attack detection, threat visibility, proactive hunting, and threat response, Microsoft Sentinel provides intelligent security analytics and threat data throughout the organization.[45]

- **Microsoft Defender for Cloud** [45]

  Microsoft Defender for Cloud gives you more insight into and control over the security of your Azure resources, enabling you to stop, identify, and react to threats. It integrates with a wide range of security solutions, helps identify risks that could otherwise go undetected, and offers integrated security monitoring and policy administration across all of your Azure subscriptions.[45]

  Additionally, Defender for Cloud assists with security operations by giving you access to a single dashboard that presents recommendations and alerts for instant action. Frequently, you only need to click once in the Defender for Cloud panel to fix problems. [45]

- **Azure Resource Manager** [45]

  The security of solutions delivered in Azure is enhanced by Azure Resource Manager template-based deployments, which may be integrated with typical security control settings.[45] By doing this, the possibility of security configuration mistakes occurring during manual deployments is decreased.[45]

- **Application Insights** [45]

  Application Insights is a web developer-focused Application Performance Management (APM) service that is expandable. You can automatically identify performance abnormalities and monitor your live web apps using Application Insights. It has strong analytics capabilities to assist you in troubleshooting and comprehending how users interact with your apps.[45] It keeps an eye on your application at all times, both while you're testing it and once you've published or deployed it.[45] You are able to identify the root cause of any crashes, malfunctions, or performance problems by thoroughly searching through the telemetry data. Additionally, the service notifies you through email whenever your app's functionality or availability changes. Thus, Application

Insight becomes an important security tool as it aids in availability, confidentiality, and integrity.[45]

- **Azure Monitor** [45]

  Azure Monitor provides data visualization, querying, routing, alerting, auto scaling, and automation on data from each individual Azure resource (Resource Logs) as well as the Activity Log from the Azure subscription.[45] Azure Monitor is a useful tool for receiving alerts about security-related events found in Azure logs.[45]

- **Azure Monitor logs** [45]

  Azure Monitor logs offers an IT management solution for Azure resources as well as cloud-based infrastructure from third parties (like AWS) and on-premises.[45] Azure Monitor data may be seamlessly routed to Azure Monitor logs, allowing you to view metrics and logs for your whole environment in one location.[45]

- **Azure Advisor** [45]

  The security suggestions that Azure Advisor offers can greatly enhance your overall security posture for any solutions you choose to implement in Azure.[45] These suggestions are derived from security research carried by Microsoft Defender for Cloud.[45]

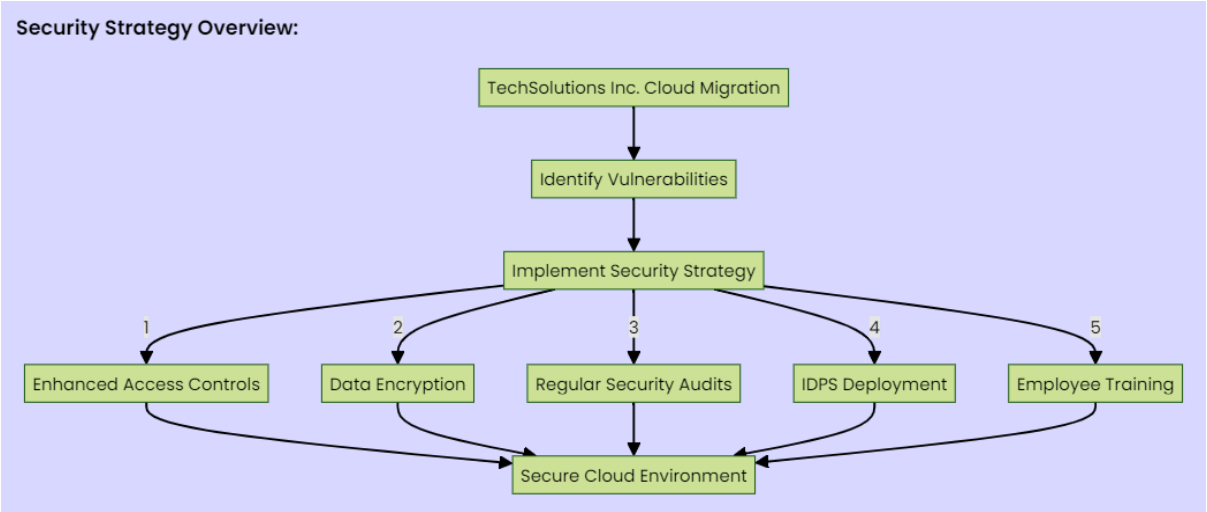
- **Azure Firewall** [45]

  Azure Firewall is an intelligent network firewall security solution that is cloud-native and offers threat protection for your Azure cloud workloads.[45] It is a fully stateful firewall as a service that offers limitless cloud scalability and high availability right out of the box. It offers traffic inspection in both directions: east-west and north-south.[45]

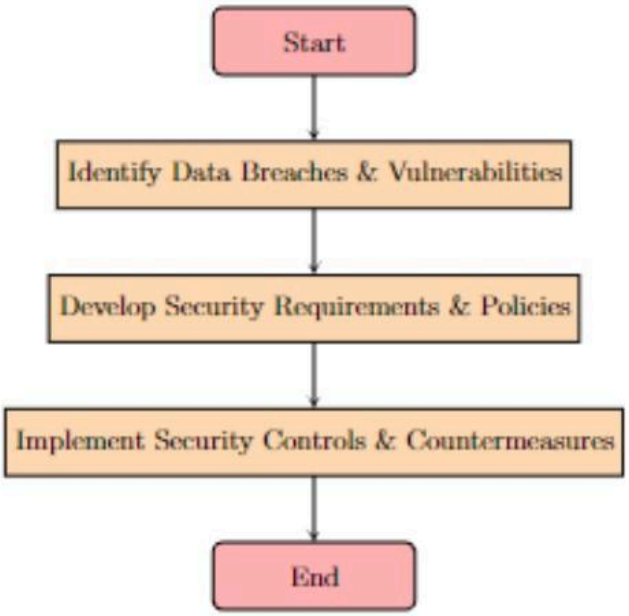
---

*part4:Address data breaches, vulnerabilities, and security requirements:

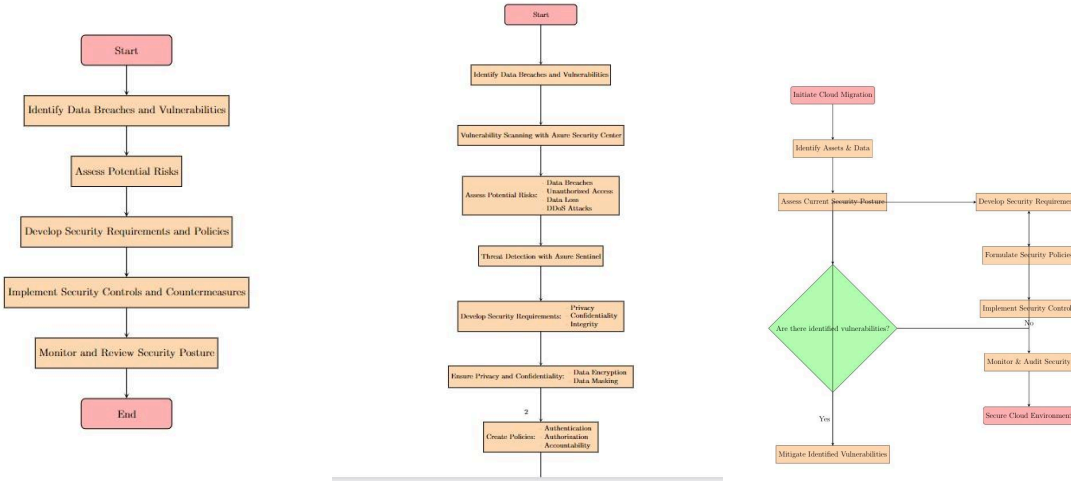
Security strategy overview:



In basic way:



More details on the flowchart**:**



Azure integration:

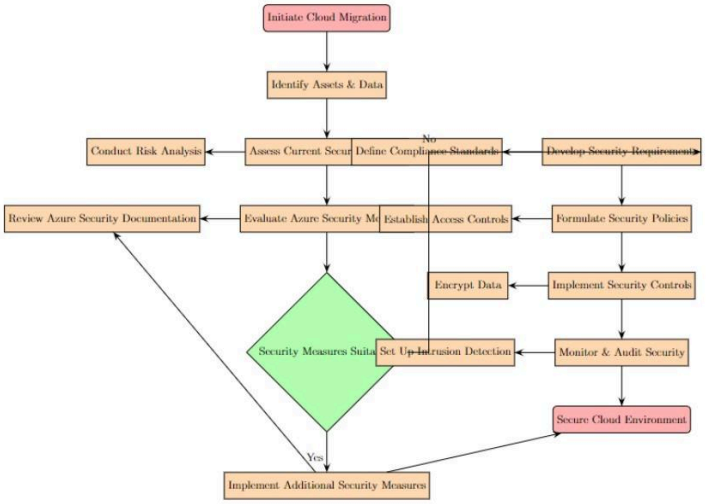


Figure 1: Security Proposal Overview with Azure Integration

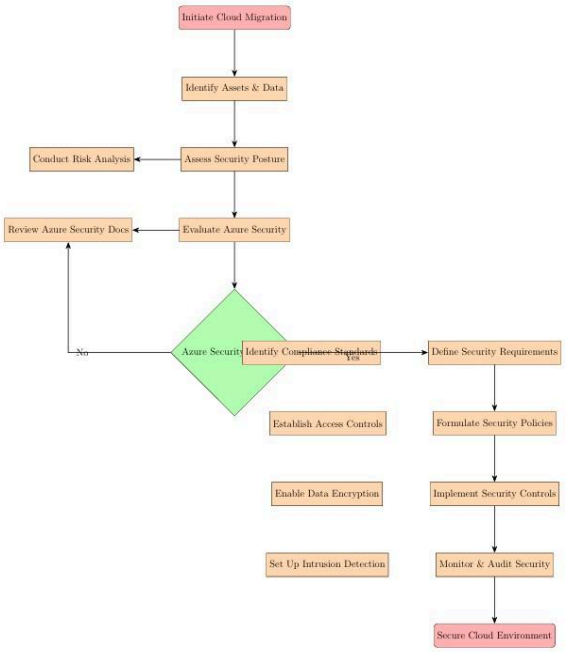
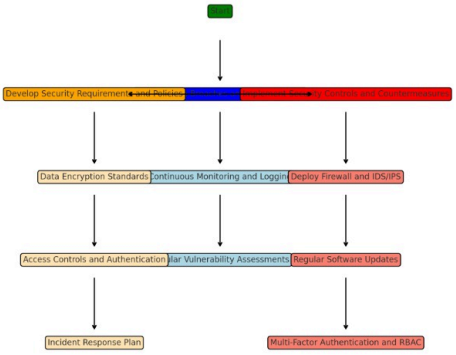


Figure 1: Security Proposal Overview with Azure Integration



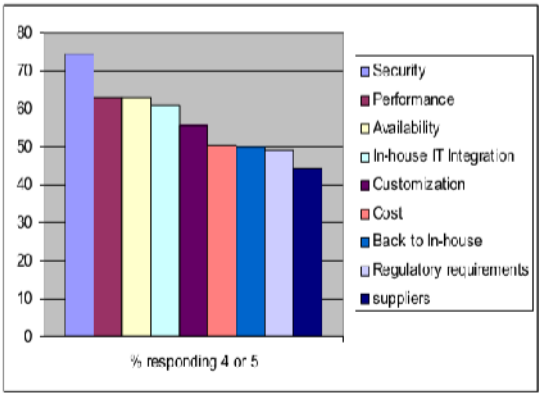


Fig 2. Graph depicting the concerns of clients on cloud computing issues

Fig. 2 depicts the summary of the survey conductedby us on the basic issues of the cloud computing. The client'sprimary concern is taken in to account. Hence only thepercentage of 4, 5 is being shown.

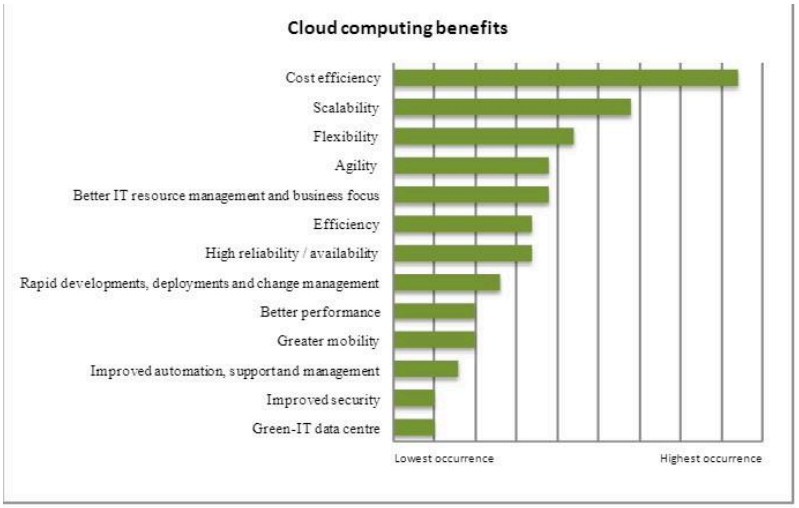


Figure 1. Cloud computing benefits.

Cloud computing benefits are listed in Fig. 1, arranged
from the highest occurrence (therefore cited most in literature)
to the lowest ost efficiency is the main driver for cloud computingadoption. Other primary benefits include scalability, flexibility,agility, better IT resource management and business focus,efficiency, higher reliability and availability, rapiddevelopment, deployment and change management, betterperformance and greater mobility. Improved automation,support and management, improved security, and green-IT datacentres were also cited as valuable drivers for moving to thecloud.

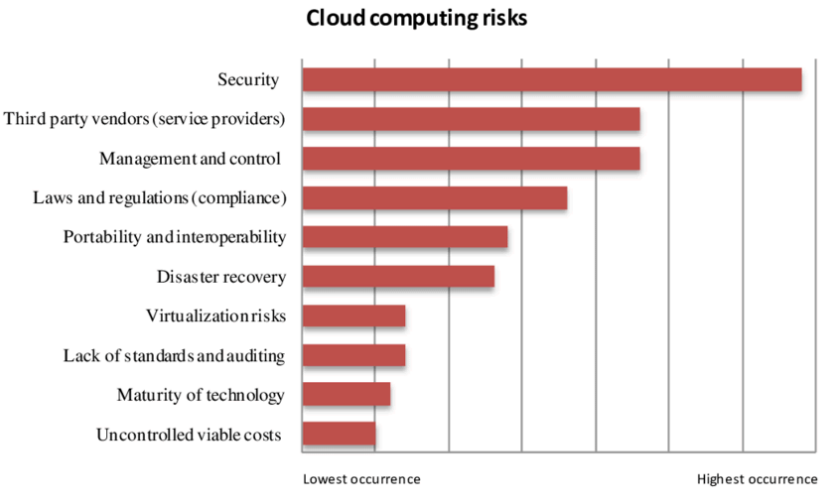


Fig. 2 presents the list of identified risks.According to the literature review, the biggest cloudcomputing concern is security (Fig.2). With applications anddata being hosted by a service provider, data is no longer underthe control of management and prone to vulnerabilities.Hosting application and data in shared infrastructures increasethe potential of unauthorised access and raise concerns such asprivacy, identity management, authentication, compliance,confidentiality, integrity, availability of data, encryption,network security and physical security.

Figure 1 Histogram of business vulnerability categories

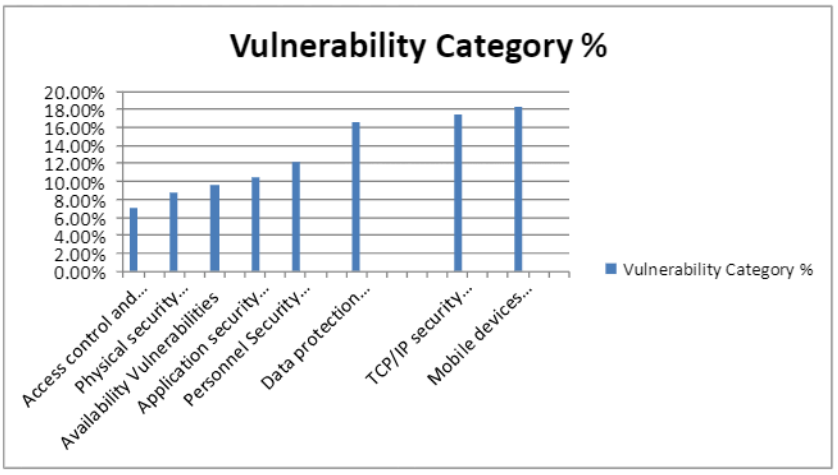


Figure 1 shows the histogram of vulnerability categories chart showing the highest vulnerability category to be the mobility access (BYOD) which is understandable as no specific policy and mechanism have been formally defined yet. According to this figure the large percentage of the is due to Mobile devices vulnerabilities ,TCP/IP security vulnerabilities,Data protection vulnerability .

References:

[1]https://www.researchgate.net/publication/335390319_Cloud_Migration_Strategy_for_Legacy_Systems_using_AWS_Platform

[2]https://www.researchgate.net/publication/354788317_CLOUD_COMPUTING_SECURITY_CHALLENGES

[3]https://www.simplilearn.com/tutorials/azure-tutorial/what-is-azure#what_is_microsoft_azure.

[4]https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds/

[5]Unveiling the Powerhouse: Exploring Microsoft's Azure Cloud Computing Strategy : TechiT Services (techit-services.com)

[6]https://www.indeed.com/career-advice/finding-a-job/technical-requirements

[7]https://learn.microsoft.com/en-us/azure/ai-services/translator/

[8]https://learn.microsoft.com/en-us/azure/search/

[9https://learn.microsoft.com/en-us/azure/ai-services/openai/

[10]https://learn.microsoft.com/en-us/composer/

[11]https://learn.microsoft.com/en-us/azure/ai-services/content-moderator/

[12]https://learn.microsoft.com/en-us/azure/ai-services/content-safety/

[13]https://learn.microsoft.com/en-us/azure/ai-services/custom-vision-service/

[14]https://learn.microsoft.com/en-us/azure/ai-services/document-intelligence/

[15]https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/overview-identity

[16]https://learn.microsoft.com/en-us/azure/ai-services/immersive-reader/

[17]https://learn.microsoft.com/en-us/azure/ai-services/language-service/

[18]https://learn.microsoft.com/en-us/azure/ai-services/luis/

[19]https://learn.microsoft.com/en-us/azure/ai-services/metrics-advisor/

[20]https://learn.microsoft.com/en-us/azure/ai-services/personalizer/

[21]https://learn.microsoft.com/en-us/azure/ai-services/qnamaker/

[22]https://learn.microsoft.com/en-us/azure/ai-services/speech-service/

[23]https://learn.microsoft.com/en-us/azure/ai-services/translator/

[24]https://learn.microsoft.com/en-us/azure/azure-video-indexer/

[25]https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/

[26]https://ritaj.birzeit.edu/bzu-msgs/attach/2596381/Chapter4_Security.pdf (DR.Ruba Awadallah Slides Official material)

[27]https://www.imperva.com/learn/data-security/cloud-governance/#:~:text=Cloud%20governance%20is%20a%20set,smooth%20operation%20of%20cloud%20systems.

[28]https://www.oracle.com/in/erp/risk-management/what-is-enterprise-risk-management/

[29]https://www.business.qld.gov.au/running-business/digital-business/online-risk-security/risk#identifying-types-of-it-risk

[30]https://www.imperva.com/learn/data-security/data-sanitization/#:~:text=Data%20sanitization%20involves%20purposely%2C%20permanently,gains%20access%20to%20the%20device.

[31]https://www.researchgate.net/publication/353824295_Homomorphic_Encryption_for_Cloud_Computing_and_Its_Challenges

[32]https://police.ucla.edu/reports-statistics/jeanne-clery-act/campus-security-authorities-csa#:~:text=A%20CSA%20is%20a%20person,annual%20safety%20and%20security%20report.

[33]https://www.getastra.com/blog/cloud/cloud-security-breaches/#:~:text=Data%20breaches%20continue%20to%20be,severe%20financial%20and%20reputational%20consequences.

[34]https://www.techtarget.com/searchsecurity/definition/data-breach

[35]https://www.wiz.io/academy/common-cloud-vulnerabilities

[36]https://builtin.com/articles/risks-of-cloud-computing

[37]https://www.infosecinstitute.com/resources/cryptography/protect-data-by-preventing-insecure-cryptographic-storage/#:~:text=Insecure%20Cryptographic%20Storage%20vulnerability%20occurs,method%20and%20poor%20key%20handling.

[38]https://www.digitalguardian.com/blog/top-data-vulnerabilities-cause-data-loss

[39]https://www.cohesity.com/glossary/backup-and-recovery/#:~:text=Backup%20and%20recovery%20is%20the,be%20again%20used%20in%20operations.

[40]https://www.imperva.com/learn/data-security/data-sanitization/#:~:text=Data%20sanitization%20involves%20purposely%2C%20permanently,gains%20access%20to%20the%20device.

[41]https://www.symptai.com/resources/insights/data-and-privacy-protection/5-common-privacy-violations#:~:text=Violations%20occur%20when%20data%20processing,Processing%20Personal%20Data%20without%20consent.

[42]https://www.tufin.com/blog/understanding-shared-responsibility-model-cloud-security#:~:text=The%20shared%20responsibility%20model%20is%20a%20fundamental%20aspect%20of%20cloud,security%20posture%20in%20the%20cloud.

[43]https://www.sentra.io/blog/azure-security-tools#:~:text=The%20Layers%20of%20Security%20in%20Azure%3A&text=Virtual%20networks%2C%20network%20security%20groups,protect%20against%20unauthorized%20network%20access.

[44]https://learn.microsoft.com/en-us/azure/security/fundamentals/overview

[45]https://learn.microsoft.com/en-us/azure/security/fundamentals/overview

[46]https://www.matillion.com/blog/the-importance-of-data-classification-in-cloud-security#:~:text=Data%20classification%20in%20cloud%20security%20assists%20an%20organization%20in%20understanding,security%20and%20data%20management%20programs.

[47]https://www.ibm.com/topics/data-lifecycle-management#:~:text=Data%20lifecycle%20management%20has%20several%20important%20benefits%20which%20include%3A&text=Process%20improvement%3A%20Data%20plays%20a,process%20improvement%20and%20increases%20efficiency.