Security and Privacy Issues in Cloud Computing

Intan Sorfina binti Mohd Fadhil
Faculty of Computer and Mathematical Sciences
Universiti Teknologi Mara, UiTM
Tapah, Malaysia
2020462348@student.uitm.edu.my

Nurul Batrisyia binti Mohd Nizar
Faculty of Computer and Mathematical Sciences
Univesiti Teknologi Mara, UiTM
Tapah, Malaysia
2020621664@student.uitm.edu.my

Raudatul Jannah binti Rostam
Faculty of Computer and Mathematical Sciences
Univesiti Teknologi Mara, UiTM
Tapah, Malaysia
2020482912@student.uitm.edu.my

***Abstract*—With a variety of software and hardware services available to users, cloud computing has developed in recent years as a very influential and transformational technology. It functions as a fundamental method for sharing resources via the internet, with virtualization being essential to making this sharing of cloud resources possible. The National Institute of Standards and Technology (NIST) has described cloud computing as a concept that permits easy, on-demand network access to a shared pool of reconfigurable computing resources. With little management work or communication with the cloud provider, these resources can be quickly supplied and released. A significant amount of businesses have adopted cloud computing due to the many advantages and opportunities it provides. But the quick shift to the cloud has also given rise to security worries. Cloud computing is one of the modern technology that must to be used with caution. Cloud computing does not come with strong data privacy protections. Therefore, it is very important to ensure the confidentiality of data storage in order to protect data security. The objective of this paper is to discuss about the cloud computing models, the cloud service providers, the security and privacy issues surrounding cloud computing. Furthermore, prevention strategies and best practices for security and privacy issues in cloud computing will also be discussed in this paper.**

Keywords—Cloud Security, Security issues, Privacy, Software as a service, Platform as a service, Infrastructure as a service

I. INTRODUCTION

The internet serves as a driving force behind different technical breakthroughs, and one of the most important among them is cloud computing. This creative technology continues to evolve, transforming cutting-edge concepts and technologies into practical utility solutions. Cloud computing, as an internet-based technology, offers unique possibilities for communication and storage. It facilitates the provision of computer services over the internet, allowing on-demand access to shared resources such as networks, storage, servers, services, and applications [1]. Rather than physically obtaining these resources, companies can access them as needed, paying for their usage on a per-use basis. This technique saves on management expenses and time, making cloud computing an increasingly attractive choice. Its flexible infrastructure, net-centric strategy, and simplicity of access have contributed to its widespread acceptance.

Cloud computing offers the advantage of delivering on-demand, scalable computing resources, minimising the need for cloud service providers to engage in substantial hardware planning. With this flexibility, cloud service providers can start with limited resources and progressively increase physical capacity as demand develops, without demanding an upfront commitment. Cloud computing can be classified into four types based on the access type: private, public, community, and hybrid cloud [2].

Private cloud: A private cloud refers to a deployment by private enterprises specifically for safely storing their data. Although third-party suppliers commonly administer private clouds, they are located on-premise. Accessibility to the private cloud can only be granted to company workers to guarantee proper authorization management for security concerns. In one example, a corporation desiring to provide access to its clients' data can construct a private data center. Private cloud affords benefits like greater security. It gives additional control over sensitive information and apply powerful data security procedures to preserve privacy. However, the disadvantage is the substantial costs connected with equipment purchases and utility bills.

Public cloud: It is a kind of cloud computing where resources are given by a third-party provider through the internet and shared by companies and individuals who want to utilise or buy them. The public cloud is generally held by large corporations that offer cloud services. For example, Amazon Web Services (AWS). Furthermore, resources in the public cloud mostly supplied as a service for a pay-as-you-go price. The key benefit is the possibility to conduct on-demand purchases, where usage immediately corresponds to payment. Other than that, all public cloud's user is free from the responsibility of maintaining the cloud. Public cloud services are more reliable which indicates that the likelihood of a breakdown interrupting the service is extremely low. Public cloud customers are often home users accessing the providers' network over the internet. The security difficulties associated with the public cloud include worries about data protection and privacy due to its public nature. There is limited control over the transfer of information or access to sensitive data. Despite these security restrictions, small firms have profited from public cloud services as they deal with limited sensitive information and incur minor privacy issues.

Community cloud: It is a cloud environment that is jointly owned by several organisations that have similar goals. Organisations also can use a single platform in the community cloud for all of their demands that will discourages them from purchasing separate cloud services. It resembles a private cloud, but the computing power and supporting infrastructure are solely in the control of two companies with related privacy and security objectives. The community cloud is more expensive than the public cloud, and because it contains untrusted parties, data access may not be adequately controlled. The benefit of a community cloud, however, is the participation of unbiased third-party access for security auditing.

Hybrid cloud: A hybrid cloud involves two or more cloud providers and combines the services of a private cloud owner and a public cloud owner through a partnership. It means that workload accessibility, coordination, and management across two or more computing platforms are all

included in a hybrid cloud installation. With this strategy, organisations may take advantage of the scalability and cost-effectiveness of public cloud environments without disclosing any data to outside parties or jeopardising mission-critical software applications. The public cloud's rapid scalability features are combined with the advantages of a private cloud, which give improved control. Compared to other methods, it considerably increases organisational agility and gives organisations more freedom. The hybrid cloud has comparable security restrictions to the public cloud, including the potential leakage of sensitive data, which poses serious security threats. One solution to this problem is to manage identity and access to cloud resources.

The sharing of user data among numerous operating organisations is made possible by cloud deployment methods, which frequently involve the authorisation of Personal Identity Information (PII). To avoid unauthorised data tampering during communication across boundaries, organisations must prioritise information confidentiality and integrity. Data integrity cannot be ensured by relying simply on data encryption. User who are considering using Cloud Computing systems are significantly discouraged by the existence of security and privacy concerns. Security was ranked as the top problem out of nine variables in an IDC study that included 244 IT executives/CIOs and their line-of-business counterparts in August 2008 [3]. A system may unintentionally be exposed to hazards of information leakage due to inadequate security control deployment in the design of cloud computing. It is essential to address privacy issues in the cloud environment to protect user identities and keep data private.

II. Cloud Computing Models

Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) are the three core models that make up cloud computing.

IaaS stands for "Infrastructure as a Service" and refers to the management of physical resources by cloud service providers. IaaS substitutes traditional on-premises data centre infrastructure by offering computation, storage, memory, networking, and supporting software, such as operating systems and databases. It enables users to set up software programmes and operating systems. Users do have some influence over the deployed programmes, operating systems, and network components, even though they might not have full control over the underlying infrastructure [4]. IaaS may supply organisations with a number of advantages, including the ability to make workloads faster, simpler, more adaptable, and more affordable.

PaaS stands for “Platform as a Service”. PaaS is an adaptable application stage with a pre-installed programming stack is accessible to clients. These platforms and programming environments are made available for cloud infrastructure services. Example of PaaS is Yahoo. It provides operational and developmental features for application deployment, facilitating the creation and hosting of applications within the cloud. Through user data privacy techniques and customizable software installs, PaaS primarily aims to maximise user control over privacy-related features and sensitive information.

SaaS stands for “Software as a Service”. Using cloud infrastructure, a third-party provider develops applications and makes them accessible to clients online through SaaS. SaaS can perform tasks continuously from any device using an internet browser. By providing software applications and APIs to developers, SaaS allows customer freedom because users pay on a subscription basis without needing to install anything first. Given that SaaS frequently operates in a shared or multi-tenant environment, it can result in advantageous cost savings.

III. Cloud Service Providers

A) Amazon Web Services (AWS)

Through AWS server farms, these cloud-based web services deliver a range of services for computing, networking, storage and IoT. AWS also offers services such as Amazon SageMaker for AI/ML capabilities, Amazon Relational Database Service (RDS) for databases, Amazon Simple Storage Service (S3) for storage, and Amazon Elastic Compute Cloud (EC2) for computational capacity. AWS as shown in Figure 1 supports clients from small businesses to major corporations.

Fig.1 : AWS logo

B) Microsoft Azure

Azure as shown in Figure 2 is Microsoft's platform for cloud computing. Numerous programming languages, third-party-specific systems and applications are supported by Microsoft Azure. It also provides services for infrastructure, storage, analytics and databases. Microsoft Azure utilises massive virtualization at Microsoft data centers internationally and it supports more than 600 services such as Server, SQL Server, and Office 365. Azure Stack offers hybrid cloud capabilities by enabling businesses to create and manage applications across on-premises and cloud environments.

Fig.2 : Microsoft Azure logo

C) IBM Cloud

IBM Cloud as shown in Figure 3 is designed for companies that place a high priority on security and industry-specific solutions. It provides services that includes IoT, blockchain, analytics, and infrastructure. Other than that, IBM Cloud focuses on hybrid cloud solutions that let businesses combine cloud resources with on-premises infrastructure.

Fig.3 : IBM Cloud logo

D) Oracle Cloud

Oracle Cloud is a cloud computing service supplied by Oracle Corporation as shown in Figure 4 provides a variety of services for IaaS, PaaS, and SaaS. Furthermore, it also offers enterprise-grade solutions, such as Oracle Autonomous Database, Oracle Cloud Infrastructure, and Oracle Cloud Applications. Oracle Cloud caters to businesses seeking a comprehensive cloud offering with a focus on data management, emerging technologies and enterprise applications

Fig.4 : Oracle Cloud logo

E) Google Cloud Platform (GCP)

GCP as shown in Figure 5 offers cloud computing services by utilising the infrastructure and technologies that power Google's search engine. In addition to computation, storage and machine learning, it provides a wide range of services. GCP is renowned for its ability to process data because of Google BigQuery and Google Cloud Dataflow.

Fig.5 : Google Cloud Platform logo

F) Alibaba Cloud

Alibaba Cloud as shown in Figure 6 is a well-known China's cloud service company. It provides a full range of cloud services, including big data processing, relational databases, storage, and networking. Alibaba Cloud gives data facilities in 24 regions and 74 availability zones throughout the entire world.

Fig.6 : Alibaba Cloud logo

IV. SECURITY ISSUES IN CLOUD COMPUTING

A) Data breaches and unauthorized access

When a company is attacked by hackers who are able to access the cloud network without authorization or use programmes to see, copy, and transfer data, a data breach frequently happens. Sensitive, protected, or confidential data that is copied, communicated, viewed, stolen, altered, or used by someone not authorised to do so constitutes to a data breach. Other terms include data spill, information leak, information leakage, and unintended information disclosure.

One of the biggest organisational threats in terms of security is data leaking [5]. This is due to cloud service providers' usage of shared infrastructure to store enormous amounts of data from several clients. So, it is also more likely to get hacked.

B) Data loss and recovery

Data loss may occur for cloud service providers as a result of hardware or software issues, natural disasters, or other unforeseen causes. Sometimes these issues happen at random so it is crucial to have effective disaster recovery and backup procedures in place. Some institutions refuse to accept data delivery through the cloud because it lacks security when communicating with other systems [6].

C) Malware and hacking threats

Malware is a term which describes any kind of malicious computer threats. Malicious software, or malware, gives an attacker complete or partial control over the target machine. There are many types of malware that constitutes as a threats to a cloud service providers as shown in Figure 7.

Fig. 7: Types of Malware

- **Trojan or File-based malware:** A type of virus that hides itself in other trustworthy files. Malware is installed and run simultaneously with the bundled software and files that contain it.

- **Account Hijacking:** Through methods like social engineering, phishing, or password cracking, unauthorised people may try to access cloud accounts. They accomplish this by sending emails or developing websites that appear to be from a reputable source, like a bank or business.

- **API exploitation:** Hackers can use improperly built or poorly secured APIs to obtain unauthorised access to cloud services or manipulate data. Vulnerabilities can be caused by poor authentication, lax access constraints, or a lack of input validation in API requests.

D) Insider threats and privileged user abuse

Malware may be introduced into the cloud environment by malicious insiders, hacked user accounts, or other third parties working for a company or cloud service provider. These people may purposefully upload dangerous files, set security options incorrectly, or abuse their powers to carry out evil deeds. Other than that, abuse by privileged users in cloud computing settings is a major security worry.

Users having higher privileges and access to vital resources within the cloud architecture are known as privileged users. These users can be system administrators, staff members of cloud service providers, or even authorised users with administrative rights. Figure 8 shows the percentage of insider threats to privileged accounts.

Fig. 8: Insider Threats to Privileged Accounts

Despite the fact that the percentage is not high, there is still a risk. Privileged users have the ability to deliberately interfere with cloud services by incorrectly configuring crucial elements, turning off virtual machines, or turning off security measures. This may result in many problems such as the service interruptions, loss in money or harm to reputation for the cloud service provider's customers. If an unauthorised person has access to a client's private information, the client must sign up for a new membership. Otherwise, more data will be leaked [5].

E) Denial of Service (DoS) attacks

In a DoS attack, the attacker will attempt to interfere with or break the performance of cloud services by flooding the target webserver using HTTP requests or by taking advantage of vulnerabilities. Certain DoS attacks target weaknesses in cloud applications or services specifically. An attacker might, for instance, take advantage of a weakness in the input validation system of an application to make it crash or use up too many resources. Figure 9 shows a respresentation of a DoS attack.

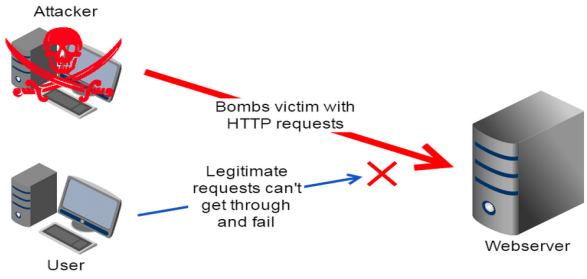

Fig. 9: A DoS Attack

There are also attacks of this type, known as distributed denial of service attacks, flood servers and networks with network traffic, preventing users from accessing particular Internet-based services. The provider will be threatened if they don't take action to stop network attacks by hackers [6].

V. PRIVACY ISSUES IN CLOUD COMPUTING

A) Data privacy concerns

The capacity of a person or group to keep information about them private and only selectively release them is known as privacy. When users access sensitive data in the cloud, privacy means that cloud services can stop possible attackers from deducing the user's behaviour based on the user's visit pattern (not by directly leaking data). The user has a right to information about how personal data is gathered, processed, and used [8]. The privacy concerns vary depending on the cloud environment:

- Who is in charge of making sure that personal information is processed in accordance with legal requirements.
- How to make it possible for users to maintain control over their data while it is stored and processed in the cloud and prevent theft, evil use, and unauthorised selling,
- How to prevent data loss, leakage, unauthorised change, or fabrication, where replicating user data to several suitable places is a common choice, and ensure data replications in a jurisdiction and consistent state.

These are the concerns that are included in a cloud service which must be address.

B) Third-party data handling and access

The management and access of data stored in the cloud by cloud service providers (CSPs) or other third-party entities is referred to as third-party data handling and access. Bussiness depend on cloud service providers to properly handle and secure the data that have been entrusted to them. For a variety of uses, including data storage, processing, or analytics, cloud providers may use subcontractors or share data with other parties. The practises of the subcontractors' data handling and security measures should be evaluated by the organisations to make sure they comply with the necessary standards.

C) Lack of control over data

Compared to keeping and managing data on-site, organisations frequently give up some direct control when moving their data to the cloud. In a SaaS (Software as a Service) setting, the service provider is accountable for data storage with little control and visibility [7]. Consumers cannot maintain control over their data while it is processed and kept on the cloud because it is required by law.

Privacy concerns may arise if users are unable to view submitted, processed data on a shared system. Proper regulation and specification of access controls are required [8]. Following are some elements that affect how control is seen to be lacking:

- **Data Security:** Users may worry about the security of their data when it is stored on the cloud. Even when cloud services has many security measures, users may be concerned about data breaches or unwanted access by strangers to their personal data.
- **Vendor lock-in:** When moving data to the cloud, one becomes somewhat dependent on the tools and services offered by the cloud provider. Organisations can be concerned about being forced to work with a particular provider and the difficulties involved in switching providers or, in the event that it becomes necessary, relocating their data and applications back on-site.
- **Physical Infrastructure:** In conventional on-site systems, businesses are in complete control of their physical infrastructure, which includes servers, storage units, and networking tools. The cloud service provider is for managing these components, and organisations may only have a limited amount of visibility or control over the underlying infrastructure.
- **Customization and Configuration:** On-site solutions give businesses more freedom to modify and tailor their applications and infrastructure to suit their particular requirements. Businesses often work within the infrastructure and service offerings of the cloud provider while using the cloud, which may restrict their capacity to customise the environment to meet their precise needs.

D) Compliance with privacy regulations

When it comes to cloud computing, compliance with privacy laws is an important factor, especially when sensitive or personally identifiable information is involved. Figure 10 shows a compliance mindmap for cloud computing.

Fig. 10: A Compliance Mindmap

Consider the following important factors to ensure that cloud computing complies with privacy laws:

- **Choose a Compliant Cloud Service Provider:** Consider the cloud service provider's (CSP) obedience to privacy laws while making your decision. Examine the provider's data protection policies, security precautions, and contractual agreements regarding privacy and data protection. Verify that the CSP utilises suitable security measures to protect personal data in line with the relevant laws.

- **Data Security and Incident Response:** To prevent unauthorised access, loss, or disclosure of personal data in the cloud environment, use strong security measures. This comprises intrusion detection systems, access controls, encryption, and regular security audits. Develop incident response procedures for data breaches in collaboration with the cloud provider, making ensuring they comply to the rules for breach notification.

- **Data Processing Agreements:** Make a data processing agreement (DPA) or a data protection amendment (DPA) with the cloud provider. Both parties must obligned to the privacy regulations.

VI. SECURITY AND PRIVACY MEASURES IN CLOUD COMPUTING

Cloud computing security and privacy measures relate to methods, actions, and technologies used to safeguard data and assure confidentiality, integrity, availability and compliance in cloud-based settings.

A) Encryption Techniques and Protocol

To maintain the security and confidentiality of data kept in the cloud, as well as data sent between client and cloud provider, encryption techniques and protocols are employed in cloud computing [9].

- **Storage Encryption:** Cloud companies often use encryption to protect data that is stored in their systems. This may involve encrypting data before it is stored on disk using methods such as Advanced Encryption Standard (AES). Cloud providers manage the encryption keys but customers can choose to manage their own encryption keys.

- **Data in Transit Encryption:** To establish secure connections between the client and the cloud provider, encryption techniques such as SSL/TLS are used. During transmission, these protocols encrypt the data, preventing unauthorised interception or manipulation. HTTPS is often used for secure online connection with cloud-based apps. It employs SSL/TLS.

- **Database Encryption:** Encryption methods can be used in cloud-based databases to safeguard sensitive data within the database itself. Encrypting certain fields or columns or even the whole database can be accomplished using methods such as column-level encryption or Transparent Data Encryption (TDE).

- **Virtual Private Networks (VPNs):** VPNs are employed in cloud computing to offer safe connections between client's network and the cloud provider's network. They use encryption techniques like IPsec or SSL/TLS to create encrypted tunnel between client and cloud provider.

- **Key Management:** Proper key management is crucial to make sure the security of encrypted data. Key management services often provided by cloud providers that allows clients to securely store and manage encryption keys. Key creation, rotation and safe storage are examples of key management practices.

B) Access controls and Authentication Mechanisms

Access restrictions and authentication systems are key components of cloud computing security [10]. Here are some instances of typical cloud computing access restrictions and authentication mechanisms:

- **Role-Based Access Control (RBAC):** In cloud computing, RBAC is commonly used to give permissions and access privileges based on preset roles. It enables administrators to govern user access based on job functions, making scaled access restrictions easier to administer.

- **Multi-Factor Authentication (MFA):** By forcing users to give several forms of identity before accessing cloud services, MFA offers an extra layer of protection. To improve authentication security, cloud providers frequently include MFA solutions like SMS-based codes, authentication applications or hardware tokens.

- **Identity and Access Management (IAM):** Cloud computing IAM solutions enable centralised control and administration of user identities, roles,

and access rights. They let businesses to establish and enforce granular access restrictions to cloud resources like virtual machines, storage, and databases.

C) Security Audits and Assessments

Security audits and assessments are systematic reviews of an organization's security controls, vulnerabilities and dangers in its systems, networks or cloud environments. Security audits and assessments are critical components of guaranteeing cloud computing systems' security and compliance. They help in the identification of vulnerabilities, the assessment of risks and evaluation of the efficacy of security controls.

Security audits entail a thorough examination of the security mechanisms and controls in place in a cloud environment. They are carried out to evaluate the efficacy of security practises, discover possible flaws, and ensure compliance with security policies and regulations. The following are important features of cloud computing security audits:

- **Access Controls Audit:** Evaluating access control techniques such as authentication, authorization, and user provisioning to ensure that proper access controls are in place.
- **Data Protection Audit:** Evaluating the efficacy of data security techniques such as encryption, data categorization, and data loss prevention in ensuring data confidentiality, integrity, and availability.
- **Infrastructure Assessment:** Auditing the cloud infrastructure to discover vulnerabilities and ensure suitable security controls are in place, including network architecture, data centres, and physical security measures.
- **Incident Response Audit:** Evaluating incident response protocols and capabilities in order to establish the organization's readiness to identify, respond to, and recover from security issues.

Vulnerability assessments entail locating and analysing flaws in cloud systems, apps, and networks. This procedure usually consists of the following steps:

- **Scanning and Assessment:** Conducting automatic and human scans of cloud infrastructure and apps in order to discover any vulnerabilities, misconfigurations, or shortcomings.
- **Risk Prioritization:** Assessing the degree and effect of detected vulnerabilities in order to prioritize remedial activities based on the risks associated with them.
- **Penetration Testing:** Controlled simulated assaults are carried out in order to exploit vulnerabilities and discover possible security weaknesses in the cloud environment.
- **Patch Management:** Examining patch management policies and procedures to guarantee that security patches and updates to address known vulnerabilities are applied on time.

Third-party audits in cloud computing may be performed by external auditors or independent assessors to give an unbiased review of cloud service providers' security posture. These audits assist organizations in gaining assurance about the efficacy of security procedures and validating the provider's adherence to industry standards.

D) Data backup and disaster recovery strategies

Data backup and disaster recovery solutions in cloud computing are critical for assuring data availability, business continuity and limiting the effect of any disasters or interruptions. Cloud computing provides several benefits for data backup and disaster recovery (DR). These are some examples:

- **Scalability:** Cloud-based backup and disaster recovery solutions may be scaled to suit the demands of any organisation, no matter how large or small.
- **Security:** Cloud-based backup and disaster recovery systems are extremely secure because they employ industry-leading encryption and access control technologies.
- **Reliability:** Because cloud-based backup and disaster recovery systems are backed up and duplicated across numerous data centres, they are extremely dependable.
- **Cost-effectiveness:** Cloud-based backup and disaster recovery solutions are frequently less expensive than traditional on-premises systems.

VII. PREVENTION STRATEGIES AND BEST PRACTICES

A) Risk Assessments and Management

Risk assessments are a specific component of risk management that involves a systematic and structured evaluation of risks. Risk assessments help organizations understand the potential risks they face and guide decision-making for risk mitigation.

Risk management is the systematic process of identifying, assessing, and mitigating risks to minimize potential harm and maximize opportunities. It involves a set of coordinated activities aimed at understanding, evaluating, and addressing risks to achieve organizational objectives effectively.

B) Service Level Agreements and Contracts

A service level agreement (SLA) is a contractual relationship between a cloud service provider and a customer that specifies service levels, performance targets and duties for cloud service delivery [11]. SLAs play a role in cloud computing because they define expectations as well as ensuring accountability and plan a framework for

measuring and monitoring the quality and availability of cloud services. Using SLAs and contracts offer benefits such as:

- **Increased transparency:** Contracts and SLAs can help in increasing transparency between cloud provider and consumer. This can assist to avoid misunderstandings or disagreements between both parties.

- **Improved communication:** Contracts and SLAs can help to improve communication between the cloud provider and the client. This also can help in the resolution of any concerns that may develop.

- **Increased accountability:** SLAs and contracts can assist to increase accountability for both cloud provider and customer. This can help to make sure that both parties meet their obligations.

- **Reduced risk:** SLAs and contracts help to reduce risk for both cloud provider and customer. This can help to ensure that both parties are protected if encountered problems.

C) Training and Awareness Program

Training and awareness program are one of prevention strategies that can be implemented to avoid security and privacy issue in cloud computing. It is important to educate staffs and users about preventive measures, best practices and potential risks.

In order to get an effective training and awareness program, the training's objectives need to be clearly defined. The objectives may include:

- Raising awareness of the security and privacy dangers associated with cloud computing.
- Encouraging responsible behaviour and compliance with security standards.
- Ensuring that appropriate legislation and data protection laws are followed.
- Providing staff with the information they need to recognize and respond to security events.
- Improving knowledge of best practises and industry standards.

Other than having clearly defined objectives, the content of the training program should be developed align with the objectives. A wide range of topics should be covered including:

- Introduction to cloud computing, benefits and risks
- Overview of security and privacy issues in cloud computing
- Risk assessments and prevention strategies
- Controls and authentication procedures for security
- Data protection, encryption and privacy measures

After getting training and awareness about cloud computing issues, it is great to create a culture of constant awareness by encouraging continuing debates and communication regarding cloud computing security and privacy. Encourage staff or user to be aware, report any security events or concerns, and establish lines of communication for continuous assistance and direction.

D) Data Classification and Access Control

Data classification and access control are critical preventative tactics for solving cloud computing security and privacy concerns. It is the process of assigning a sensitivity level to data. This assists in determining which data is most critical and requires maximum protection. Organizations can implement suitable security measures and guarantee that data is handled and kept according to its unique classification level by categorizing data. Access control can be used to secure data after has been classified. The practice of limiting who has access to data and what can be done with it is known as access control [12]. There are several access control systems but they all employ a mix of accounts, passwords and permissions. Few benefits when using data classification and access controls are as follows:

- **Enhanced Data Protection:** Data classification and access control can assist to improve cloud data security. This is because they can assist in identifying and protecting sensitive data, as well as restricting who has access to it and what they can do with it.
- **Reduced Risk and Compliance:** Data classification assists organizations in assessing and managing the hazards associated with various types of data. Organizations may prioritize their efforts and deploy resources more efficiently by matching security measures with the sensitivity of the data. Implementing data categorization and aligning access restrictions accordingly facilitates compliance with data protection requirements, industry standards for both wired and wireless security infrastructure [13], and contractual responsibilities.

VIII. CONCLUSION

In the IT sector, cloud computing has become the real paradigm, offering affordable on-demand services. In order to meet the growing demand for accessing and utilising resources made available over the Internet, it supports multi-tenancy. The adoption of cloud computing, however, presents serious security and privacy challenges. Without appropriate answers to these problems, mainstream acceptance might take longer. In this paper, the basic ideas and the main security issues surrounding cloud computing have been pointed out. The security and privacy issues related to cloud computing have been taken into account to reduce the worries that cloud users have raised that would prevent them from using the cloud. With the help of this

evaluation, it may help to influence the future directions of research in the area of cloud security and privacy.

ACKNOWLEDGEMENT

The authors wish to thank Dr. Mohammad Hafiz Mohd Yusof, our lecturer for CSC662 and Universiti Teknologi Mara Tapah for helps in providing us with the needed facilities and platform to complete this paper.

REFERENCES

[1] S. Abdullah and K. Azmi, "Security and Privacy Challenges in Cloud Computing," Nov. 2018, doi: https://doi.org/10.1109/cr.2018.8626872.

[2] W. Kong, Y. Lei, and J. Ma, "Data security and privacy information challenges in cloud computing," International Journal of Computational Science and Engineering, vol. 16, no. 3, p. 215, 2018, doi: https://doi.org/10.1504/ijcse.2018.091772.

[3] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," Nov. 2010, doi: https://doi.org/10.1109/skg.2010.19.

[4] Y. S. Abdulsalam and M. Hedabou, "Security and Privacy in Cloud Computing: Technical Review," vol. 14, no. 1, pp. 11–11, Dec. 2021, doi: https://doi.org/10.3390/fi14010011.

[5] R. Barona and E. A. M. Anita, "A survey on data breach challenges in cloud computing security: Issues and threats," 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Apr. 2017, doi: https://doi.org/10.1109/iccpct.2017.8074287.

[6] A. Narang and D. Gupta, "A Review on Different Security Issues and Challenges in Cloud Computing," IEEE Xplore, Sep. 01, 2018. https://ieeexplore.ieee.org/abstract/document/8675099.

[7] O. O. Aldawibi, M. A. Sharf, and M. M. Obaid, "Cloud Computing Privacy: Concept, Issues And Solutions," Jul. 2022, doi: https://doi.org/10.1109/isiea54517.2022.9873688.

[8] Pahalage Dona Thushari, "Current security and privacy issues, and concerns of Internet of Things (IoT) and Cloud Computing: A review," Nov. 2022, doi: https://doi.org/10.1109/icccis56430.2022.10037730.

[9] I. Gupta et al., Compendium of data security in cloud storage by applying hybridization of encryption algorithm, 2022. doi:10.36227/techrxiv.20306157

[10] A. R. Khan and L. K. Alnwihel, "A brief review on cloud computing authentication frameworks," Engineering, Technology & Applied Science Research, vol. 13, no. 1, pp. 9997–10004, 2023. doi:10.48084/etasr.5479

[11] N. K. Neeraj et al., "Service level agreement violation detection in Multi-cloud environment using Ethereum Blockchain," 2023 International Conference on Networking and Communications (ICNWC), 2023. doi:10.1109/icnwc57852.2023.10127520

[12] K. Almarhabi, A. Bahaddad, and A. Mohammed Alghamdi, "Security Management of BYOD and cloud environment in Saudi Arabia," Alexandria Engineering Journal, vol. 63, pp. 103–114, 2023. doi:10.1016/j.aej.2022.07.031

[13] M. M. Hafiz and F. H. Mohd Ali, "Profiling and mitigating brute force attack in home wireless LAN," 2014 International Conference on Computational Science and Technology (ICCST), Kota Kinabalu, Malaysia, 2014, pp. 1-6, doi: 10.1109/ICCST.2014.7045190.