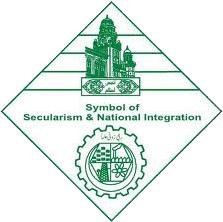
**Anjuman-I-Islam**

**M.H. Saboo Siddik Polytechnic**



Data communication and computer network (dcc) (22414)

Micro-Project

Computer Engineering

Department

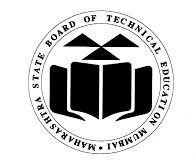
Co-4i

Title: Cloud Security

Year: 2022-23 **Prepared by:**

* 210451 Abdurrahman Qureshi
* 210453 Saad Ansari
* 210460 Arya More
* 210463 Adnan Kazi

**Under the guidance of**: Prof. Mohammad Ali



**MAHARASHTRA STATE**

**BOARD OF TECHNICAL EDUCATION**

# Certificate

This is to certify that Mr. Abdurrahman Qureshi Roll no.

210451 of fourth semester of Diploma in Computer

Engineering of institute M.H. Saboo Siddik Polytechnic(code:0002) has completed Micro-Project satisfactorily in the subject: DCC (22414) for the academic year 2022-23 as prescribed in the curriculum.

Place: Mumbai Enrolment no:2100020112 Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Exam seat no:

## Signature Signature Signature

## Project guide H.O.D Principal

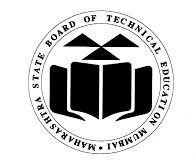


SEAL OF



INSTITUDE





**MAHARASHTRA STATE**

**BOARD OF TECHNICAL EDUCATION**

# Certificate

This is to certify that Mr. Saad Ansari Roll no. 210453 of fourth semester of Diploma in Computer Engineering of institute M.H. Saboo Siddik Polytechnic (code: 0002) has completed Micro-Project satisfactorily in the subject: DCC (22414) for the academic year 2022-23 as prescribed in the curriculum.

Place: Mumbai Enrolment no:2100020102 Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Exam seat no:

**Signature Signature Signature**

## Project guide H.O.D Principal

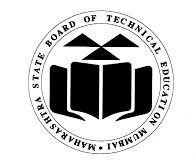


SEAL OF



INSTITUDE





**MAHARASHTRA STATE**

**BOARD OF TECHNICAL EDUCATION**

# Certificate

This is to certify that Mr. Arya More Roll no.

210460 of fourth semester of Diploma in Computer

Engineering of institute M.H. Saboo Siddik Polytechnic(code:0002) has completed Micro-Project satisfactorily in the subject: DCC (22414) for the academic year 2022-23 as prescribed in the curriculum.

Place: Mumbai Enrolment no:2100020097 Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Exam seat no:

## Signature Signature Signature

## Project guide H.O.D Principal

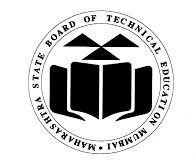


SEAL OF



INSTITUDE





**MAHARASHTRA STATE**

**BOARD OF TECHNICAL EDUCATION**

# Certificate

This is to certify that Mr. Adnan Kazi Roll no.

210463 of fourth semester of Diploma in Computer

Engineering of institute M.H. Saboo Siddik Polytechnic(code:0002) has completed Micro-Project satisfactorily in the subject: DCC (22414) for the academic year 2022-23 as prescribed in the curriculum.

Place: Mumbai Enrolment no:21000200117 Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Exam seat no:

## Signature Signature Signature

## Project guide H.O.D Principal



SEAL OF



INSTITUDE



# Acknowledgment

We wish to express our profound gratitude to our guide Mr. Mohammad Ali Sir who guided us endlessly in the framing and completion of the micro project. He

guided us on all the main points in that micro project. We are indebted to his constant encouragement, cooperation, and help. It was his enthusiastic

support that helped us in overcoming various obstacles in the micro-project.

We are also thankful to our Principal, HOD, faculty members and classmates of

Computer Engineering department for extending their support and motivation in the completion of this micro-project.

Names of Team Members with Roll Nos.

1. 210451 Abdurrahman Qureshi
2. 210453 Saad Ansari
3. 210460 Arya More
4. 210463 Adnan Kazi

**Annexure-I**

***Micro-Project proposal***

## Title of Micro-Project: Cloud Security

### Aims/Benefits of Micro-Project

Cloud security is a set of policies, strategies, controls, procedures, and practices designed to safeguard the data, resources, and applications hosted on the cloud. It provides multiple levels of protection within the network infrastructure against data breaches, unauthorized access, [DDoS attacks](https://www.indusface.com/blog/how-to-stop-ddos-attack/" \t "_blank), and so on.

### Course outcomes addressed

* Analyse the functioning of data communication and computer network
* Select relevant transmission media and switching techniques as per need
* Configure various networking devices

### Proposed methodology

1. Introduction to cloud Security.

1. Challenges in cloud security.
2. Encryption in cloud security.
3. Access control in cloud security.
4. Threat detection in cloud security.

* Discussion of the given topic among group members.
* Literature survey
* Submission of project proposal
* Analysis of data
* Work divided among group members
* Compilation of content
* Representation
* Editing the content as per the instructions
* Report Preparation
* Viva and presentation

**Annexure-I**

#### IV. Action Plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Weeks** | **Details of activity** | **Planned start date** | **Planned finish date** | **Name of responsible team members** |
| 1& 2 | Discussions & finalization of topics |  |  |  |
| 3 | Preparation of abstract |  |  |  |
| 4 | Literature review |  |  |  |
| 5 | Submission of Micro-Project proposal(Annexure -I) |  |  |  |
| 6 | Collection of information on given topic |  |  |  |
| 7 | Collection of all relevant contents |  |  |  |
| 8 | Discussion and submission of outline of the project |  |  |  |
| 9 | Analysis/execution of collected data/information and Preparation of prototypes/drawings/charts/graphs/ tables/models/circuits/programs etc. |  |  |  |
| 10 | Compilation of contents of project |  |  |  |
| 11 | Compilation of weekly progress report |  |  |  |
| 12 | Preparation of the project report (Annexure II) |  |  |  |
| 13 | Viva Voce / Delivery of presentation. |  |  |  |

#### V. Resources required

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. no.** | **Name of resources** | **Specifications** | **Qty** | **Remarks** |
| 1. | Online | Learning resources and various websites | 5 sites |  |
| 2. | Desktop | Microsoft word, Tools with internet facility. | 1 for each |  |
| 3. | Software | SQL plus | 1 for each |  |

Names of Team Members with Roll Nos.

1. 210451 Abdurrahman Qureshi
2. 210453 Saad Ansari
3. 210460 Arya More
4. 210463 Adnan Kazi

Approved by:

Sign of Faculty:

Name of faculty: Prof. Mohammad Ali

**Annexure-II**

***Micro-Project Report***

**Title of Micro-project: Cloud Security**

#### Rationale

#### Cloud security is a collection of procedures and technology designed to address external and internal threats to business security. Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.

#### II. Aims/Benefits of Micro-Project

Cloud security is a set of policies, strategies, controls, procedures, and practices designed to safeguard the data, resources, and applications hosted on the cloud. It provides multiple levels of protection within the network infrastructure against data breaches, unauthorized access, [DDoS attacks](https://www.indusface.com/blog/how-to-stop-ddos-attack/" \t "_blank), and so on.

#### Course outcomes achieved

* Analyze the functioning of data communication and computer network
* Select relevant transmission media and switching techniques as per need
* Configure various networking devices

#### IV. Literature review

the literature on Cloud security is extensive and continues to evolve as new generations are introduced and new research is conducted. Cloud security have had a profound impact on society and have enabled new applications and services that were once unimaginable.

**REFERECNCES:**

* + <https://www.microsoft.com/en-us/security/business/security-101/what-is-cloud-security>

#### <https://www.microsoft.com/en-us/windows-365/cloud-security>

* + https://www.redhat.com/en/topics/security/what-is-hybrid-cloud-security

#### Actual Methodology Followed

We were assigned with the Micro-Project topic and time was assigned to us to complete the project in 13 weeks. All team members worked together in these 13 weeks together in order to complete this Micro-Project. Data was collected according to our topic finally at last technical report was prepared.

#### Actual resources used

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. no.** | **Name of resources** | **Specifications** | **Qty** | **Remarks** |
| 1. | Websites | https://www.ibm.com/ | 1 for each |  |

#### VII. Outputs of the Micro-Project

# Cloud security

# What is cloud security?

**Cloud security** is the set of control-based security measures and technology protection, designed to protect online stored resources from **leakage, theft**, and **data loss**. Protection includes data from **cloud infrastructure, applications**, and **threats.** Security applications uses a software the same as [**SaaS (Software as a Service)**](https://www.javatpoint.com/software-as-a-service) model.



## How to manage security in the cloud?

Cloud service providers have many methods to protect the data.

Firewall is the central part of cloud architecture. The firewall protects the network and the perimeter of end-users. It also protects traffic between various apps stored in the cloud.

Access control protects data by allowing us to set access lists for various assets. For example, you can allow the application of **specific employees** while restricting others. It's a rule that employees can access the equipment that they required. We can keep essential documents which are stolen from **malicious insiders** or hackers to maintaining strict access control.

Data protection methods include [Virtual Private Networks](https://www.javatpoint.com/vpn-full-form) (**VPN**), encryption, or masking. It allows remote employees to connect the network. VPNaccommodates the tablets and smartphone for remote access. Data masking maintains the data's integrity by keeping identifiable information private. A medical company share data with data masking without violating the **HIPAA** laws.

For example, we are putting intelligence information at risk in order of the importance of security. It helps to protect mission-critical assets from threats. Disaster recovery is vital for security because it helps to recover lost or stolen data.

## Benefits of Cloud Security System

We understand how the cloud computing security operates to find ways to benefit your business.

Cloud-based security systems benefit the business by:

* Protecting the Business from Dangers
* Protect against internal threats
* Preventing data loss
* Top threats to the system include **Malware, Ransomware**, and
* Break the Malware and Ransomware attacks
* Malware poses a severe threat to the businesses.

More than **90%** of malware comes via email. It is often reassuring that employee's download malware without analyzing. Malicious software installs itself on the network to steal files or damage the content once it is downloaded.

**Ransomware** is a malware that hijacks system's data and asks for a financial ransom. Companies are reluctant to give ransom because they want their data back.

Data redundancy provides the option to pay a ransom for your data. You can get that was stolen with **minimal** service interruption.

Many cloud data protection solutions identify **malware** and **ransomware**. Firewalls keep malicious email out of the inbox.



## Top 7 Advanced Cloud Security Challenges

It becomes more challenging when adopting modern cloud approaches Like: **automated cloud integration**, and **continuous deployment (CI/CD)** methods, distributed server less architecture, and short-term assets for tasks such as a service and container.

Some of the advanced cloud-native security challenge and many layers of risk faced by today's cloud-oriented organizations are below:



**1. Enlarged Surface**

Public cloud environments have become a large and highly attractive surface for hackers and disrupt workloads and data in the cloud. Malware, zero-day, account acquisition and many malicious threats have become day-to-day more dangerous.

**2. Lack of visibility and tracking**

Cloud providers have complete control over the infrastructure layer and cannot expose it to their customers in the **IaaS** model. The lack of visibility and control is further enhanced in the **SaaS** cloud models. Cloud customers are often unable to identify their cloud assets or visualize their cloud environments effectively.

**3. Ever-changing workload**

Cloud assets are dynamically demoted at scale and velocity. Traditional security tools implement protection policies in a flexible and dynamic environment with an ever-changing and short-term workload.

**4. DevOps, DevSecOps and Automation**

Organizations are adopting an automated [**DevOps**](https://www.javatpoint.com/devops)**CI/CD** culture that ensures the appropriate security controls are **identified** and **embedded** in the development cycle in code and templates. Security-related changes implemented after the workload is deployed to production can weaken the organization's security posture and lengthen the time to market.

**5. Granular privileges and critical management**

At the application level, configured keys and privileges expose the session to security risks. Often cloud user roles are loosely configured, providing broad privileges beyond the requirement. An example is allowing untrained users or users to delete or write databases with no business to delete or add database assets.

**6. Complex environment**

These days the methods and tools work seamlessly on public cloud providers, private cloud providers, and on-premises manage persistent security in hybrid and multi-cloud environments-it including geographic Branch office edge security for formally distributed organizations.

**7. Cloud Compliance and Governance**

All the leading cloud providers have known themselves best, such as **PCI 3.2, NIST 800-53, HIPAA** and **GDPR**.

It gives the poor visibility and dynamics of cloud environments. The compliance audit process becomes close to mission impossible unless the devices are used to receive compliance checks and issue real-time alerts.

**THREATS TO CLOUD SECURITY**



There are several threats to cloud security that organizations should be aware of:

* **Data Breaches:**

One of the biggest threats to cloud security is data breaches. This occurs when unauthorized users gain access to sensitive data stored in the cloud.

* **Malware and Viruses:**

Malware and viruses can infect cloud-based systems, which can then spread to other connected systems, causing significant damage.

* **Insider Threats:**

Insider threats refer to employees or other authorized users who intentionally or unintentionally cause harm to the organization's cloud infrastructure, either by stealing data or disrupting operations.



* **DDoS Attacks:**

Distributed denial-of-service (DDoS) attacks can overwhelm cloud-based systems with a flood of traffic, causing them to crash and become unavailable to legitimate users.

* **Insecure APIs:**

Application programming interfaces (APIs) are a common way for cloud-based applications to interact with each other. If these APIs are not properly secured, they can be vulnerable to attack.

* **Data Loss:**

Data loss can occur due to a variety of reasons, including accidental deletion, hardware failure, and natural disasters.

* **Lack of Compliance:**

Compliance with regulatory requirements is important for many organizations, particularly those in heavily regulated industries such as healthcare and finance. Failure to comply with these requirements can result in legal and financial penalties.

* **Account Hijacking:**

Cloud-based systems can be vulnerable to account hijacking, in which an attacker gains access to a user's account and uses it to steal data or launch attacks.

**CONTROLLED ACCESS IN CLOUD SECURITY**

To mitigate these threats, organizations should implement robust security measures such as encryption, multi-factor authentication, and regular security audits. It is also important to choose a reputable cloud service provider with a strong track record of security and compliance.Controlled access is an important aspect of cloud security, as it helps organizations limit who can access their cloud-based systems and data. Here are some best practices for implementing controlled access in cloud security:



* **Role-Based Access Control:**

Implementing role-based access control (RBAC) is an effective way to control access to cloud-based resources. RBAC assigns users to specific roles with predefined permissions, based on their job function or level of authority.

* **Multi-Factor Authentication:**

Multi-factor authentication (MFA) adds an extra layer of security by requiring users to provide additional verification, such as a code sent to their mobile phone, in addition to a password.

* **Encryption:**

Encryption is essential for protecting sensitive data in the cloud. Data should be encrypted both at rest (when it is stored) and in transit (when it is being transferred).

* **Network Segmentation:**

Network segmentation can help limit the impact of a potential security breach by isolating different parts of the network and controlling the flow of traffic between them.

* **Monitoring and Logging:**

Monitoring and logging are important for detecting and responding to security incidents. Organizations should implement tools for real-time monitoring and logging of user activity, network traffic, and system events.

* **Access Reviews:**

Regular access reviews help organizations ensure that users have only the access they need to perform their job functions. Reviews should be conducted at least annually and whenever there are changes to user roles or job functions.



**ENCRPYTION IN CLOUD SECURITY**

By implementing these best practices, organizations can improve their cloud security posture and minimize the risk of unauthorized access to their cloud-based systems and data.Encryption is a critical component of cloud security. It involves transforming sensitive data into a form that is unintelligible to unauthorized users, so that even if the data is intercepted or stolen, it cannot be read or used without the decryption key. Here are some important considerations for encryption in cloud security:

* **Encryption at Rest:**

Data stored in the cloud should be encrypted when it is "at rest," meaning when it is stored on disk or in a database. This protects against unauthorized access if the physical storage device is stolen or compromised.

* **Encryption in Transit:**

Data should also be encrypted when it is "in transit," meaning when it is being transmitted over a network. This protects against interception and eavesdropping.

* **Strong Encryption Algorithms:**

Strong encryption algorithms, such as AES-256, should be used to encrypt data. These algorithms are virtually unbreakable and provide strong protection against unauthorized access.

* **Key Management:**

Encryption keys should be managed carefully to ensure that they do not fall into the wrong hands. Keys should be stored securely, rotated regularly, and only accessible to authorized users.

* **Performance:**

Encryption can sometimes impact performance, particularly for data-intensive applications. Organizations should evaluate the impact of encryption on performance and take steps to optimize performance where possible.

By implementing strong encryption practices, organizations can significantly enhance the security of their cloud-based systems and data. However, encryption is only one part of a comprehensive cloud security strategy, and organizations should also implement other security measures, such as access controls, network security, and threat detection.

**Micro Project Evaluation Sheet**

|  |  |  |
| --- | --- | --- |
| Name of student: Abdurrahman Qureshi | Enrolment no: 2100020112 | |
| Name of programme: Computer Engineering | Semester: 4th | |
| Course title: Data communication and computer networking | | Code: 22414 |

Title of Micro-Project: Cloud security

Course outcomes achieved:

* Analyse the functioning of data communication and computer network
* Select relevant transmission media and switching techniques as per need
* Analyse the transmission errors with respect to IEEE standards
* Configure various networking devices
* Configure different tcp / ip services



**Comments/Suggestions about teamwork/leadership/interpersonal communication \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

#### Name and designation of teacher: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Dated signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Micro Project Evaluation Sheet**

|  |  |
| --- | --- |
| Name of Student: Saad Ansari | Enrollment no: 2100020102 |
| Name of programme: Computer Engineering | Semester: 4th |
| Course title: Data communication and computer networking | Code: 22414 |

Title of Micro-Project: Cloud security

Course outcomes achieved:

* Analyze the functioning of data communication and computer network
* Select relevant transmission media and switching techniques as per need
* Analyze the transmission errors with respect to IEEE standards
* Configure various networking devices
* Configure different tcp / ip services

**Comments/Suggestions about teamwork/leadership/interpersonal communication \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

#### Name and designation of teacher: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Dated signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Micro Project Evaluation Sheet**

|  |  |
| --- | --- |
| Name of Student : Arya More | Enrolment no: 2100020097 |
| Name of programme: Computer Engineering | Semester: 4th |
| Course title: Data communication and computer networking | Code: 22414 |

Title of Micro-Project: Cloud security

Course outcomes achieved:

* Analyse the functioning of data communication and computer network
* Select relevant transmission media and switching techniques as per need
* Analyse the transmission errors with respect to IEEE standards
* Configure various networking devices
* Configure different tcp / ip services



**Comments/Suggestions about teamwork/leadership/interpersonal communication \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

#### Name and designation of teacher: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Dated signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Micro Project Evaluation Sheet**

|  |  |
| --- | --- |
| Name of Student : Adnan Kazi | Enrolment no: 2100020125 |
| Name of programme: Computer Engineering | Semester: 4th |
| Course title: Data communication and computer networking | Code: 22414 |

Title of Micro-Project: Cloud security

Course outcomes achieved:

* Analyse the functioning of data communication and computer network
* Select relevant transmission media and switching techniques as per need
* Analyse the transmission errors with respect to IEEE standards
* Configure various networking devices
* Configure different tcp / ip services



**Comments/Suggestions about teamwork/leadership/interpersonal communication \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Name and designation of teacher: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Dated signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_