### Slide 2: Introduction

1. **Overview**:
   1. There is a growing need for monitoring and analyzing network traffic.
   2. The benefits of cloud-based storage are scalability, flexibility, and cost-effectiveness.
   3. A brief introduction to the project using cloud storage to collect and analyze network data.

### Slide 5: Why Cloud Storage for Network Monitoring?

1. **Scalability**: Cloud platforms like AWS, Google Cloud, and Azure can automatically scale to accommodate increasing traffic data.
2. **Cost Efficiency**: Pay-as-you-go models ensure you only pay for what you use.
3. **Global Access**: Data can be accessed from anywhere with internet connectivity.
4. **Integration**: Easily integrates with other monitoring tools and services.

### Slide 6: How Cloud-Based Storage Works

1. **Data Collection**: Traffic data is collected from various network devices.
2. **Data Transfer**: Data is transferred to cloud storage using secure protocols (e.g., SFTP, HTTPS).
3. **Data Analysis**: Stored data can be processed and analyzed using cloud-based analytics tools.
4. **Storage**: Data is stored in a cloud environment, ensuring redundancy, security, and availability.

### Slide 7: Types of Cloud Storage Solutions

1. **Object Storage**: (e.g., AWS S3, Google Cloud Storage) – Scalable storage for large amounts of unstructured data.
2. **Block Storage**: (e.g., AWS EBS, Google Persistent Disk) – For high-performance applications requiring fast read/write access.
3. **File Storage**: (e.g., AWS EFS, Azure Files) – Shared storage for file-based applications.

### Slide 8: Advantages of Cloud-Based Storage for Network Monitoring

1. **Scalability**: Instantly scale storage based on traffic volume.
2. **Security**: Cloud providers offer robust encryption and security features.
3. **High Availability**: Ensure data is always accessible due to multiple data center locations.
4. **Automatic Backups**: Reduce the risk of data loss with automated backups and disaster recovery.

### Slide 9: Cloud Security Considerations

1. **Data Encryption**: Both in transit and at rest.
2. **Access Control**: Ensure that only authorized users can access the data.
3. **Compliance**: Choose cloud providers that meet industry standards (e.g., GDPR, HIPAA).
4. **Monitoring and Alerts**: Continuously monitor the integrity of the data and receive alerts for unusual activities.

### Slide 13: Conclusion

1. **Summary**:
   1. Cloud-based storage offers scalability, flexibility, and cost efficiency for network traffic monitoring.
   2. Improves data accessibility, security, and analysis capabilities.
   3. Helps overcome traditional on-premise storage limitations.
2. **Future Work**:
   1. Implementing AI/ML-based anomaly detection using cloud storage.
   2. Exploring hybrid cloud storage options for enhanced performance.