A Report on

Webinar On

Cloud computing and Security

20 July 2021

Submitted by **Dr. K Dinesh**, Associate Professor, Department of CST.

Resource Person details:

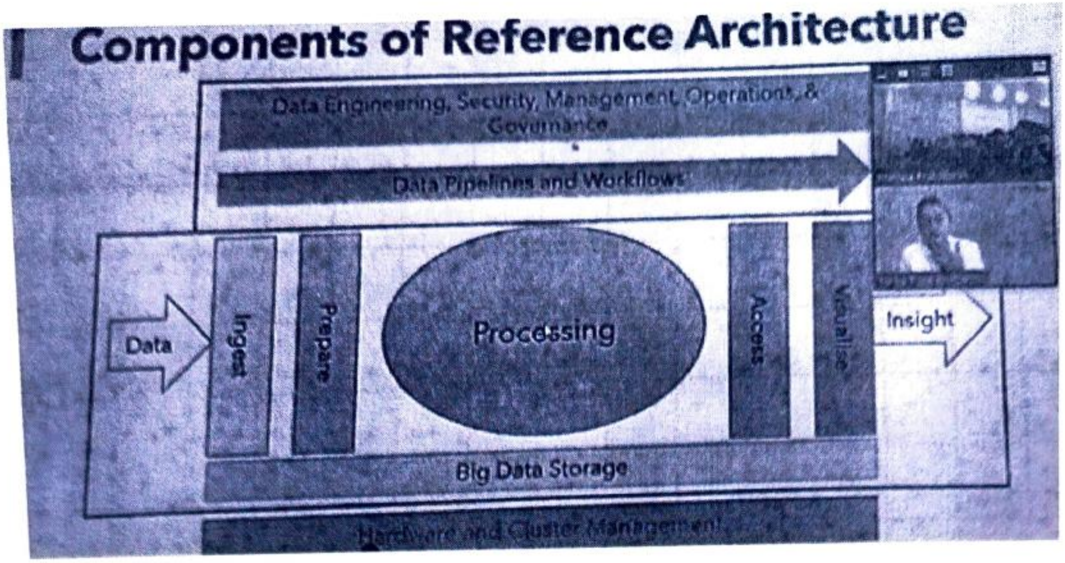
Resource Person:	**Dr. P. Syam Kuma,**
Designation:	**Assistant Professor,**
Organization:	**Institute of Development and Research in Banking Technology,**
Location:	**Hyderabad.**
Participants:	**III year CST students**
Attendance:	**150** participants (Internal)
Mode:	**Virtual**

Department of Computer Science and Technology, has organized **Webinar on "Cloud computing and Security"** on **20-07-2021, 10:00 am**.

Objective:

To gain valuable insights into both the opportunities and challenges associated with using cloud computing. They can also learn about best practices for securing their data and applications in the cloud, which can help them make informed decisions about their cloud strategy.

The event explored the relationship between cloud computing benefits and the inherent security concerns associated with it.



Components of Reference Architecture

Data Engineering, Security, Management, Operations, & Governance
Data Pipelines and Workflows
Data
Ingest
Prepare
Processing
Access
Visualise
Insight
Big Data Storage
Hardware and Cluster Management

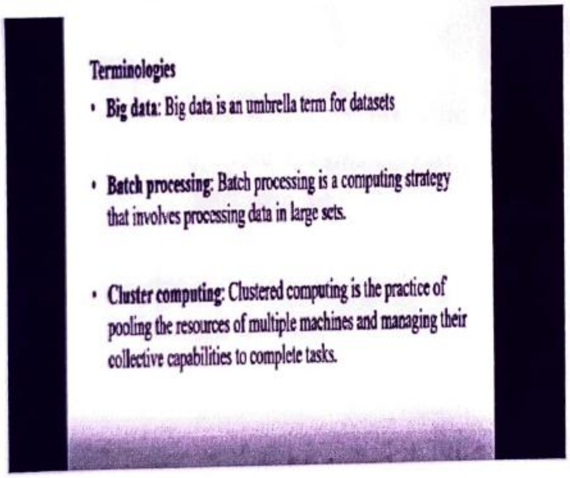
Key Points Discussed

- **Benefits of Cloud Computing:** The speaker(s) highlighted the numerous benefits of cloud computing, including:
  - **Scalability and flexibility:** Cloud services allow businesses to scale their resources up or down as needed, fostering agility and cost-efficiency.
  - **Increased uptime and disaster recovery:** Cloud providers offer high availability and disaster recovery solutions, ensuring minimal downtime and data protection.
  - **Enhanced collaboration:** Cloud-based tools and platforms facilitate effortless collaboration among team members and remote workforces.
  - **Reduced IT infrastructure costs:** Businesses can shift from capital expenditure on hardware to operational expenditure for cloud services, leading to potential cost savings.
- **Security Concerns in Cloud Computing:** The session also addressed the prevalent security concerns associated with cloud adoption, such as:
  - **Data breaches:** The risk of unauthorized access to sensitive data stored in the cloud remains a significant concern.
  - **Shared responsibility model:** In a shared responsibility model, the cloud provider secures the underlying infrastructure, while businesses are responsible for securing their data and applications hosted on the cloud.
  - **Compliance challenges:** Businesses need to ensure their cloud environment adheres to relevant industry regulations and data privacy laws.

Solutions and Recommendations

The speaker(s) offered various solutions and recommendations to enhance cloud security:

- **Implementing robust access controls:** Utilizing strong authentication protocols, multi-factor authentication, and granular access control lists are crucial for safeguarding data access.
- **Data encryption:** Encrypting data at rest and in transit adds an extra layer of protection against unauthorized access.
- **Regular security assessments:** Conducting regular vulnerability assessments and penetration testing helps identify and address potential security weaknesses before they can be exploited.
- **Staying informed:** Staying updated on the latest cloud security threats and best practices is essential for proactively mitigating risks.



Terminologies

- **Big data:** Big data is an umbrella term for datasets
- **Batch processing:** Batch processing is a computing strategy that involves processing data in large sets.
- **Cluster computing:** Clustered computing is the practice of pooling the resources of multiple machines and managing their collective capabilities to complete tasks.

Outcomes

The webinar provided valuable insights into the advantages and challenges of cloud computing from a security perspective. Attendees gained a deeper understanding of:

- The inherent benefits and security concerns associated with cloud adoption.
- The shared responsibility model in cloud security.
- Practical solutions and best practices to enhance cloud security.

This knowledge can empower attendees to make informed decisions regarding cloud adoption and implement appropriate security measures to protect their data and applications in the cloud environment.