DATA SECURITY IN CLOUD COMPUTING

PAVANI POLURU - EAC19041
SAI AKSHITH -EAC19061

CONTEXT

- What is cloud?
- What is cloud security ?
- Challenges in cloud security
- Data security in cloud
- Protecting the data using encryption
- Conclusion

CLOUD COMPUTING?

- Cloud computing is service oriented.
- The data can be shared among other parties easily.
- Data is recommended to store in internal organizational cloud.

TYPES OF CLOUD

- 1.Private Cloud – A private cloud can be accessed by single group or single organization.
- 2.Public Cloud – A public cloud can be accessed by any user with the internet connection and want to pay as per their usage.

TYPES OF CLOUD

- Community Cloud – A community cloud will be accessed by two or more organization that has similar cloud requirements
- Hybrid Cloud – A hybrid is the combination of two or more cloud (public, private, and community)

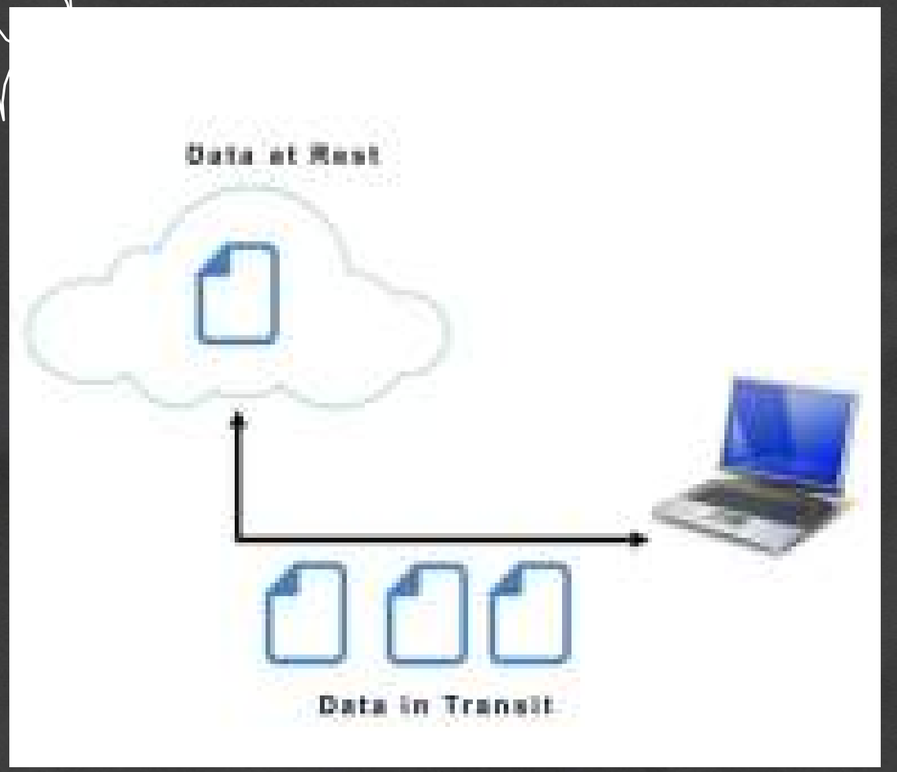
RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING

- Virtualization
  - Virtualization is a technique in which a fully functional operating system image is captured in another operating system to utilize the resources of the real operating system fully.
  - Compromising a hypervisor . A hypervisor can become a primary target if it is vulnerable and allocation and de-allocation of data.
  - Data must be properly authenticated before de-allocating the resources.

RISKS AND SECURITY CONCERNS IN CLOUD COMPUTING

- Storage in Public Cloud
  - Clouds implement centralized storage facilities, which can be an appealing target for hackers.
  - It is always recommended to have a private cloud if possible for extremely sensitive data.

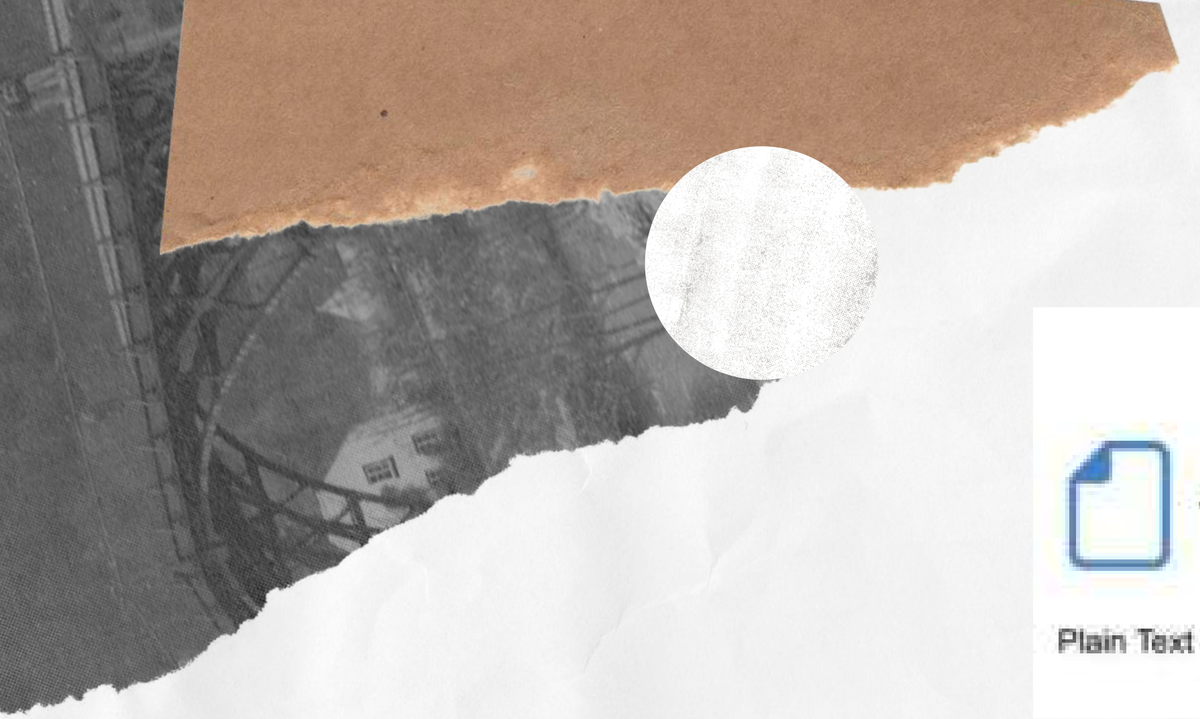
DATA SECURITY IN CLOUD COMPUTING

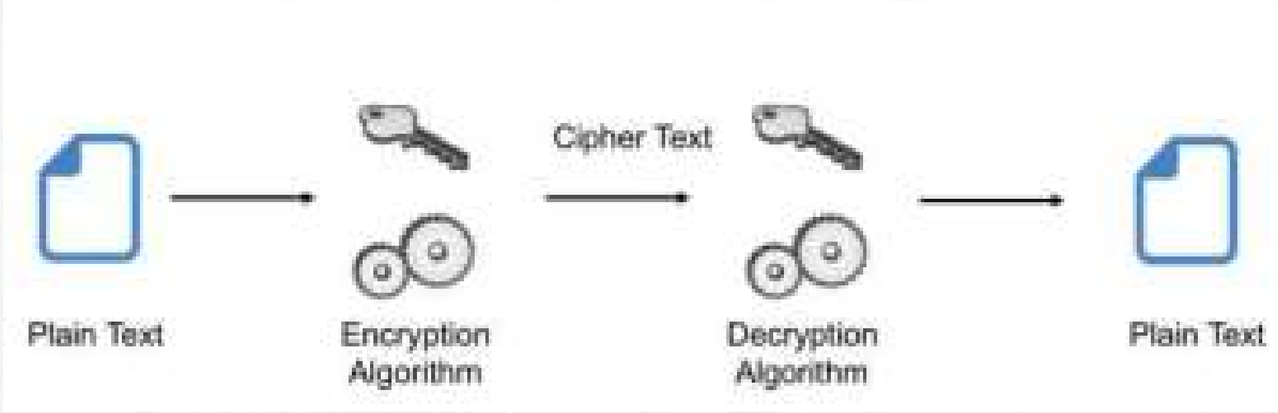


- Data at rest.
- Data at transit.

PROTECTING DATA USING ENCRYPTION

- Encryption keys for data in transit can be short-lived, whereas for data at rest, keys can be retained for longer periods of time.





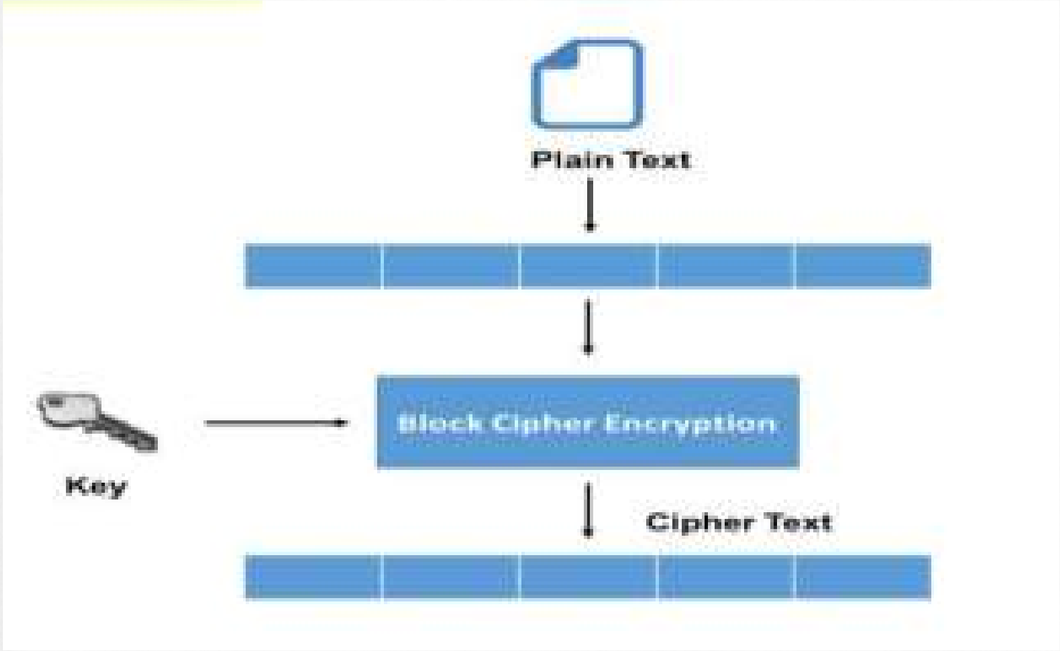
PROTECTING DATA USING ENCRYPTION

Cryptography

In the basic form of cryptography, plaintext is encrypted into cipher text using an encryption key, and the resulting cipher text is then decrypted using a decryption key

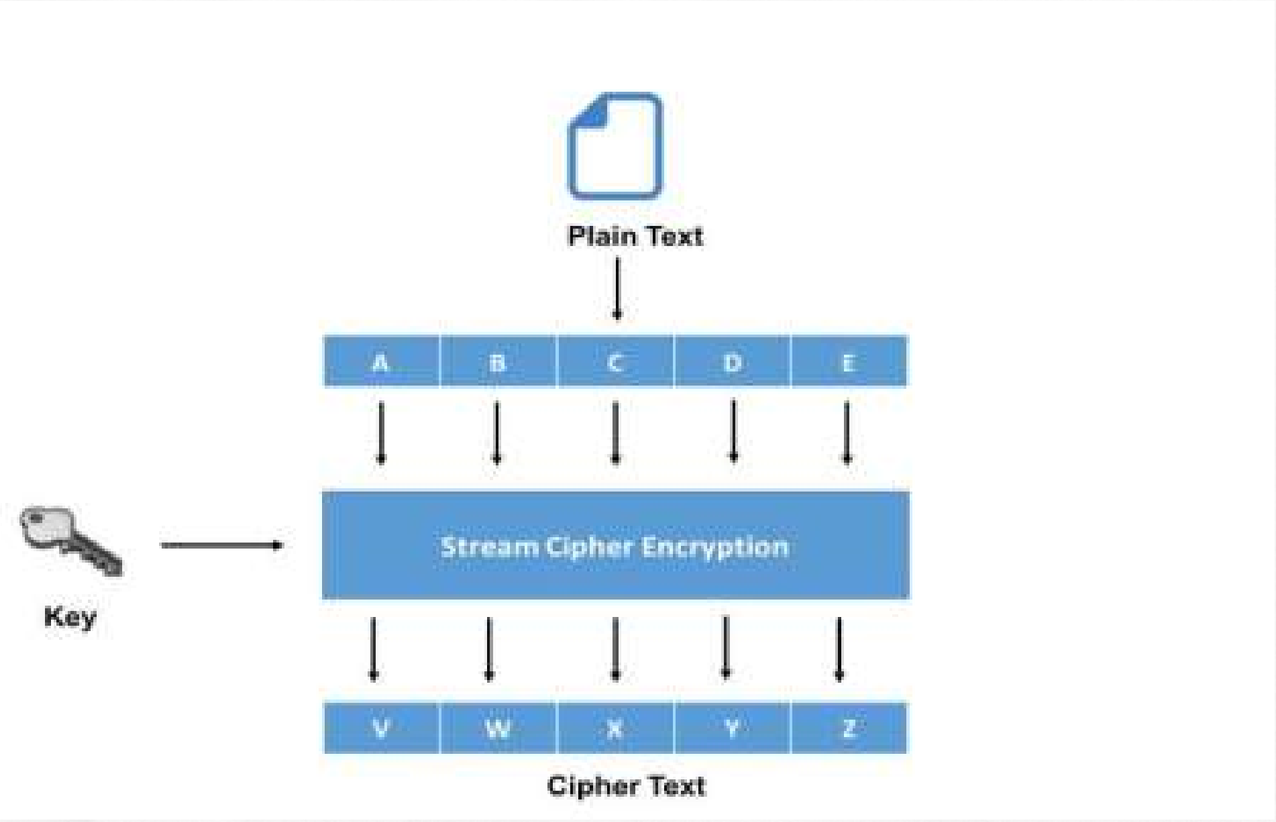
FOUR BASIC USES OF CRYPTOGRAPHY:

A. Block Ciphers



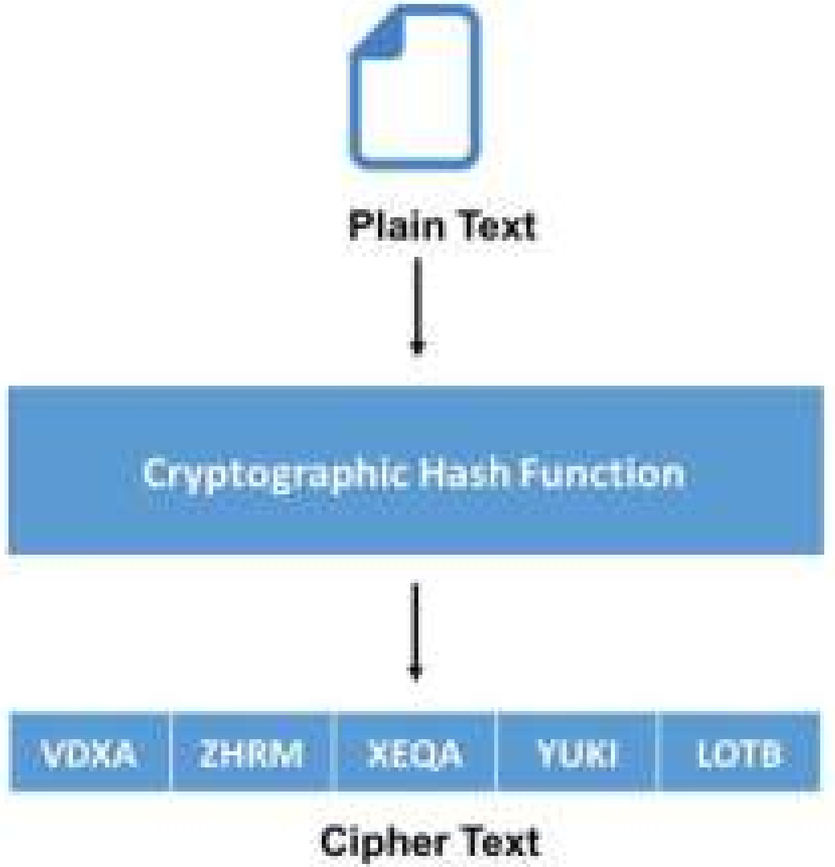
B. Stream Ciphers

FOUR BASIC USES OF CRYPTOGRAPHY:



C. Hash Functions

FOUR BASIC USES OF CRYPTOGRAPHY:



PROTECTING DATA USING STEGANOGRAPHY

Stenography is the process of hiding a secret message by embedding messages within the other message like text, audio, video, and images.

CONCLUSION

The data is first scrambled utilizing the cryptography procedure and concealing the data inside the content, picture, sound or video record utilizing steganography. Joining cryptography and steganography
procedure to guarantee security in cloud computing.