Security Essentials

AWS follows Shared Security Responsiblity Model.This means that there are certain portions of the cloud of which AWS is responsible for and there are certain portions of cloud where you are responsible for security.

This Shared Security model also reduces the Operational burden from you. As you dont need to look after the components of **host operation system**, the underlying **virtualization layer** or the physical **security of data centers**.

The portions of which you need to look after include:

1. Guest Operating system (its updates / security patches)
2. Application softwares installed on Gest OS
3. Configuration of Security firewalls.
4. Data stored on volumes.

Avoiding DDOS attacks:

DDOS attacks can be avoided using traditional measures, which include:

i. - Firewalls (NACL and security groups)
ii. - Traffic rate limiting
iii. - WAF (Web application firewall also called Reverse proxy)
iv. - Filtering incoming traffic.

Along with traditional methods, AWS provides cloudfront which can avoid DDOS attacks by routing traffic to different cloudfront edge locations. Thus, preventing the traffic from reaching main servers.

AWS does not allow port scanning of EC2 instances.

Data Encryption:

---

1. You can choose to encrypt your data while storing in S3. AWS provides AES-256 Encryption.

2. You can choose to store data in EBS volumes as encrypted. Any snapshot taken of an encrypted volume is automatically encrypted.

3. RDS Encryption:
   - You can choose to have encrypted database connections.
   - You can choose to store the data in encrypted form. In such a case, all automated backup snapshots will be encrypted as well and also the read-replicas will be encrypted.

CloudHSM (Hardware Security Module)

In this a physical server is dedicated for storing security keys. The basic idea is that security keys never go out of this HSM server.

Plain text is sent to the server for Encryption, and encrypted text is sent back from server.
Similarly, encrypted data is sent to server and corresponding decrypted text is sent back from server.

To communicate with a HSM server, one needs a HSM client. A HSM Client exposes API's which can be used to communicate with HSM server. A HSM client is simply a software which can be installed on an EC2 machine.

Fig: 3:14
NOTE: Once a key is lost, there is no way to restore data or key.

Even, AWS engineers dont have access to the keys. They can only apply updates to HSM server.
Sample keys that can be stored in HSM:
- Keys used to encrypt EBS volumes
- Keys used to encrypt database.
- Keys used for S3 Encryption.

HSM vs Key management service:

Both are exactly same, with the only difference that HSM provides more fine grained control over key management infrastructure and the types ok keys one can store.