DALHOUSIE UNIVERSITY

Faculty of Computer Science

CSCI 5409 Advanced Topics in Cloud Computing

Assignment-4

April 20, 2020

Submitted By

Vamsi Gamidi

B00834696

VM709690

Section A

Key Management Service:

AWS Key Management Service is used to create and manage customer master keys which can be used to encrypt data. AWS KMS uses FIPS 140-2 cryptographic module validation program to validate the encryption keys [1]. The encryption keys can only be accessed by the user who created the keys. By using AWS KMS, users can create both symmetric and asymmetric keys. AWS KMS is integrated with most of the AWS services. Symmetric customer master key is a 256-bit encryption key which is used to encrypt and decrypt data [4]. AWS services that are integrated with KMS does not support asymmetric customer master keys. Asymmetric customer master key is a mathematically related public and private key pair. AWS KMS uses the key pair to encrypt and decrypt or sign-in and verification. The private key in asymmetric customer master key is encrypted by a symmetric customer master key. There are two types of asymmetric customer master keys, RSA and Elliptic Curve (ECC) [5]. Users can set their own encryption rules by completely overriding the existing rules or can add additional rules on top of the default rules. To prevent the extensive use of encryption keys, users can enable automatic key rotation for a customer master key. Automatic key rotation provides the additional advantages such as preserving the properties like key ID, region, policies, and permissions. AWS charges $1/month for each customer master key that was created.

Feasibility in group project:

The major advantage of AWS Key Management Service is its capability to integrate with most of the AWS services. So, there is a lot of scope to use KMS in the project to encrypt the data.

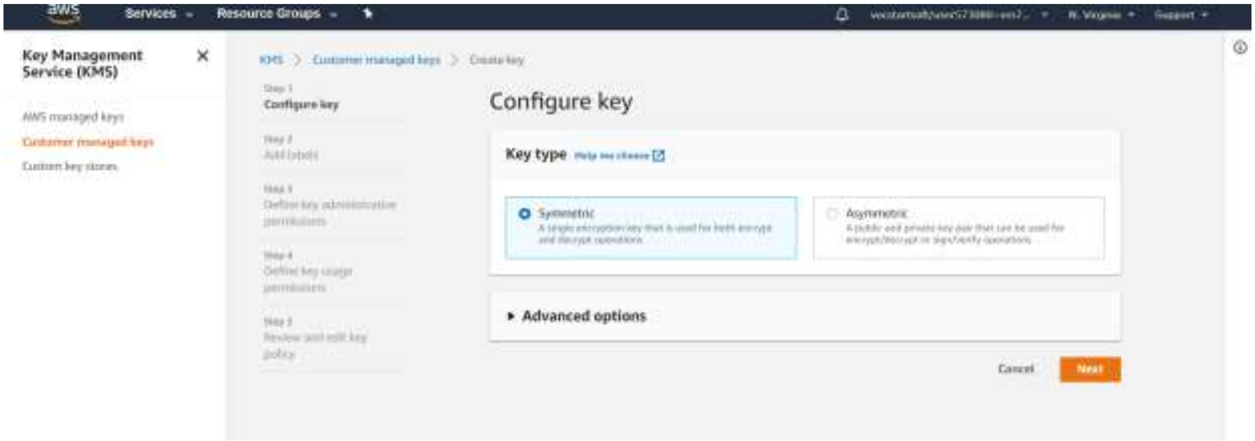
Simple Notification Service (SNS):

AWS Simple Notification Service can be used to send the OTP for two-factor authentication. By using AWS Key Management Service, we can encrypt the email address or any other sensitive data of the user.

Relational Database Service (RDS):

AWS Key Management Service can be integrated with RDS. So, sensitive user data such as password, phone number can be encrypted using KMS.

Key Creation Screenshots:



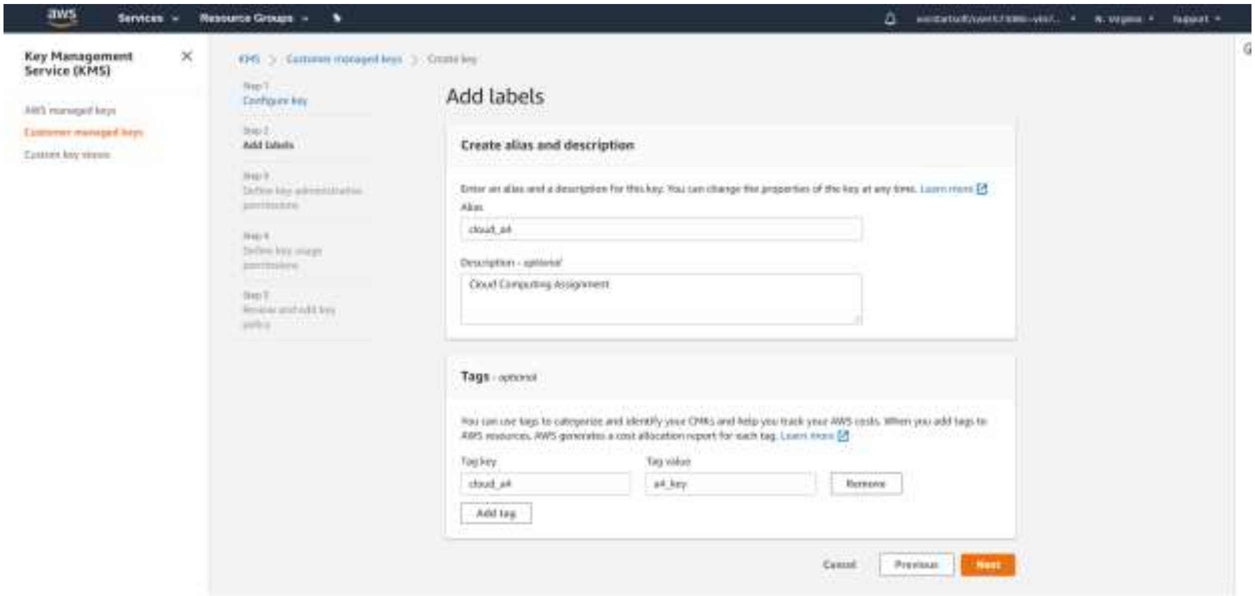
Configure key

Key type

● Symmetric
A single encryption key that is used for both encrypt and decrypt operations.

○ Asymmetric
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations.

Figure 1: Symmetric Key



Add labels

Create alias and description

Enter an alias and a description for this key. You can change the properties of the key at any time. Learn more

Alias: cloud_a4

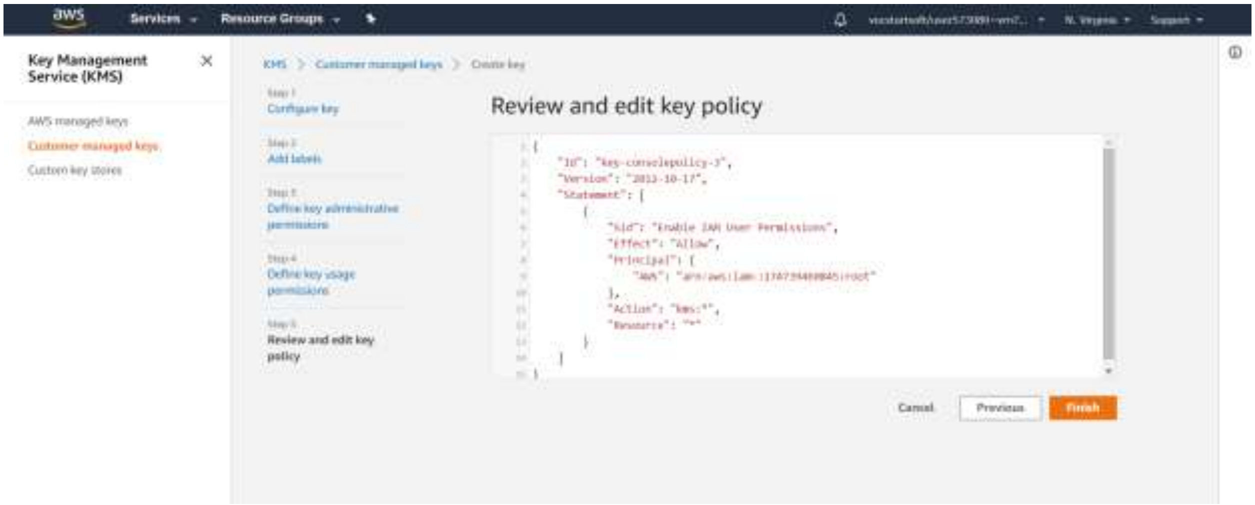
Description - optional: Cloud Computing Assignment

Tags - optional

You can use tags to categorize and identify your CMKs and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more

Tag key	Tag value
cloud_a4	a4_key

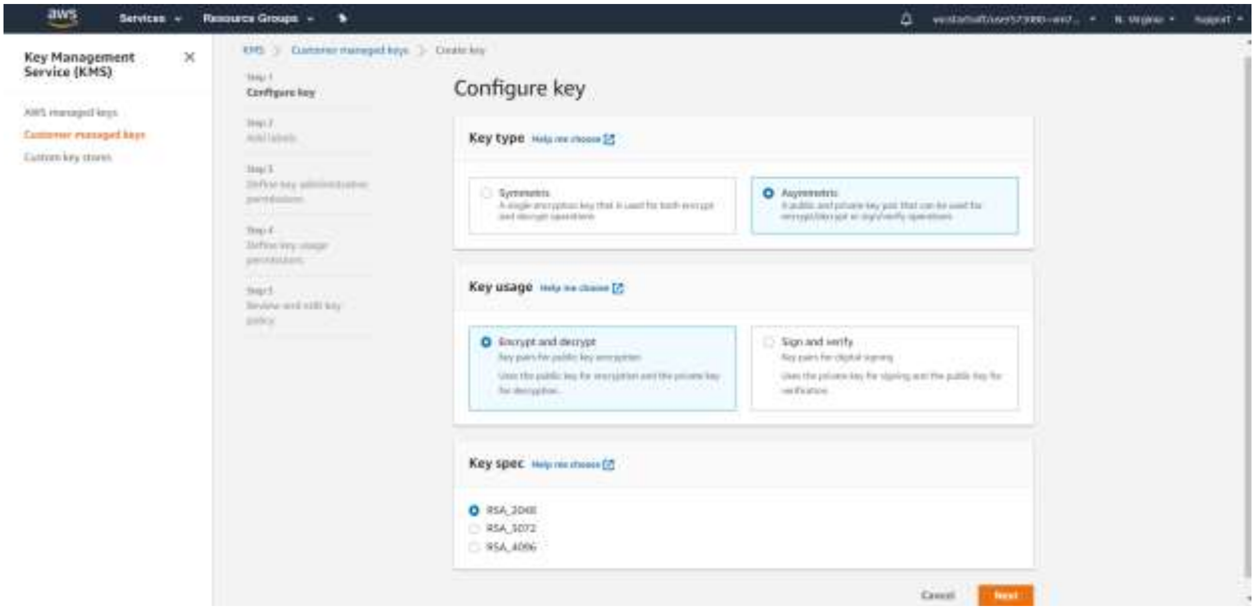
Figure 2: Symmetric Labels


aws
Services
Resource Groups
N. Virginia
Support
Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review and edit key policy

Review and edit key policy

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::174739488045:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

Figure 3: Symmetric Key Policy


aws
Services
Resource Groups
N. Virginia
Support
Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review and edit key policy

Configure key

Key type Help me choose

○ Symmetric
A single encryption key that is used for both encrypt and decrypt operations

● Asymmetric
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

Key usage Help me choose

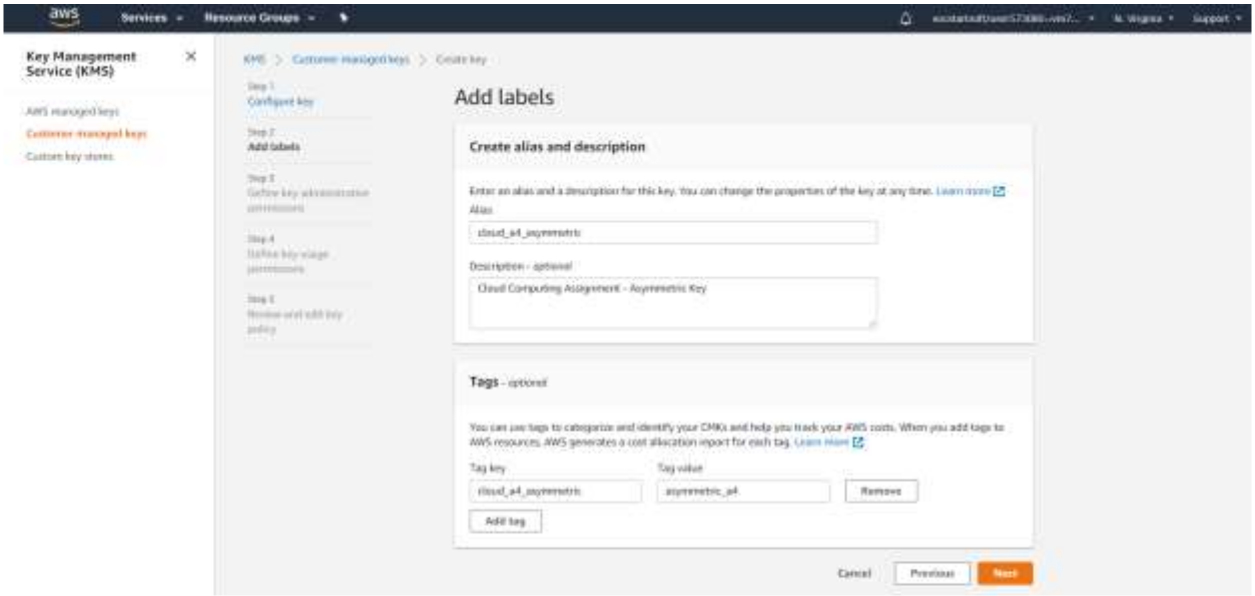
● Encrypt and decrypt
Key pairs for public key encryption
Uses the public key for encryption and the private key for decryption.

○ Sign and verify
Key pairs for digital signing
Uses the private key for signing and the public key for verification.

Key spec Help me choose

● RSA_2048
○ RSA_3072
○ RSA_4096

Figure 4: Asymmetric Key



Add labels

Create alias and description

Enter an alias and a description for this key. You can change the properties of the key at any time. Learn more

Alias: cloud_a4_asymmetric

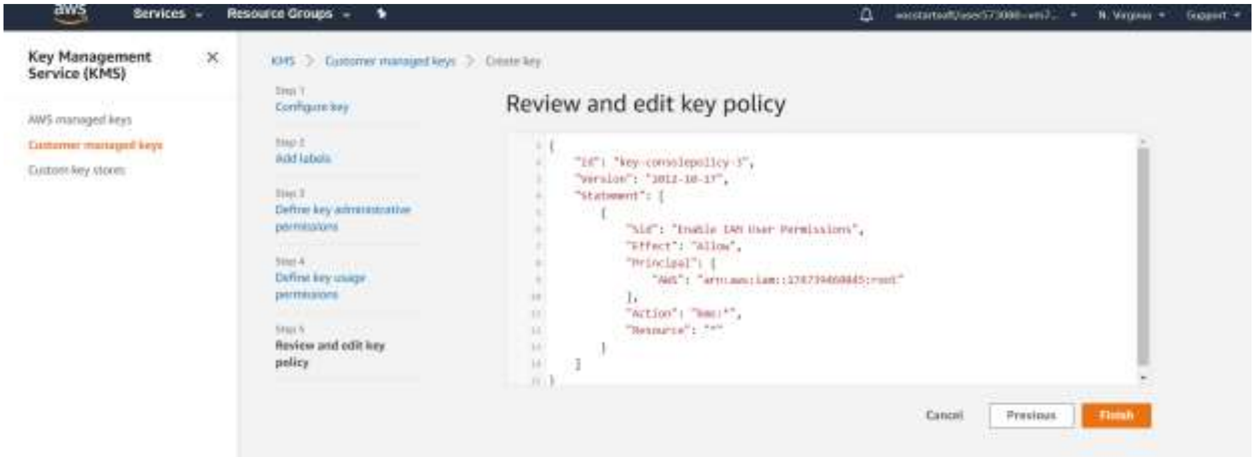
Description - optional: Cloud Computing Assignment - Asymmetric Key

Tags - optional

You can use tags to categorize and identify your CMKs and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more

Tag key	Tag value
cloud_a4_asymmetric	asymmetric_a4

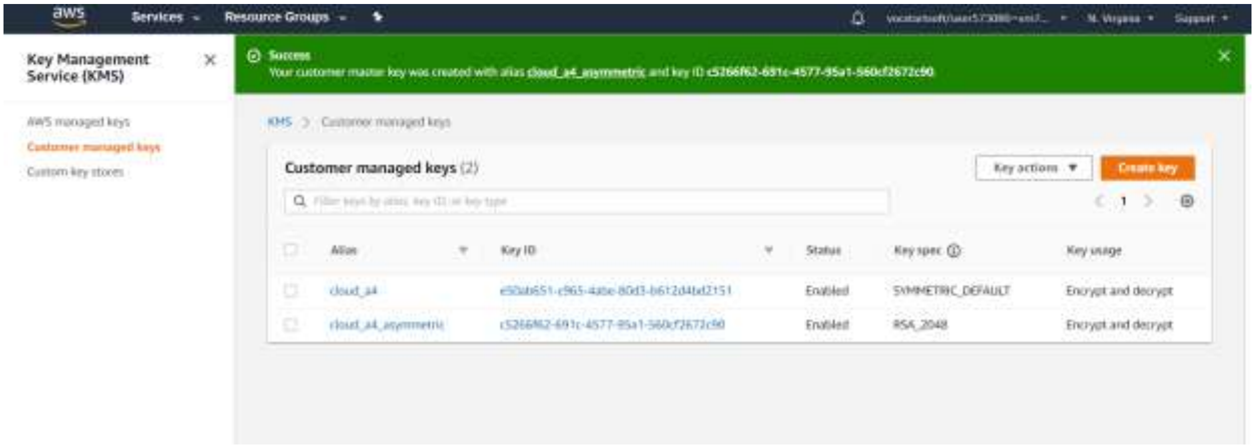
Figure 5: Asymmetric Labels



Review and edit key policy

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::178739460845:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

Figure 6: Asymmetric Key Policy



Success
Your customer master key was created with alias cloud_a4_asymmetric and key ID c5266f62-691c-4577-95a1-560cf2672c90

Customer managed keys (2)

Alias	Key ID	Status	Key spec	Key usage
cloud_a4	e50ab651-c965-4abe-80d3-b612d4bd2151	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt
cloud_a4_asymmetric	c5266f62-691c-4577-95a1-560cf2672c90	Enabled	RSA_2048	Encrypt and decrypt

Figure 7: Generated Keys

Section B

Migrating from legacy software to the cloud provides compelling advantages to the government and private industry due to the flexibility and scalability of Cloud Computing Systems (CCSs). Security concerns were raised because of the shared hardware usage of cloud tenants to run Virtual Machines. The major factors that affect the security status of the CCSs are security application used in the system, the hypervisor, protected measures, design patterns used for isolation and the level of protection provided by the Cloud Service Provider (CSP). The security controls issued by government does not provide complete assessment of CCS security status and integrity of specific cloud architectures. This paper contributes to the development of a cloud security assessment model, Cloud-Trust, which provides high level security assessments of IaaS Cloud Computing Services and Cloud Service Provides. Cloud-Trust uses unique attack paths that cover all the major elements of IaaS architecture. To summarise the CCS security status, Cloud-Trust provides two high-level security metrics, probability of an Advanced Persistent Threat (APT) can access high value data and the probability of an APT being detected by CCS security monitoring systems.

The identity and access management (IAM) controls and the network segmentation will be combined to form a trust zone. IAM uses hardware information, usernames, passwords, access control lists (ACL), active directory domain controllers, federated trusts, multifactor authentication, time limited codes to make access decisions. The network segmentation is based on VMware virtual network capabilities which uses both virtual network and physical firewall barriers to provide security to information in trust zone. Amazon Web Services uses virtual private cloud (VPC) to provide similar security feature. The configuration of domain controllers, firewalls, routers, and switches play an important role in the security of trust zone. Cloud-Trust is restricted to the cloud deployment model, Infrastructure as a Service (IaaS). So, the cloud tenant controls the guest OS whereas the CSP controls virtual machine manager, hypervisor, hardware, and network. In the CCS reference model, the subnets, firewalls, domain controllers, and internet access points separate the CSP management and security servers from cloud tenant virtual machines. Access to virtual trust zones is controlled by a CSP domain controller.

The CSP trust zone contains cloud management servers, software defined network controller servers, and IAM servers. To isolate the CSP management and monitoring systems from cloud tenant, CSP management systems communicate through a separate firewall. The security capabilities of modern firewalls include blocking IP ports and protocols, host-based intrusion detection systems (IDSs), keystroke logging, reverse web proxy servers, security incident event managers (SIEMs), and IAM servers. SIEMs is used to collect event data from security devices, network infrastructures, systems, and applications. The collected data can be analysed for user activity monitoring and compliance reporting. To identify suspect data flows, configuration changes, network performance monitoring tools such as netflow can be used. Apart from the security actions provided by the cloud computing service, physical protection measures, security awareness training, maintaining a vulnerability management database are some actions required for system protection and risk reduction.

Four cloud architectures are presented which are based on the Cloud-Trust model and uses software defined networking (SDN) for virtual machine networking. The first architecture provides very few security features such as single factor authentication, unencrypted memory pages, no network and CPU isolation. The second architecture has extended features like two factor authentication (2FA), time limited token code. The third architecture provides advanced security features such as restricted access for employees and 2FA. The fourth architecture is the most secure one with features such as encryption of VM images, encryption of memory pages and packets, temporal CPU isolation, application whitelisting, and CPU with trusted platform module (TPM). The TPM provides boot time management and remote attestation capabilities. Servers used in fourth architecture use signed BIOS.

The cloud computing service attacks can be categorised into outsider and insider attacks. Outsider attacks can be implemented by exploiting weaknesses in cloud access control mechanisms or by stealing valid credentials of a cloud user outside the cloud or by using valid credentials and legitimate access to the cloud. Insider attacks initiate onside the cloud where the credentials for at least one trust zone are exploited. There are different types of attacks explained in the paper. The VM CPU timing side channel attack is based on vulnerabilities of the virtual machine. In this attack, the advanced persistent threat (APT) gains access to the cloud for surveillance to obtain credentials by analyzing user’s inter-keystroke timings. SDN attack exploits the vulnerabilities in SDNs by accessing virtual machines in trust zone. The APT installs malware on the trust zone virtual machine that enables APT to control the hypervisor. By using the hypervisor, APT will collect credentials, network architecture, decryption keys from RAM. The VM attack through the HV is similar to the SDN attack. This attack proceeds by obtaining valid user credentials to access the virtual machine and compromise the HV. The Live VM attack begins by obtaining agency credentials from outside the cloud to gain regular user access. The APT then installs a malware to extract the file which contains hashed system admin password. The hashed password will be decrypted by APT to gain control of VM in the trust zone. VM migration attack is another common attack as virtual machines are migrated frequently to prevent overheating of servers and for optimal allocation of network loads to available resources. The APT obtains the user credentials to monitor network traffic and whenever a VM transfer is detected, associated packets are stored by the attacker. Data extracted from the packets will be used to compromise other VMs and gains access to agency gold data. The other types of attacks include undetected configuration modification, VM manager control compromise, CSP personnel with physical access, disk injection to Live VM, Live VM attack, and nested virtualization attack.

The Cloud-Trust security model has two Bayesian sub-networks, infiltration sub-network and exfiltration subnetwork. The infiltration subnetwork is used to assess the probability that an APT will be able to access the data in trust zone whereas the exfiltration sub-network is used to assess the probability that the APT can exfiltrate the accessed data. After examining the results from tests conducted on the four architectures, architecture 4 has the lowest probability of APT infiltration due to its encryption to protect VM images during migration. To conclude, the paper demonstrates the Cloud-Trust model to assess the security status of IaaS cloud computing systems by providing APT infiltration and detection probabilities. Additionally, Cloud-Trust can also be used to conduct sensitivity analyses of specific security controls, quantify the value of specific cloud computing system security controls.

References

[1] *Docs.aws.amazon.com*, 2020. [Online]. Available: https://docs.aws.amazon.com/kms/. [Accessed: 19- Apr- 2020].

[2] "What is AWS Key Management Service? - AWS Key Management Service", *Docs.aws.amazon.com*, 2020. [Online]. Available: https://docs.aws.amazon.com/kms/latest/developerguide/overview.html. [Accessed: 19- Apr- 2020].

[3] D. Gonzales, J. Kaplan, E. Saltzman, Z. Winkelman and D. Woods, "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds", *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 523-536, 2017. Available: 10.1109/tcc.2015.2415794 [Accessed 19 April 2020].

[4] "Using symmetric and asymmetric keys - AWS Key Management Service", *Docs.aws.amazon.com*, 2020. [Online]. Available: https://docs.aws.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html. [Accessed: 19- Apr- 2020].

[5] "About symmetric and asymmetric CMKs - AWS Key Management Service", *Docs.aws.amazon.com*, 2020. [Online]. Available: https://docs.aws.amazon.com/kms/latest/developerguide/symm-asymm-concepts.html#asymmetric-cmks. [Accessed: 19- Apr- 2020].