National College of Ireland

Protecting Virtual Environments with an Attribute-Based Encrypted Access Control System

MSc Research Project
Cloud Computing

Gnanendra Reddy Siripireddy
Student ID: 21169420

School of Computing
National College of Ireland

Supervisor: Aqeel Kazmi

National College of Ireland Project Submission Sheet School of Computing

Student Name:	Gnanendra Reddy Siripireddy
Student ID:	21169420
Programme:	Cloud Computing
Year:	2022
Module:	MSc Research Project
Supervisor:	Aqeel Kazmi
Submission Due Date:	28/01/2023
Project Title:	Protecting Virtual Environments with an Attribute-Based Encrypted Access ControlSystem
Word Count:	
Page Count:	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on TRAP the National College of Ireland's Institutional Repository for consultation.

Signature:	
Date:	15th December 2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Gnanendra Reddy Siripireddy
21169420

I. Introduction

Motivation of the document

As per project module guide, the document covers design, implementation, and evaluation for ABE-Model utilising algorithms on cloud hosting platforms. This setup manual defines the prerequisites for a ABE-Model.

Research Question: How could attribute-based access control become modified to safeguard virtual environments?

Objectives: - Attribute-based encrypted access secures virtual environments to avoid VM escapement. The ABE algorithm encrypts the VM VPN network, and we give responsibilities and policies to each VM in the cluster. After inputting credentials into Putty, the remote VM's lack of characteristics should prevent access.

Virtualization and Security

- Protecting servers
- Virtual machines Hypervisor services interruption security
- Virtual machines escape and Hypervisor security against software attacks
- Protect virtual services and vital services

II. Related Work

Security Implications

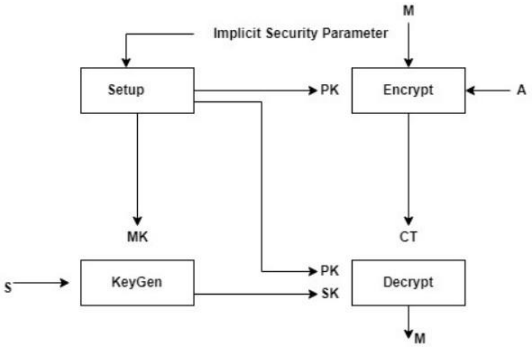
This research found many security issues in virtual environments. The user and cloud provider are responsible for cloud security due to the volume of data stored.

Attribute based Encryption

In this article, I have discussed the ABE Model and provided a description of attribute-based encrypting, including information on how it works, as well as a research study on a digital model of a typical hierarchical model.

III. Methodology

I have provided an explanation below on the operational model of the encryption method along with a diagram.



IV. Design Specification

System Requirements

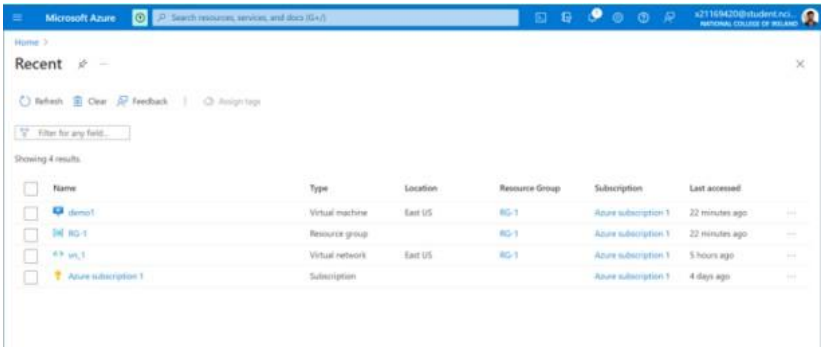
The system requirements for the suggested native machine implementations are shown below.

- Intel
- VMWare Workstation
- Mininet for designing virtual network
- Ubuntu Bionic (18.04 LTS)
- Python 3.0 - 3.8.4 for KP-ABE

Microsoft Azure Infrastructure

For the deployment of a virtual environment, the relevant cloud services are needed:

- Microsoft Azure Active Subscription
- Azure Virtual Machines
- Azure VNET
- Azure Blob Storage
- Azure Active Directory
- Ubuntu Bionic Machine Image



List of Virtual Resources

V. Implementation

The initial implementation will operate on an AMD PC with an A6 APU processor (2 CPUs), 8GB RAM, and 8GB Storage. Oracle Virtual Box virtual machines were used for the procedure. Virtual Box created a two-VCPU, 40-GB RAM virtual machine. The method defined a virtual network for VM communication. Due to AMD A6 APU's low system resources and virtualization constraints, cloud environments may use the technology.

Attribute Based Encryption in Cloud Infrastructure

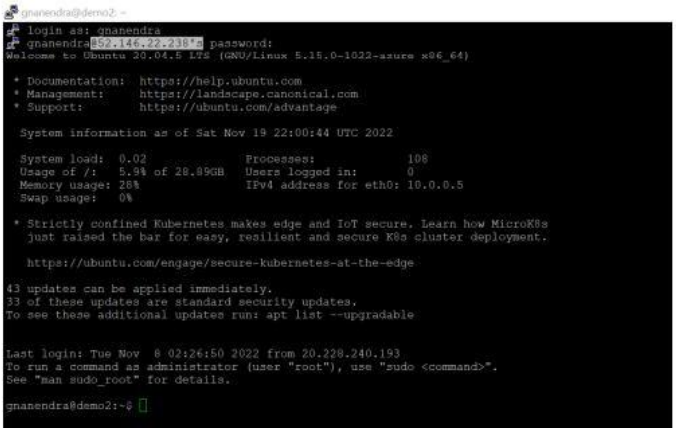
```
def main():
    pairing_group = PairingGroup('MNT224')

    cpabe = AC17CPABE(pairing_group, 2)

    (pk, msk) = cpabe.setup()

    attr_list = ['ONE', 'TWO', 'THREE']
    key = cpabe.keygen(pk, msk, attr_list)

    msg = pairing_group.random(GT)

    policy_str = '((ONE and THREE) and (TWO OR FOUR))'
    ctxt = cpabe.encrypt(pk, msg, policy_str)

    rec_msg = cpabe.decrypt(pk, ctxt, key)
    if debug:
        if rec_msg == msg:
            print ("Successful decryption.")
        else:
            print ("Decryption failed.")

if __name__ == "__main__":
    debug = False
    main()
```

The suggested methodology's attribute-based encryption algorithm for access control

VI. Evaluation

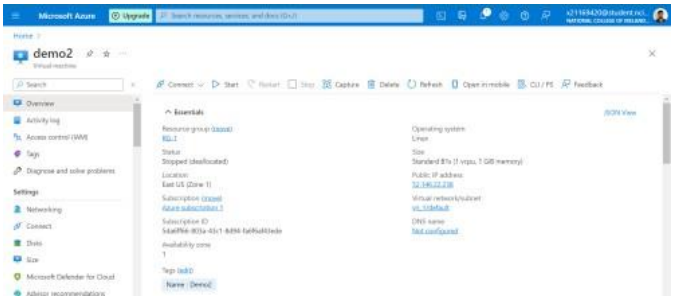
Here I have explained the Results of system after attaching the ABE-Model to the VM.

Accessing the network resources externally

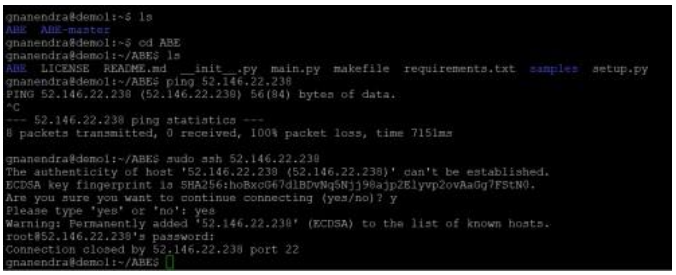


```
gnanendra@demo2: ~
login as: gnanendra
gnanendra@52.146.22.238's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-1022-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Nov 19 22:00:44 UTC 2022

  System load:  0.02              Processes:             108
  Usage of /:   5.9% of 28.89GB   Users logged in:       0
  Memory usage: 28%               IPv4 address for eth0: 10.0.0.5
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

43 updates can be applied immediately.
33 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Tue Nov  8 02:26:50 2022 from 20.228.240.193
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

gnanendra@demo2:~$
```

Establishing the connection without attaching the algorithm



External Virtual Instance



rejection to provide access to the second Virtual Machine