Protecting Virtual Environments with an Attribute-Based Encrypted Access ControlSystem

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:	15/12/2022
Project Title:	Protecting Virtual Environments with an Attribute-Based Encrypted Access Control System
Word Count:	
Page Count:	24

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 keepa 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):	

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

Gnanendra Reddy
Siripireddy21169420

Abstract

The primary technology behind cloud infrastructures has been virtualization. Commodities both hardware and software technologies were quickly deployed asa consequence of the rising need for computing. The needs for computing have indeed been met by virtual machines, which have consolidated hardware from dis- parate settings. Virtualization methods that use a decoupled architecture provide special security advantages. Moreover, the complexities of the technology's deploy- ments and design implementation results in brand-new infrastructures risks and vulnerabilities, such compromising VMM and Virtual Machine escapement. The study's goal is to provide a unique way for isolating virtual computers inside a network and controlling network access using an enhanced major policy Model for attribute-based encryption.

Contents

List of Figures

1 Introduction

Cloud is a highly innovative technology. Users can utilize computation, network, storage, etc. for diverse purposes. Cloud computing's improvements promote speedier innovative thinking at scaling of high availability. Cloud technology provides cost-effective, scalabil- ity, and dependable compared to conventional IT services (on-premise). Cloud platforms reduce enterprises' TCO. Cloud's strength is virtualized. Cloud Technology offers on- demand access to a group of services via an existing network, NIST [1]. On-demand resources, wide network connectivity, quick flexibility, service availability, metered ac- cessibility are cloud computing features. Existing IT platforms enable a few of these traits, but lack cloud adaptability.Cloud technologies' 'pay as you use' strategy decreasesinfra maintenance costs. Various cloud-based infrastructures provide various services as study grows. It increases the number of cloud - based services that can meet soft- ware needs.Public, private, and hybrid cloud systems are implemented. Public cloudis cloud resources open to several organisations, however private cloud is limited to a specific company, which enhances security. Hybrid clouds allow enterprises with current IT infrastructure to utilize cloud resources. Clouds are dispersed ecosystems. Distrib- uted information services, storage and compute, HPC, and other distributed technologiesdrove cloud resources in business platforms.

High demands for cloud resources involves the effective networking such as storage and networking for web-scale computation. Cloud computing services rely heavily on virtualized resources. Virtualization lets computational cluster operate on a physical machine's device. Hypervisor lets virtual computers accessing physical machine hardware. To meet todays modern computational demands, computers must be able to handle web-scale petascale operations. Distributed system services in warehouse-scale data centres enable parallel cloud technology. High-performance and high-throughput computing are essential that are powering computing technologies.Cloud platforms are formed by cluster of linked computing nodes. Figure 1 shows that cloud applications include virtual computing, storage, network, and compute resources. Such networking resources communicate to hardware.Pay-as-you-go users obtain services through internet. Whenever an user require a services, that service gets paid. Vm services might be virtual or physical. Cloud-based virtual instance controlling infrastructure. The hardware underlying Virtual machines are partitioned and virtual so other applications may utilise it. Machines virtualization allows cluster, grid, and cloud computing systems. Figure represents that paying clients may utilize such virtual resources. Virtual networks require powerful security measures to prevent access to the core physical infrastructure. Physical Infrastructural accessibility may harm virtual environments.

> ***Research Question*** *: How could attribute-based access control become modified to safeguard virtual environments?*
>
> ***Objectives:***
> *1. The goal of the current effort is to prevent VM escapement by securing virtual environments using attribute-based encrypted access.*
> *2. We use the ABE algorithm to encrypt the network inside the VM VPN, and we assign certain roles and policies to each VM within the cluster.*
> *3.Since the external VM has no properties, it is anticipated that access would be refused after entering the credentials into the SSH client Putty.*

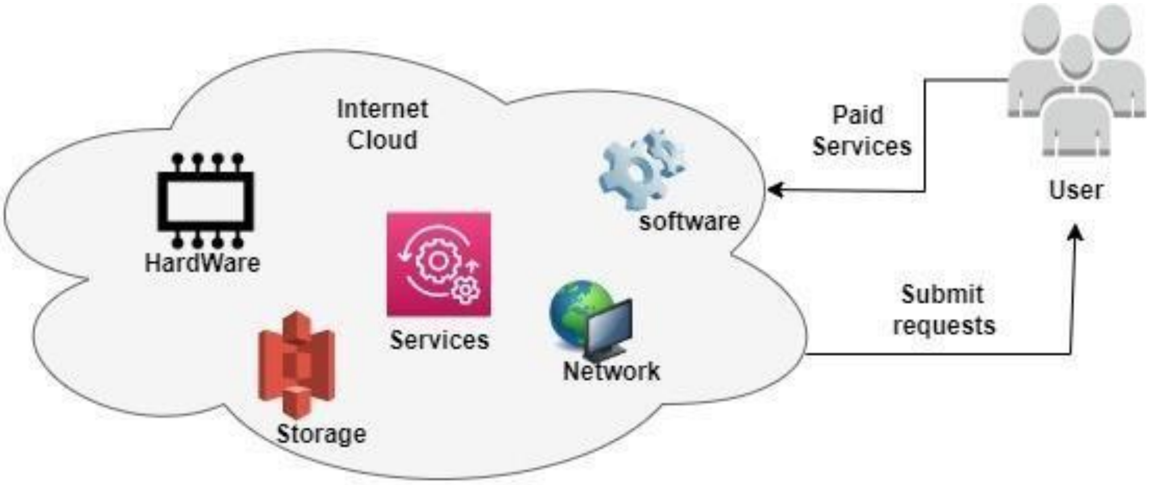


Figure 1: Paid virtual resources in a cloud service model.

1.0.1 Virtualization and Security

In a traditional physical machine, resources are in hardware, or systems space. The OS handles overall hardware accessibility in system space. The apps able to run on the os classified as user space. Applications make clients request to the OS, which controls and allocates services. Than a real machine, machine's virtualization may create numerous OS instances within the same hardware. Vms are software packages that may execute application programs in a virtual environment. The packages may be deleted afterwards since it doesn't change system dynamics. As vms depend upon this host machine's hardware, instruction must executes in system space. Vms over an abstraction layer behave like actual machines.

A Hypervisor manages vm privileges. It generates trap to stop systems call synchronously. Improper behaviour may threaten the ability to access system space at this level. Virtual machine monitor provides the guests apps' physical services. Distributed systems use virtual infrastructure for effectiveness and lower servicing costs. Virtualization privacy is widely debated. It covers processes techniques to secure virtual environments. Confidentiality in these infrastructures affects SLAs [2]. Vulnerabilities include;

o Protecting servers

o Virtual machines Hypervisor services interruption security

o Virtual machines escape and Hypervisor security against software
attacks

o Protect virtual services and vital services

Virtual machines, physical infra, and networking have security flaws. DoS attacks, MITM(Man-in-the-middle) attacks, etc. are frequent dangers. Attackers could utilize the network to reach virtual machines launch Vms escapement assaults. Closely linked infrastructure could have single points of failure that might benefit invaders despite the abstraction's extra safety layer. Cloud services provide a collective responsibility paradigm that outlines the clint's responsibility to safeguard cloud-stored apps and data.

Therefore, clients must define personalised, secured, and scalable access rules [20]. The cloud's information at rest and during transit are vulnerable. Networking security is essential when migrating data from one Vm to the other and from one Vm to a real computer. To receive encrypted information, the data owner or admin must establish a public key. Public key encryption secures the enviroment. Providing user-specific keys adds complexity to messages in transit [3]. Attribute-based encryption uses security keys to construct characteristics that handle complexity. Earlier studies proposed attribute-based data encryption methods. Key attributes of attribute-based encryption paradigm include:

Data Privacy Prior to being uploaded to the cloud, data may be encrypted by the client. There is a possibility that access to unauthorised files may be banned. Only usersare able to access the encrypted data stored in the cloud since cloud service providers adhere to the shared responsibility model. Regulation of Access, Users fall into a varietyof types, each of which is subject to a unique set of access rights and constraints. In order to limit each user's access to the data.a unique policy will be issued to them. Scalability, Because public cloud applications are made accessible to many users, the system must be able to effectively handle fluctuating work loads.

This means that data accessibility must be consistent regardless of the number of users that are accessing the information at the same time. Collusion-free, Encryption results in attributes that are unique to each user. These user-specific characteristics are normally defined during the creation process. Information cannot be obtained via the properties of other users. Each of these attributes is produced on an individual basis in order to provide authorised users with unambiguous access.

2 Literature Review

Although cloud networks excels at delivering storing DB instances, and flexi- bility and scalability compute, cloud technology remains one of most important areas of study. Managing virtualized networking environments involves a wide range of policy, tools, and login credentials, but also is regarded like a sub-domain for informational safety and network safety. Development of Virtual servers, computational services, and infrastructures includes not just physical hardware but additionally the virtualized networking and many other aspects. Dubey.A and Pal.S accepted that virtualisation was detrimental to both business and open-source software [4]. It is already been noted that now vulnerabilities posed from technology aspects on virtualization could be exposed threats to security and its countermeasures. Malware problems are contributing factor to such vulnerability, in addition to aspects that are unreliable in the virtualized architecture. An OS must buildits belief upon both virtual-machine monitor as well as machine's hardware [5]. Al-Aqrabi et al suggested a data cloud environment to safeguard the virtu- alized resources from potential dangers. Various cloud applications are imple- mented to prevent security at- tacks by isolating the cloud technologies in differ- ent operating regions [6]. It is crucialto secure the storage systems.

Virtual computers and dedicated servers must be able to obtain sensitive information securely via authorisation and string operations in line with the suggested de- sign. did play multi certificates a part towards accomplishing an attribution of believe for PKI entities. In order to achieve personal information coloring and technology watermarking, services records must be shielded from virtual services It's designed to separate login from provider. The system where the virtualized infrastructure is located may be vulnerable due to its strong coupling. Virtual machines are linked to the actual resource. the cloud's resource Infrastructure projects must be protected in order to prevent service interruption.

2.1 Security Implications

The research in this field have noted a number of problems with virtual environments' security mechanisms. Given the amount of information stored in the cloud technology, the consumer and the cloud provider bear responsibility for cloud security. Distinct providers of cloud services have established various network guidelines for managing accessibility. Lists of access controls may be established quickly following the deployment of a client virtualized environment, whether depending on the needs of the client or from the dashboards that the service provider provides. It is possible to limit who has access to the information saved in cloud storage by using cryptographic techniques. [7]. Networking integrity is important in cloud settings since the majority of virtual machines there are linked to one another, creating a single source of failure as in scenario of a network break- down.

The vulnerabilities of a hypervisor in addition to the dangers brought on by both the low and strong virtual implementation have been discovered by Ahuja et al by examining the features of safety in Vms depending on Xen and KVM[5]. As previously indicated, the vms monitoring is essential to the virtual networks driving business cloud services (Hypervisor) Because it serve also as sole conduit here between hardware and the digital

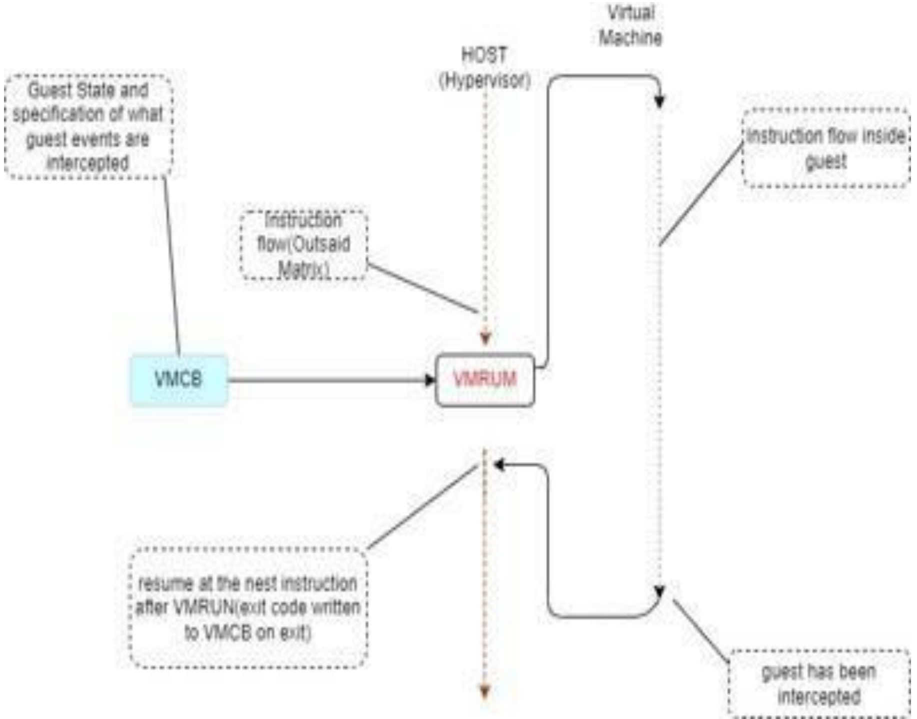

Virtual Machine
HOST (Hypervisor)
Guest State and specification of what guest events are intercepted
Instruction flow inside guest
Instruction flow(Outsaid Matrix)
VMCB
VMRUM
resume at the nest instruction after VMRUN(exit code written to VMCB on exit)
guest has been intercepted

Figure 2: Secure virtual machines (SVM)' core components are the VMRUN commands as well as the guest instructions

PCs, especially virtual machine monitors, are very vulnerable. These are the only points at which a breakdown might possibly occur. It was emphasised how important it is to use packages such as trustworthy platforms module (TPM) in order to maintain the authenticity and dependability of monitoring virtual machines. It is frequently referred to as a chain of belief, and it is something that delivers assurance of the legitimacy or status of the programme as well as the hardware components[8].

The hyperjacking of virtual machines (VMs) and VMM-caused interventions are two examples of attacks that go beyond the ordinary damaging assaults that are discussed here. The practise of secretly moving an operating system from a physical computer to a virtual machine (VM) while the VM is starting up or functioning is referred to as "hyperjacking vms." It is feasible to move the operating system from a physically based environment to a virtual one by inserting the virtual machine monitor under the surface of the operating system. VMM rootkits, in general, are considered to be very dangerous threats because of their capacity to completely compromise an operating system. The altered system startup documents and page junk raw disc scans are, in fact, the primary components of the attack platform used by these rootkits [9].

The operation route that must be followed between admin PCs and even the servers is shown in the graphic that was just presented. In point of fact, the VMRUN rules are the ones that are sent by the hypervisor. These recommendations for the client are being carried out in such a way that they may be intercepted by workers of the hosts, and it will continue only after orders have been carried out. This is how the specifications are being carried out. The VMM may be placed into the instruction cycle in order to monitor it, and the captured actions can subsequently be carried out as virtual instructions by the hypervisor once they have been monitored. Interventions made with the use of VMM The command that the hypervisor has over the instances allows for the participation of VMM to be practical. When the VMM obtains the system's inputs, it adjusts the already-existing programme and then modifies the guidelines for its own system. When observing the actions of Machines, hypervisors and virtual machine monitors (VMMs) use an introspective strategy.

2.2 Attribute based Encryption

As was said before, customers are given the option to encrypt any data that is put into the cloud, and the cloud service providers will not have access to or control over any data that is encrypted and uploaded by users. If for any reason the user decides to make their data accessible to other users or even the cloud service provider, the application will generate a public key that can be used to decode the data that has been uploaded. Additionally The power to control the virtualized environment is held by a cloud services provider. The management of client access to cloud services is possible via the use of encryption architecture.

The encrypting paradigm that was employed by earlier approaches ran into certain challenges, and one possible solution that has been proposed is to encrypt information depending on the properties of the data. In its most basic form, the encryption method creates characteristics for the identification of the user. These qualities are given to the users so that they may access networks, encrypted data, and anything else that could be involved. The existing method of encryption using public keys might be replaced with attributes. As a consequence of this, it is possible to use them for encrypting as well as decrypting data. When employing public keys for encryption and decryption, additional computational and networking activities are required to identify clients [11]. These actions are connected to the client identification process.

A key issuing authority is responsible for producing the keys that are essential for clients to input the same necessary facts [12]. Both the characteristics' public and master keys have previously been predefined before they are used. It is necessary for the administrators to get an advance copy of the user profile along with any connected information. It is necessary to encrypt the information using public keys and the descriptive qualities since the list of characteristics has to be kept up to date at all times, regardless of whether or not there are new clients. Using a method similar to encryption with a public key, the users may be able to decode the information by using the keys that have been provided to them.

However, the number of features in the list must correspond to the number of characteristics that are stated in the public key. D. Boneh and his colleagues [11] presented a fundamental policy feature that is based on the access-control model. The purpose of the concept was to provide access restrictions that would make it possible for specific persons to get the data or cloud service they want if they are in possession of private keys.

The major objective of the project is to provide users with more flexibility on the encryption technique that depended on the system's features and to make it easier for users to get the permissions they need. The user is not responsible for decrypting the information since the private keys are configured together with the rules at the time of setup. If an administration or the key issuing company does not know and trust its customers, then unnecessary overheads may emerge, making the strategy less successful overall. The bad qualities cannot be conveyed to users group or individuals since the idea is based on a monotonous key policy model. This prevents the communication of the qualities. Furthermore, an authorization agent is responsible for managing permissions in cloud environments [13].

Chan, T. further observed the existence of the Virtual machines authorization agents in addition to the authorisation enforcers as components of the administrator virtual machine (vm). These kinds of organisations create each and every safety procedure that is implemented in clusters. [14] provided a way to conform to security requirements in consideration of the virtualization that was based on the Xen hypervisor. The server-first strategy that was used in the past established secure metrics against threats posed by co-residents and attacks. It is possible to employ key strategy encryption to restrict access control to specified networks, despite the fact that it requires the construction of a set of user characteristics and is regarded as being demanding in terms of the amount of overhead it requires [15]. [Citation needed]

Wan, Z., and Liu, J.E. suggested a method for authentication mechanism in cloud services using hierarchy-based confidentiality methods. Both encrypting and decryption of information in public cloud services and virtual infrastructures may be accomplished by blind encryption algorithms [16]. In order to protect the access rules and credentials from malevolent clients, confidential information is kept about them. In business clouds, Hierarchical architecture becomes visible in access privileges, and developed model provides insight into the privacy-preserving approach across applications. Hierarchical password

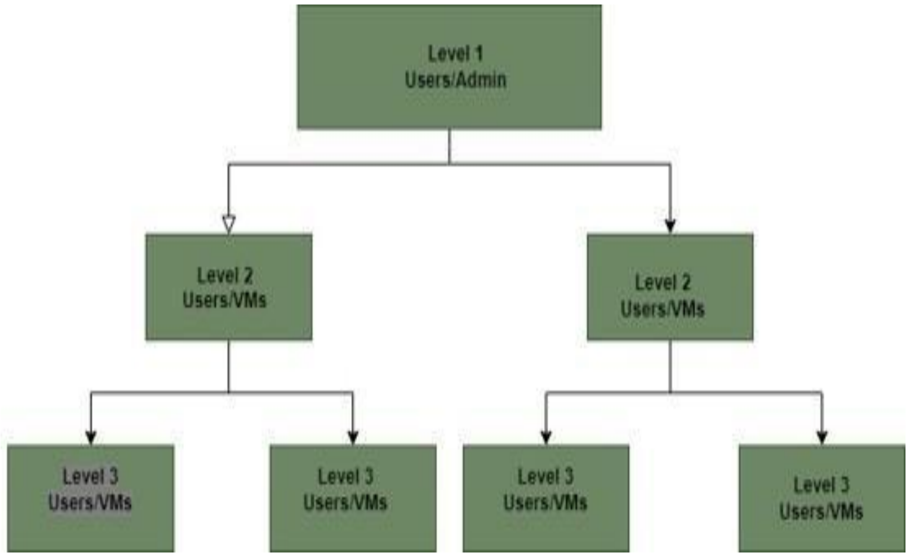


Figure 3: A virtual representation of a typical hierarchical model.

protection may be proven to increase protection for cloud infrastructures and the networkit is linked to in comparison to encryption method that is relies on characteristics. In Figure 3, this hierarchical model is shown. Virtual servers or clients are the networking objects at every layer that call for networking access control. One sees that the level 1 users manage the nodes and at lower levels. A networking object may, as was already indicated, become an user of a virtual server.

To access the services, VMs, or datasets, the clients or VMs will need identity until they are given authorization to a property that has been predefined by the administrator. It is comparable to the objects that are located on level 3 of the hierarchical system. If they were made through a node in level 2, which was the case, then they would be constructed and given an attribute in order to get access to certain other parts of a hierarchy. Enhancing the hardware permissions in the Linux kernel is one method that has been identified as having the potential to provide increased levels of security [17]. According to a project called bluepill[10], virtual machines have the potential to "bluepill" the hypervisor. This is done by monitoring the host servers' commands and then executing them on the hypervisor. The physical instance would be converted into a virtual machine as a direct consequence of this action. Management of access control seems to be a significant consideration for networks that allow anybody to connect. Controlling access to virtual servers housed on these networks is very necessary in order to protect the secrecy of a virtual environment.

Encryption and decryption of data as it is being sent might potentially improve the security of the infrastructure. An attribute-based encryption paradigm is used in dispersed networking to encrypt the cross-communications that take place between nodes. Because the provider of cloud computing delegates power to clients, it is the administrator's responsibility to create accessibility roles and rules that clients and applications must follow in order to connect to cloud services. In addition to this, it is of the utmost importance to monitor and verify the database host's accessibility [12]. In addition to this, the key management-based encryption architecture has shown that it is capable of effectively preserving the security of the network. The purpose of this article is to provide a method for access control that is safe and dependable via the use of encrypted user information that is transported across different virtual computers. The proposed system is built from the ground up on the attribute-based encryption paradigm, which serves as the underlying structure.

3 Methodology

Virtual infrastructure privacy can affect cloud settings, according to study. To provide uninterrupted resources, business cloud technology solutions must handle privacy issues. Distributed system contain several dangers weaknesses due to virtual element connection. Vms may jeopardise infrastructures [10]. Application virtualization software platforms provide security, but for every virtualization has its own privacy threats. Complicated dangers like ”Virtual Machine escape” are serious. Massive computational cluster’s Virtual machine escapes may damage infrastructures information. Virtual machine interceptions occurs when a hacked Virtual machine on networking accesses a networked Virtual machine as intercept operations [19].virtualisation powers cloud computing,Virtualized security considerations include infrastructures, networking, storage, and others. To decentralise virtualization administration, vms were formed as independent entities. Decentralized access identity management pose security risks. Virtual machine escape attacks occur frequently despite isolated networking, federation access control, and isolated VMs [20].

Networking encryption approach [5] secures vms hosts operations. It cannot isolate Machines. Virtual machine escapes attack expose entire networking Virtual machines. Threats may capture network activity. Attribute-Based Encryption helps secure dispersed network. An administrator gives every clients in an user-group a secret key using security key for encryption. Every user secret key is shared with the group. The administrator key unlocks encrypted information for clints. Key policy attribute-based encryption [18] creates user keys as the previous method. Users get encrypted keys as attributes. Users Virtual machines receive access keys under this circumstance. Cloud providers many access management options to safeguard Virtual machine accesses. Amazon AWS1 and Microsoft Azure2 give role for vms to utilize cloud services. Admins establish grant such roles. OpenStack uses Key Stone to provide public keys to clients policy for vms.

3.1 Network Encryption Algorithm

This strategy is to produce encrypted characteristics via treating Vms to be clients in order to control the virtual network access. This encryption method is based on [21] Attribute-based encryption technique. This model is intended for online cloud environments. It is noted that the encryption method is effective for control accessing to modest data repositories. Consequently, analogous encryption concept may be evaluatedin virtual settings. Therefore, every organization as in virtualized environment must have complicated security regulations set. Its encrypting system is founded on a hierarchical attribute-based approach that protects confidentiality [16]. Several factors are evaluatedto handle the system’s timing and spatial complexity. Two organizations occur in a typ- ical network: a cloud provider or admin (trust authority) and a users, who might be termed a recipient.

A information provider is accountable for providing networking user have accessing to the delivered information. A trusted authorities is indeed the organization inside a network that allows centralize safe administration of a clusters node. A trusted authorities plays a key role in ensuring the safety of a de-centralised clusters of compute nodes when virtual environment are considered. A dministrator is regarded as a trustworthy source here on algorithms. The organization creates clients’ private keys for encrypting and decrypting information. Such private keys were produced depending on the characteristics of a public key or the master key.

The properties are produced preset for all networked devices. When new users were started adding, attributes are produced, but they are not included to a listing of preset attributes.The authorities will thereafter modify the attribute lists in order to change the public key. In addition to the qualities, the admin encrypts the information using a secret key. The individual will be able to decrypt the information using the administrator- supplied secret key. Nevertheless, the individual attributes must correspond to a lists of characteristics associated to an encrypted files. In virtual environments, inter-device communications may be encrypted to keep user access control inconsistencies across Vir- tual machines. The method is composed of four distinct implementation components. Each component of the algorithm is conducted to perform exclusive and operation. The algorithm consists of four divisions: setup, Keygen, encrypt, and decrypt. Two bilinear sets, G1 and G2, are explored to illustrate the approach. The sequence of the these group is prime, and ’g’ is the generator of G1. The notation for the bilinear map is e:G1XG2-G2, where d seems to be the threshold.

Setup The administrator chooses randomized values for key generation. Let the numbers t1,t2,..., tn,y originate from set Zq. All digits are chosen in accordance with the following expression to create a public key.

$$PK = (T1 = gt1; ::::; Tn = gtn; Y = e(g; g)y)where, MK = (t1, t2, ...tn) \tag{1}$$

MK is the master key created by trusted authorities (Admin) for such list contained in t1 through tn.

Keygen The users’ access structure in the private key may be expressed as

$$A_U -_{K\ P}; PK; MK \tag{2}$$

The administrator or key-generation authority generates a private key component ’U’ for each node in the access structure. The degree of d-1 of the polynomial ’q’ is chosen arbitrarily such that q(0) = y. Admin produces the private key components for every leaf node ’x’ in the access hierarchy. These are the components of each private key:

$$Dx = g^{(qx(0)/ti)} \tag{3}$$

”i” indicates the user access node. The private key is then associated to user characteristics and sent to the user or virtual machine (VM).

Encrypt The administrator picks a random number from the list of uniform random numbers Zq in order to encrypt the data. The encrypt method encrypts the specified message M using the bilinear group G2. Attached to the message ’M’ is a collection of characteristics ’ACT’. The encoded data may be presented as follows:

$$CT = (A_{CT}, E = MY^{s} = e(g, g)^{ys}, E_i = gtis_iA_{CT} \tag{4}$$

Decrypt The method for decryption may be implemented as a recursive algorithm. It utilises the encrypted data, the user-supplied private key(PK), and the end-node credentials specified in the user access key. The method then determines whether the produced number I matches the number specified in the user’s private key’s access structure. If ’I’ does not correspond to the private key, the decrypt-node function is called which is denoted by

$$e(D_x; E_i) = e(g; g)^{s.qx(0)} \tag{5}$$

If a random number I doesn’t really match the user’s private key, the decrypt method is run, but incorrect output is returned. Moreover, when I does not match the leaf node, the decryptnode function evaluates all the child nodes and calculates the values of e(g;g) s.qx (0). Calculation is performed by applying the called function to the root of the access control list.

$$e(g; g)^{ys} = Y^{s} \tag{6}$$

Lastly, the decrypted message or, in this instance, the VM access value may be acquired as

$$M = E/Y^{s} \tag{7}$$

The diagram depicts the workflow of an attribute-based encryption technique. As stated before, the method consists of four distinct modules that each fulfill a specific function. After the algorithm’s elements, the setup module has responsibility for specifying the data restrictions (Security Parameters). The administrator gathers user information and login permissions before generating characteristics using random integers. The keygen section of a method establishes access restrictions for every networking item generates access control keys and now the master key (MK) for administrator access. Regarding cloud services, the created security keys (SK) are distributed to both users and services (Virtual Machines). In addition to a secret key, the Attributes (ACT) used to encrypting the information are also supplied to users. The users with correct qualities and the security key are capable of accessing the necessary encrypted data part. Virtual machines acquire access to Virtual environments utilising the characteristics and security key policies set during in the services creation. The programme verifies if the given security rules match the properties supplied by users and virtual machines (VMs). Users get a decryption message to acquire access once encrypted with the aid of characteristics [21].

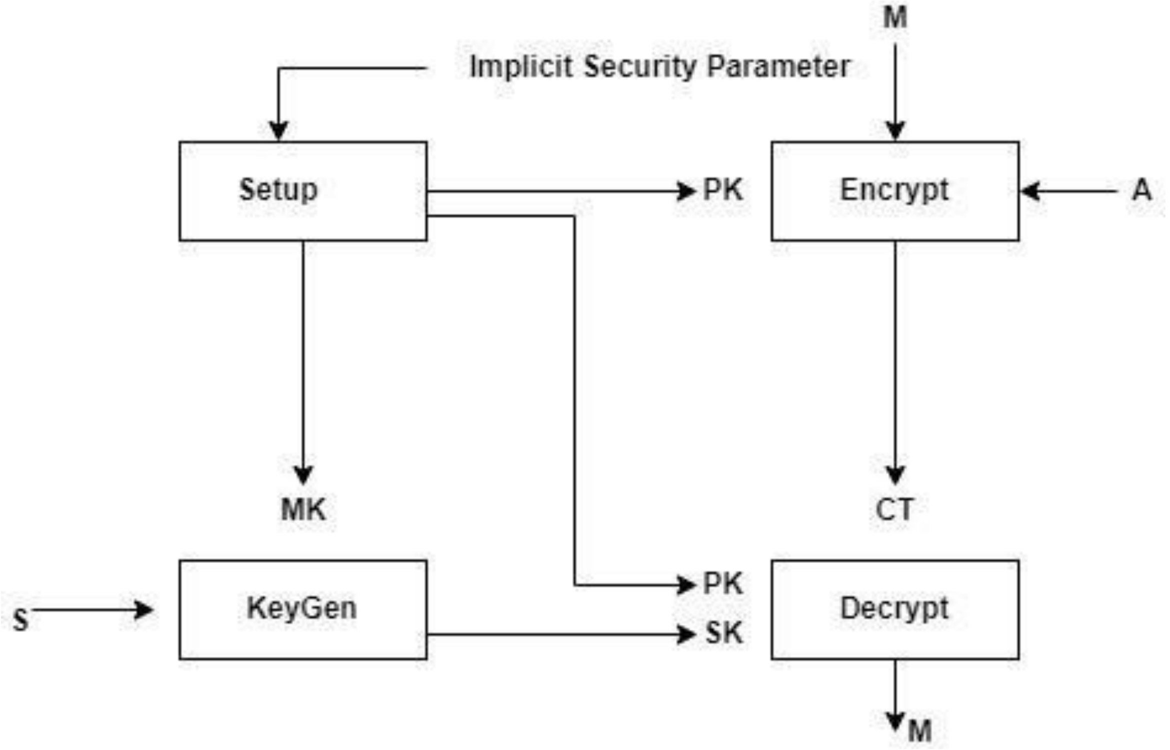


Figure 4: Working Model of ABE scheme

3.2 Attribute based encryption for Virtual Environments

Virtual machine isolation strategies vary depending on the kind of virtualization. Usually, business clouds feature a network of vms including an unified hardware or independent system or system components. But, isolation of every vms may be accomplished by modifying the os kernel in numerous ways. The administrator-generated secret key is connected with access control and encrypted info coupled with a set of attributes maybe used to build file permissions for access control and accessibility of services in cloud platform in a safe reliable manner.Both decrypt and encrypt data, the qualities specified when encrypting the information must match the attributes built into the user's access keys. Implementing this may separate virtual computers and restrict access to other vms within the same network. The escaping VMs must have accessibility to a secret key characteristics produced during data encryption. According to [8], the implementation may be conducted on virtual infrastructures. Python 3.0 is used to execute the technique. The original encrypting strategy was derived from the created attribute-based encryption scheme, with the adaption including the key encryption policy initiatives specified in [21]

4 Design Specification

The system requirements for the suggested native machine implementations are shown below.The system's needs served as the foundation for developing the implementation building standards. Cloud services became taken into consideration because of processors restriction. The approach appears to being put into practice on Azure VMs.Our implementation's flow chart is shown in Figure 3. A dedicate network is taken into consideration while deploying the virtual servers to construct separate VMs. Each virtual servers have attributes and keys defined for them. When defining access permissions, Virtual machines are taken into account as customers. After specifying the security permissions, the Virtual machines are generated. The Virtual machine is given following policies. The Virtual machines utilize the keys and characteristics to obtain the network's permissions. It protects the virtual machines' confidentiality. Is if deployment of a Virtual machines is unsuccessful, every design of a Virtual machines is modified in accordance with needs. Virtual machines have been hacked or have escaped from custody must have network access. Despite being linked to a similar network, these Virtual machines becomes external to it, therefore the administrator must grant them permission. After that, the privacy may be assessed.

The virtual network, as well as the Virtual machines, may be modified and they might be launched again for stricter security permissions is if virtual infrastructure isn't really protected sufficient. Virtual Network is essential for ensuring resources isolates in the project execution. VPNs may limit access from outside parties towards the networking, and infrastructure created in these kind of networking are linked to a certain networks. Security groups(SG) with restricted internet connectivity usually established after the routes were configured. TCP inbound rules HTTPS keep SSH ports open. In Azure, virtual machines are generated, one of which is the administrator. In Ubuntu Bionic, the encrypted method is applied in Python 3 using several packages.

4.0.1 System Requirements

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

- Intel or AMD X86-64 architecture with (VT-X, VT-D) Virtualization Support
- VMWare Workstation
- Mininet for designing virtual network
- OpenDayLight (Optional) to monitor network traffic
- Ubuntu Bionic (18.04 LTS) or Linux X86-64, Libvirt
- Python 3.0 - 3.8.4 for KP-Attribute based encryption

The X86-64 platform of AMD or Intel, that can enable virtualization technologies, is selected. Because Intel CPUs have hypervisors, virtualization is feasible. Virtual networks are designed deployed using Mininet. Virtual servers were deployed utilizing VMware Workstation to evaluate the vulnerabilities. A reason to choose VMware above Oracle Virtual Box is can handle activities between guests and hosts as well as make system evaluation simpler. The relevant cloud services are taken into consideration becauseof various native machine constraints.

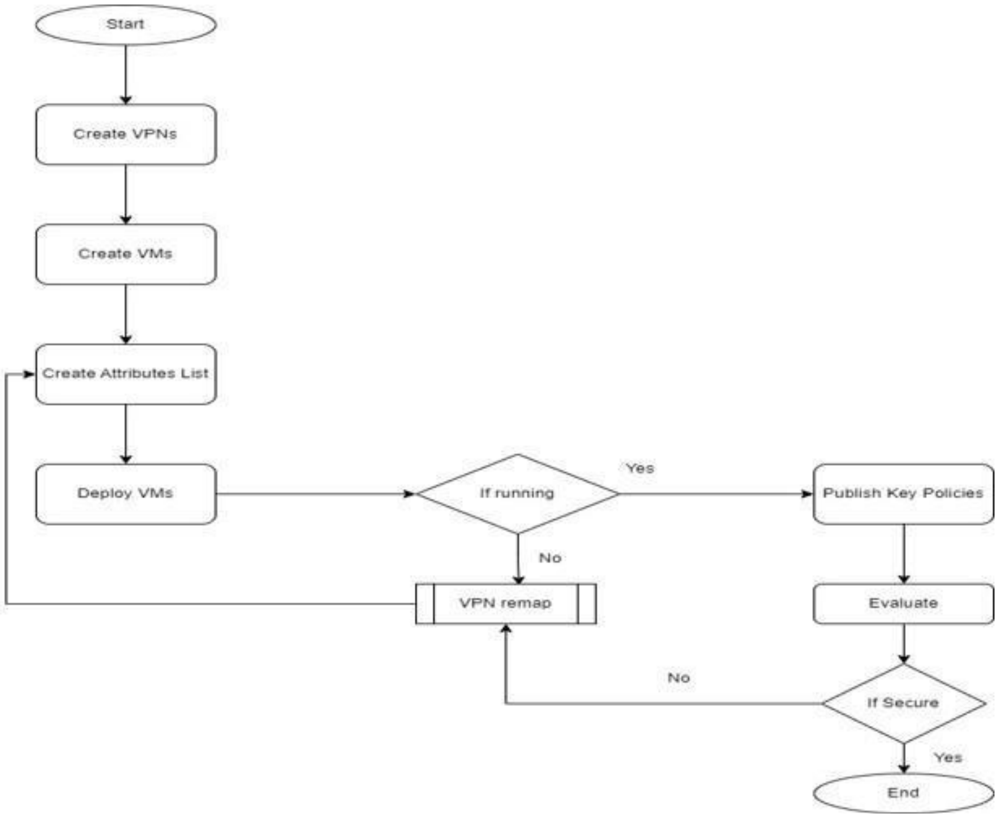


Figure 5: Flowchart for implementing a key policy attribute-based encryption model

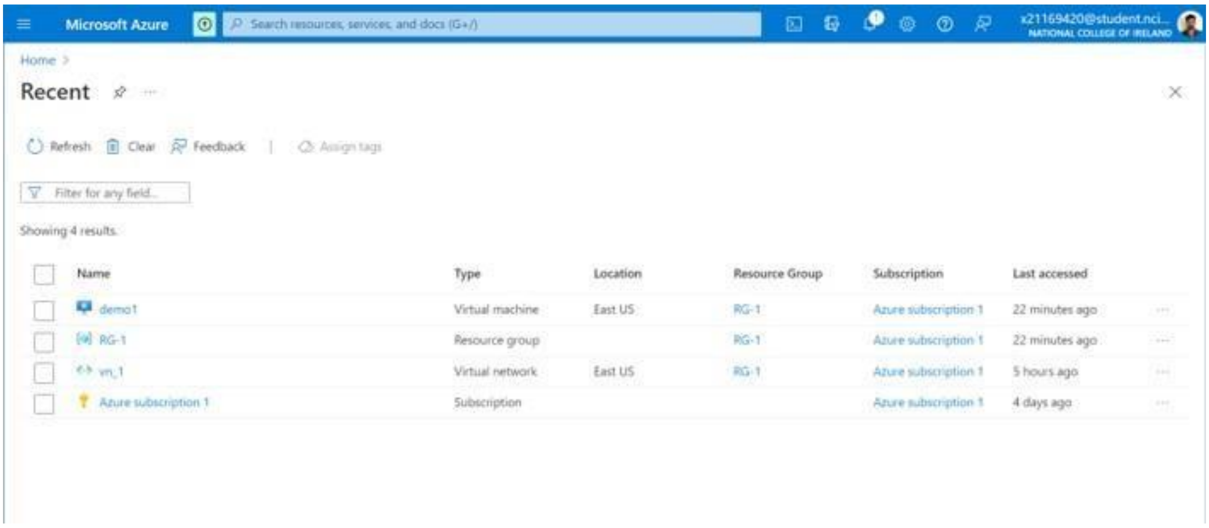
- Microsoft Azure
- Putty or Windows PowerShell with Azure Modules and Perl
- Azure Virtual Network
- Storage for VM volumes
- Ubuntu Bionic (18.04 LTS) or Linux X86-64
- Python 3.0 - 3.8.4 for KP-Attribute based encryption
- GCC and wheel packages for dependencies

4.1 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

Virtual Networks were built in the way of achieve better access to the infrastructure after it was installed, as seen by the installation flowchart in figure 3. The Networking in Microsoft Azure console are used to construct Virtual Networks. A collection of services



Showing 4 results.

□	Name	Type	Location	Resource Group	Subscription	Last accessed
□	demo1	Virtual machine	East US	RG-1	Azure subscription 1	22 minutes ago
□	RG-1	Resource group		RG-1	Azure subscription 1	22 minutes ago
□	vn_1	Virtual network	East US	RG-1	Azure subscription 1	5 hours ago
□	Azure subscription 1	Subscription			Azure subscription 1	4 days ago

Figure 6: List of Virtual Resources

established on Microsoft Azure is shown in above Figure.

The formed networks would include pre-configured security groups subnets. In order to receive data coming from different VMs on the networking, the security groups were redesigned to allow inbound traffic via HTTP, TCP, HTTPS, and SSH port's. To decrease the amount of network participants, a tiny CIDR block is used to form the subnets. A multi purpose VMs of type standards B2ms with 2 vCPUs and 8GiB of RAM was selected for the implementation in order to set up VMs in the cloud. For the purpose of allocating IP addresses from various CIDR blocks, 2VMs are built within a networking with separate subnets. Each VM will have greater network isolation under this manner.

As they are hosted within the same networks, the VMs generated in VNet would be able to communicate with one another. When being utilised in an application development environment, both machines will be able to communicate with one another. The capability of the machine to communicate is evaluated whenever it establishes a connection to SSH using the public key that was created exclusively at the time the VM was created. Both of these computers have the Ubuntu Bionic 18.04 operating system installed, but each virtual machine has its own hard drive for the machine image. The distinction between two Virtual Machines at this level is that one of them was produced in the form of a hosting while the other was produced in the form of a user. Through the use of Active Directory, tenancy rules are implemented across all of the virtual machines. Accessibility standards, such as owners having unrestricted access, were implemented to ensure uninterrupted service. All of the assets have been consolidated into a single category and are being stored in data centres in the eastern part of the United States.

5 Implementation

The first implementation will run over an AMD computer equipped through an A6 APU processor (2 CPUs), 8GB of Ram, and 8GB of Storage. The technique was put into use using certain of the Oracle Virtual Box-made virtual machines. In Virtual Box, a virtual computer with two VCPUs 40 GB of RAM been built. The technique led to the definition of a virtual network like a communication channel across VMs. Furthermore, cloud environment is thought to apply the technique owing to AMD A6 APU's limited system resources and virtualization restrictions.

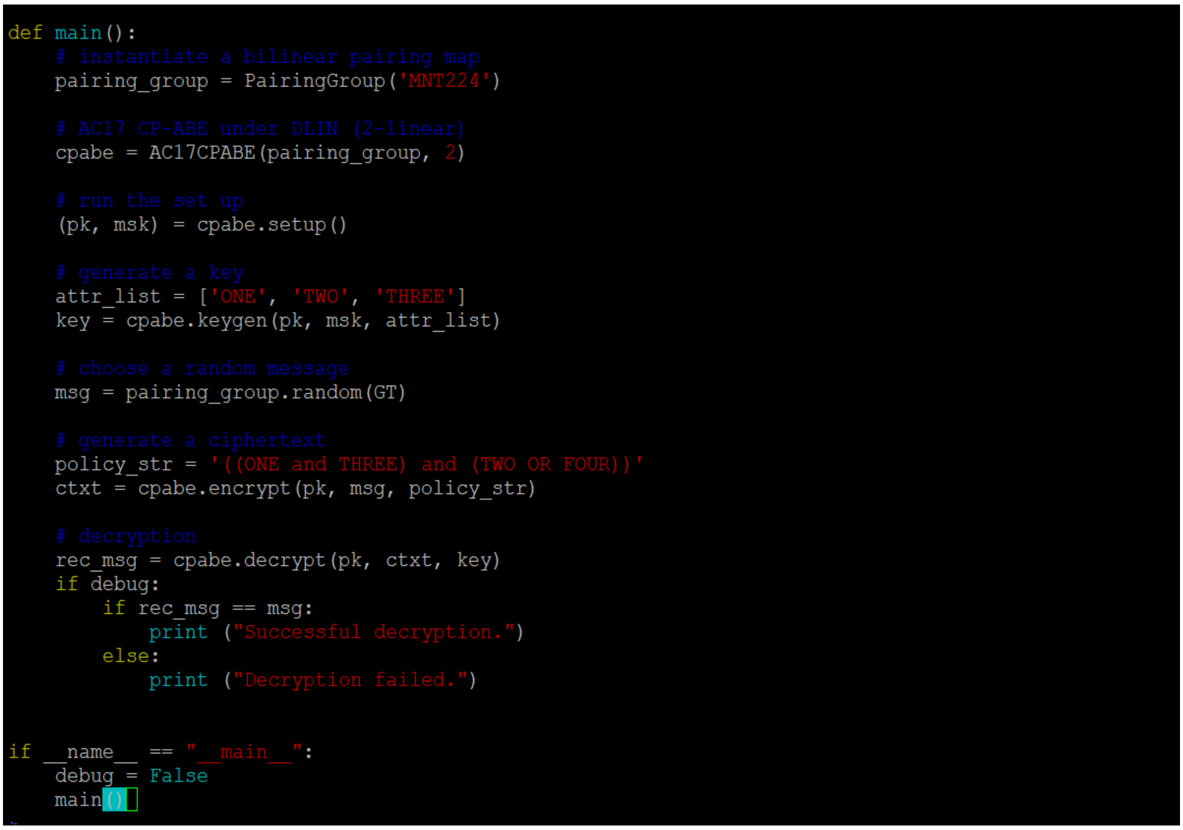
Two distinct implementations of the approach each use it in a variety of different ways. The primary policy modifications were developed based on the packages described in [12], and the attribute-based encryption system was adopted as a result of the work described in [18]. Both of these modifications were based on previous research. Python and C are being used throughout the design process. Utilizing the cloud computing resources made available by Microsoft Azure, the aforementioned method was successfully implemented. A range of purposes, Azure provides regulated and adaptable virtual infrastructures.

5.0.1 Attribute Based Encryption in Cloud Infrastructure

The Following the completion of the construction of the cloud infrastructure, the attribute-based encryption technique is developed. The algorithm functions in four main blocks to establish dependencies, generate private keys and public keys with attributes to every network entity, encrypt information in transit using attributes defined by the administrator, and encrypt using private key attributes made available by the administrator. The Pairing Based Cryptography (PBC) module is used throughout the technique to do the algebraic computations that are required. Because it enables portability as well as rapid execution, the PBC package would be an essential component in the construction of a pairing-based cryptosystem.

In addition, the packages provide functions that may be used for linking calculations, constructing elliptic curves, and performing elliptic curve arithmetic. The tool is helpful in the process of creating characteristics for individual clients. These packages are taken into consideration by the algorithm since it makes position-based access permissions possible. Interactions between virtual instances in the cloud might take place due to the functions that each instance is responsible for. In addition to this, the use of such a technology eliminates the need of a dependable data storage system. In addition, the C programme that was created with the GMO library is capable of running in parallel with the packages.

Python 3 was used in the development of the primary technique, which employs an attribute-based approach to data encryption [18]. In order for the technique to work properly with encrypted root filesystem data, it has to be developed. It has been modified to function properly on cloud deployments of virtual infrastructure. In addition to the construction of the virtual machines, the policies of the users are also specified. The picture that you see above is the dashboard of the VM, which is where the approach was used. The term "virtual instance" refers to a hosted node in a network.

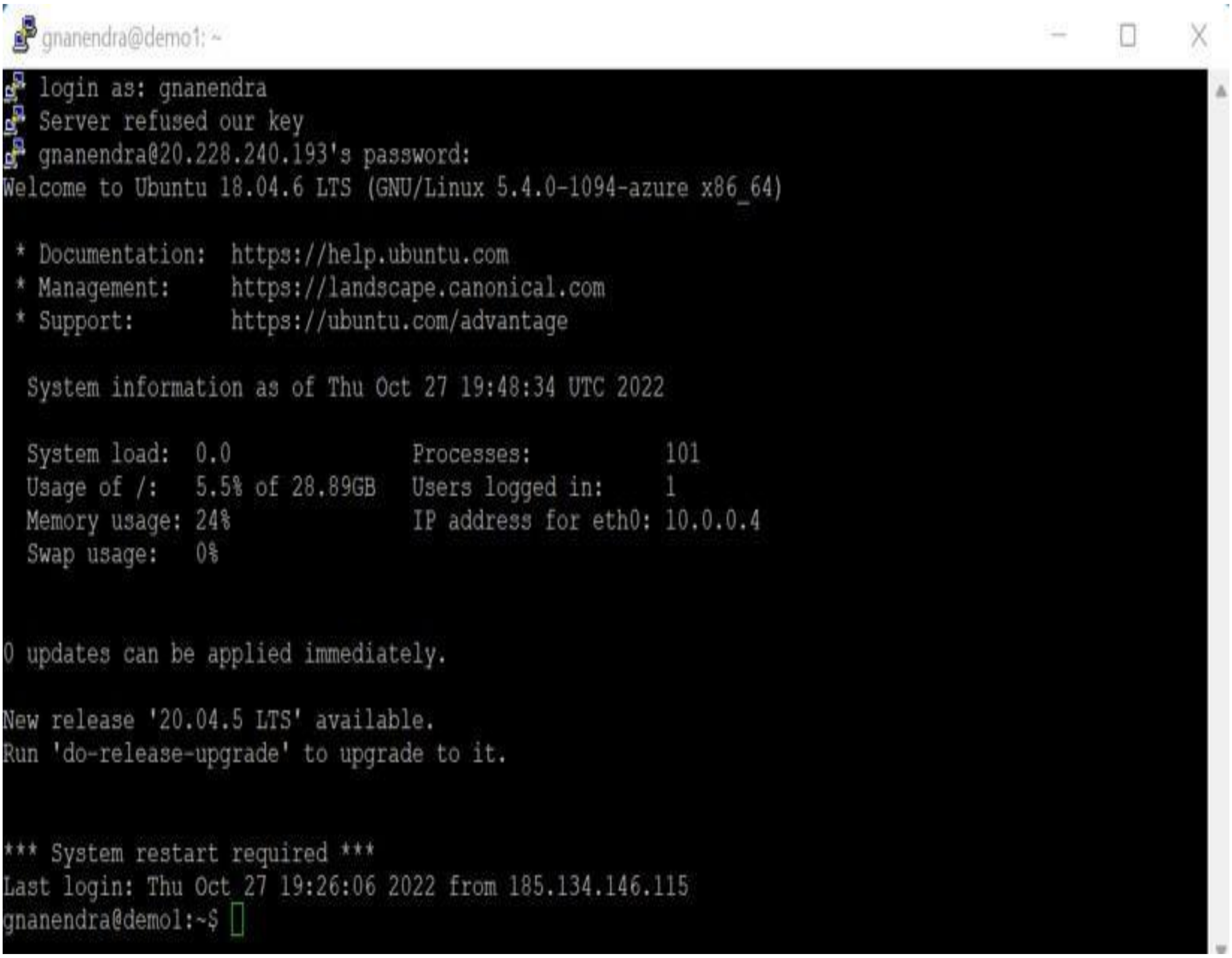


```
def main():
    # instantiate a bilinear pairing map
    pairing_group = PairingGroup('MNT224')

    # AC17 CP-ABE under DLIN (2-linear)
    cpabe = AC17CPABE(pairing_group, 2)

    # run the set up
    (pk, msk) = cpabe.setup()

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

    # choose a random message
    msg = pairing_group.random(GT)

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

    # decryption
    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()
```

Figure 7: The suggested methodology’s attribute-based encryption algorithm for access control

The ABE-Master incorporates the algorithm, in contrast to the other documents on the dashboard, which are dependencies developed for the policy-based access control paradigm. The algorithm is what is utilised to produce a policy for each user's computer that is part of the network. This rule takes into account both the attributes that are provided by the ABE master and the secret key. Using the policy, one is able to access the encrypted data stored on the network.

The algorithm that was constructed by following the methodology that was proposed may be found in the main.py file. After the policies have been set in the relevant files, it will be possible to implement the algorithms by running a build function. The rules for accessing the network are crafted by this algorithm, which also encrypts the data. Users are able to monitor the performance of their virtual instances using the Azure portal.

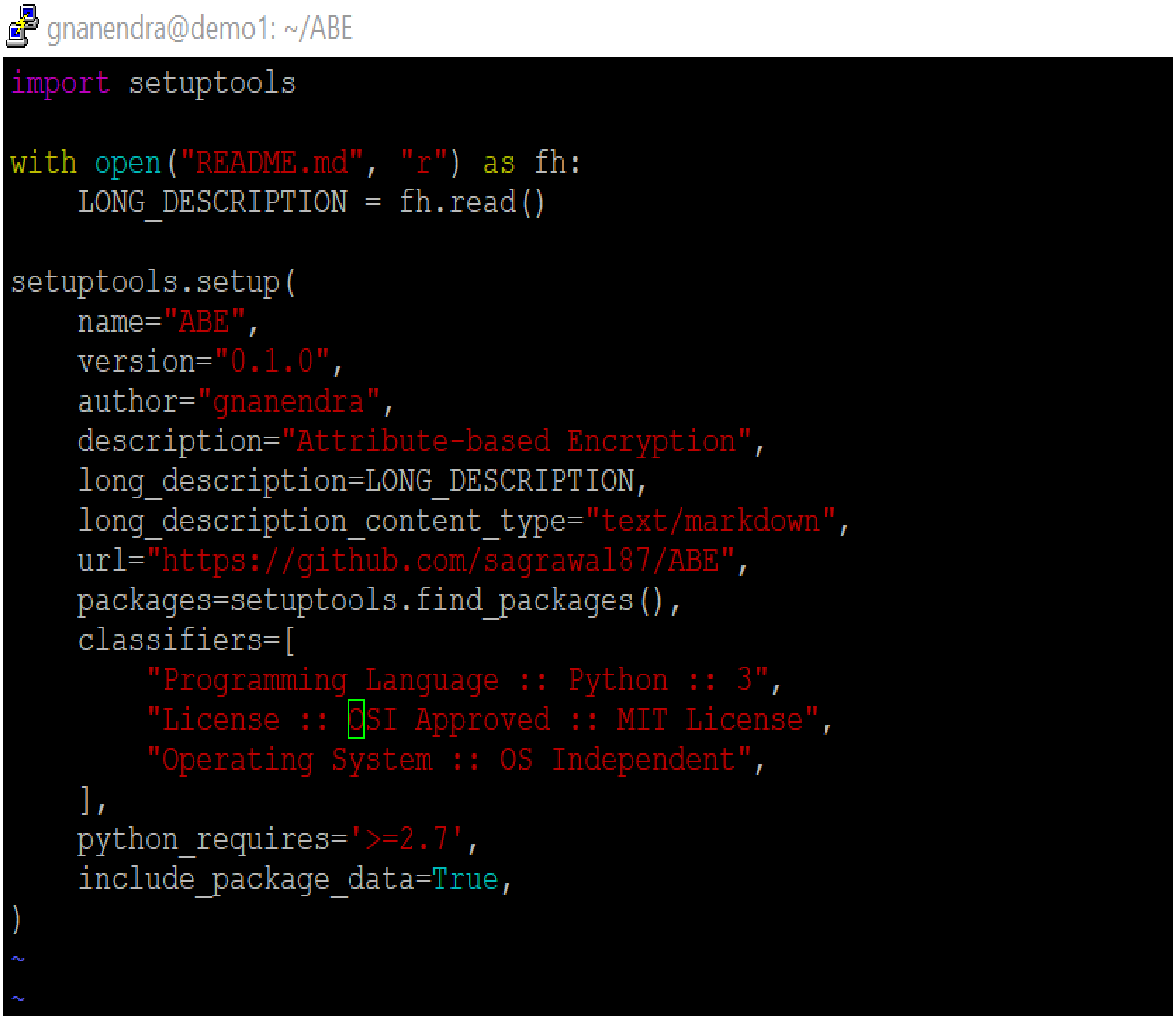


```
login as: gnanendra
Server refused our key
gnanendra@20.228.240.193's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1094-azure x86_64)

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

  System information as of Thu Oct 27 19:48:34 UTC 2022

  System load:  0.0               Processes:           101
  Usage of /:   5.5% of 28.89GB   Users logged in:     1
  Memory usage: 24%               IP address for eth0: 10.0.0.4
  Swap usage:   0%


0 updates can be applied immediately.

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Thu Oct 27 19:26:06 2022 from 185.134.146.115
gnanendra@demo1:~$ 
```

Figure 8: Using PBC and GMP packages, a list of requirements for the ABE algorithm was constructed.

The algorithm must be capable to function for cloud-basedweb-scale platforms. The algorithm must be capable of accommodating the requirementsof the applications since the cloud services are scalable. In order to patching the attributelists broadcast its secret key to an instances, additional VMs in Azure is established asa users on the network. The secondary virtual machine is separated by establishing a directory tenant relation to increase the system’s security.

A tenant of the first vm is how the newly generated Virtual machine is described. Can have full control over the network, the current directory access policy have been set to administrator. Conversely, the administrator for a Directory tenancy may limit the accesses. The VMs, however,is given complete permission in order to limit accessibility that used an algorithm. The initial VM updates a attribute list produced by algorithm, and both the private key and the attributes produced for that Virtual machine were expected to share.



```
gnanendra@demo1: ~/ABE
import setuptools

with open("README.md", "r") as fh:
    LONG_DESCRIPTION = fh.read()

setuptools.setup(
    name="ABE",
    version="0.1.0",
    author="gnanendra",
    description="Attribute-based Encryption",
    long_description=LONG_DESCRIPTION,
    long_description_content_type="text/markdown",
    url="https://github.com/sagrawal87/ABE",
    packages=setuptools.find_packages(),
    classifiers=[
        "Programming Language :: Python :: 3",
        "License :: OSI Approved :: MIT License",
        "Operating System :: OS Independent",
    ],
    python_requires='>=2.7',
    include_package_data=True,
)
~
~
```

Figure 9: setup.py

A putty console shown in Figure is shown. This contains the definition of a attribute-based encryption scheme. Our suggested technique is in line also with algorithm’s step-by-step explanation. Instead of include customers as in bilinear group, virtual instances exist. The specified access control policies are communicated to the VMs as well as the key produced in step 4 in shape of an arbitrary message. The private key (pk), the policy attribute (ctxt), as well as the public key must match with the already-existing attributesto start the decryption process. The entry is refused if the characteristics need not line up.

6 Evaluation

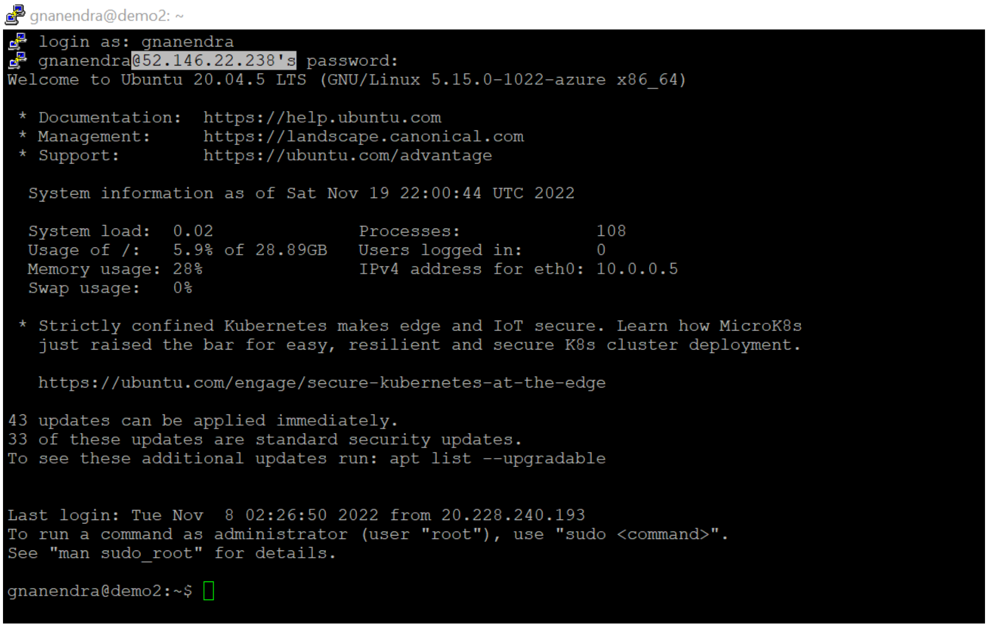
The performance of the implementation was evaluated using the evaluation technique suggested in [14], which was utilised. On the virtualized environment provided by Azure, the experimental method was carried out. This technique was put into action by applying the method that was given. There are a variety of methods available for analysing the comprehensive safety of cloud-based systems. An effort by simulated VMs to flee the cloud environment was not actually feasible since the resources available in the cloud were thought to be resistant to attacks based on the infrastructure. In light of this, the following is how the practical evaluation of a key policy attribute-based encryption tech- nique of network access should be carried out:

6.1 Accessing the network resources externally

An extra virtual machine is used to examine the access granted to the network in orderto guarantee that the implementation is correct. machine is produced by using the same network that the host system uses. Two virtual instances are already functioning in the same way as the architecture on the same networks. There is a deployment of a third Virtual machine, however the execution of the algorithm does not result in the production of the characteristics. Through the use of Azure Active Directory, restricted access priv- ileges have been assigned to the third Virtual machine so that rejection may be increased.

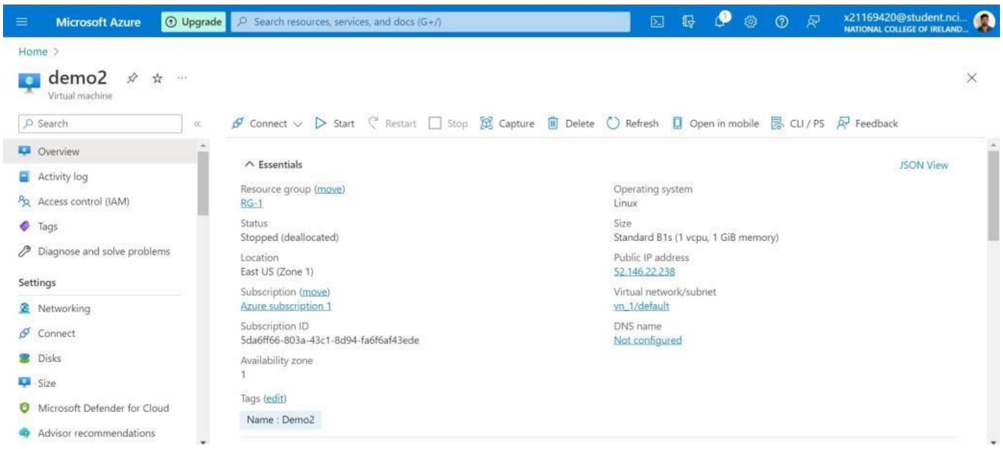
The networking configuration of the third virtual machine has been set up such thatit is isolated from the settings of the other two virtual machines. This is done in order to ensure that the third Virtual machine is completely separate from the first two Virtual machines, functioning similarly to an external escape Virtual machine. An escape Virtual machine is able to work as an external factor because it can break out of its hypervisor and communicate with the resources of the underlying hardware. In this demonstration, the virtual machine cannot communicate with the physical hardware; instead, it may imitate the behaviour of an external computer by accessing network services. The extra Vm is not produced using the attributes that already exist in the networks when the algorithm is executed; rather, it is formed with new properties. Launching an SSH client is done using Putty, which is then used to connect to the instances. Even after supplyingthe necessary credentials, the connection cannot be established with the external VM since none of its attributes have been specified.

The second Vm built in Azure with out any dependency on the current infrastructure. The public ID is accessible from Administrator machine through Serial port. Above Figure shows that as the private key is now not established, VM connection is restricted. On a native implementation, although, network security may be evaluated using a VM escaping strategy. Initially, the host machine's direct memory address is deliberately accessible via VMWare Tools to execute instruction to reach the host's OS. If the hardware is hacked, the memory address may be accessible through an explicit Backdoor() call. Methods such as memcall() also are identified as in list for remote calls to procedures that have the possibility of disrupting the infrastructures.



```
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:~$ 
```

Figure 10: Establishing the connection without attaching the algorithm



Resource group (move)
RG-1

Status
Stopped (deallocated)

Location
East US (Zone 1)

Subscription (move)
Azure subscription 1

Subscription ID
5da6ff66-803a-43c1-8d94-fa6f6af43ede

Availability zone
1

Tags (edit)
Name : Demo2

Operating system
Linux

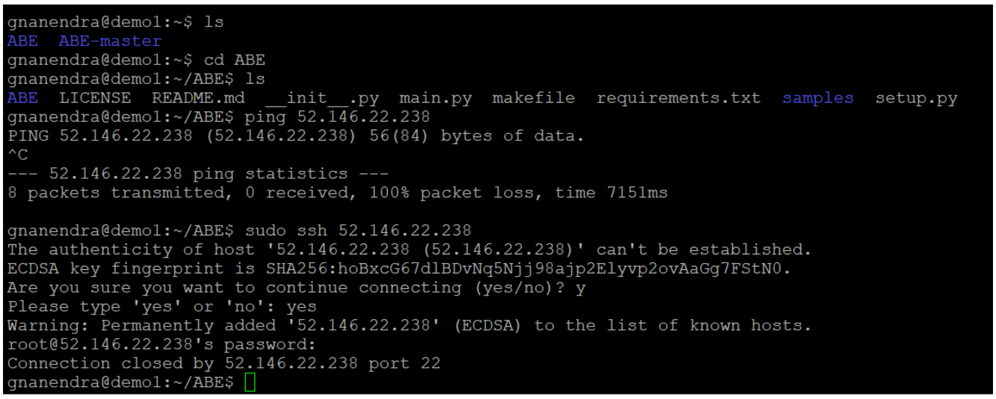
Size
Standard B1s (1 vcpu, 1 GiB memory)

Public IP address
52.146.22.238

Virtual network/subnet
vn_1/default

DNS name
Not configured

Figure 11: External Virtual Instance



```
gnanendra@demo1:~$ ls
ABE  ABE-master
gnanendra@demo1:~$ cd ABE
gnanendra@demo1:~/ABE$ ls
ABE  LICENSE  README.md  __init__.py  main.py  makefile  requirements.txt  samples  setup.py
gnanendra@demo1:~/ABE$ ping 52.146.22.238
PING 52.146.22.238 (52.146.22.238) 56(84) bytes of data.
^C
--- 52.146.22.238 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7151ms

gnanendra@demo1:~/ABE$ sudo ssh 52.146.22.238
The authenticity of host '52.146.22.238 (52.146.22.238)' can't be established.
ECDSA key fingerprint is SHA256:hoBxcG67dlBDvNq5Njj98ajp2Elyvp2ovAaGg7FStN0.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '52.146.22.238' (ECDSA) to the list of known hosts.
root@52.146.22.238's password:
Connection closed by 52.146.22.238 port 22
gnanendra@demo1:~/ABE$ 
```

Figure 12: rejection to provide access to the second Virtual Machine

7 Conclusion and Future Work

Virtualization is seen as a critical element of cloud environments. This cloud computing paradigm enabled different people all over the globe to have access to different cloud computing services. Cloud infrastructure are well recognised for their scalability resilience, but security in corporate clouds has piqued the attention of the academic environment. The research assessed the hazards and vulnerabilities of cloud-based virtual infrastructures. And including network security, many risk detection reduction approaches were examined. The suggested approach has created to increase virtual environment security.

The implementation is evaluated based upon good accessibility control and the data confidentiality. According to studies, these encryption algorithms are optimal for data secrecy and user responsibility. However the approach was effective in preserving user ac- cess, it can only provide fine-grained access control. The encryption algorithm leverages the properties provided when creating the access control rules to connect with private key provided by administrator. This approach can only provide the most basic secur- ity needs in dispersed network. Furthermore, this encryption technique was capable of creating characteristics with access controls and private keys. The access control were cre- ated by the security is the major, in this instance the administrator or the host computer.

The characteristics described are provided with a public key, a secret key, and a randomized integer, making it impossible for multiple users to randomly select their attrib- utes in order to obtain the data access and thereby avoiding network collusion. Attribute encryption may be accomplished in a variety of methods to provide confidentiality at various levels of accessibility. However, user responsibility is difficult to accomplish with such encryption methods. It may be observed that the administrator is in charge of creat- ing access control rules. Customers won’t be produced duplicate keys since the rules are established in the attribute-based encryption paradigm. When new customers are added, the policies really aren’t produced, however the list of characteristics is changed to fit a new user. Upgrading characteristics assigning access policies for users may be time-consuming and inefficient in cloud settings. However, future research might concentrate on better assessment methodologies and increased temporal difficulty of attribute-based encryption algorithms.

References

1. Simmon, E., 2018. Evaluation of cloud computing services based on NIST SP 800-145. NIST Special Publication, 500, p.322.
2. Hwang, K., 2017. Cloud computing for machine learning and cognitive applications. Mit Press.
3. Chia-Te Liao, C.C.C. and Lin, I.C., An Access Control System with Time-constraintUsing Support Vector Machines.
4. Dubey, A. and Pal, S., 2017, January. Dynamic service composition towards database virtual-ization for efficient data management. In 2017 7th International Conference on Cloud Compu-ting, Data Science Engineering-Confluence (pp. 519-526). IEEE.
5. Ahuja, S.P. and Komathukattil, D., 2012. A survey of the state of cloud security. Network and Communication Technologies, 1(2), p.66.
6. Al-Aqrabi, H., Liu, L., Xu, J., Hill, R., Antonopoulos, N. and Zhan, Y., 2012, April. Investigation of IT security and compliance challenges in security-as-a-service for cloud computing. In 2012 IEEE 15th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (pp. 124-129). IEEE.
7. Bowers, K.D., Juels, A. and Oprea, A., 2009, November. HAIL: A high-availability and integri-ty layer for cloud storage. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 187-198).
8. Carroll, M., Kotzé, P. and Van der Merwe, A., 2011. Secure virtualization: benefits, risks and constraints.
9. Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I. and Warfield, A., 2003. Xen and the art of virtualization. ACM SIGOPS operating systems re-view, 37(5), pp.164-177.
10. Korkin, I., 2015. Two challenges of stealthy hypervisors detection: Time cheating and data fluctuations. arXiv preprint arXiv:1506.04131.
11. Boneh, D., Crescenzo, G.D., Ostrovsky, R. and Persiano, G., 2004, May. Public key encryp-tion with keyword search. In International conference on the theory and applications of cryp-tographic techniques (pp. 506-522). Springer, Berlin, Heidelberg.
12. Boyen, X., Mei, Q. and Waters, B., 2005, November. Direct chosen ciphertext security from identity-based techniques. In Proceedings of the 12th ACM conference on Computer and communications security (pp. 320-329).
13. Subramanian, N. and Jeyaraj, A., 2018. Recent security challenges in cloud compu-ting. Computers Electrical Engineering, 71, pp.28-42.
14. Han, Y., Chan, J., Alpcan, T. and Leckie, C., 2014, June. Virtual machine alloca- tion policies against co-resident attacks in cloud computing. In 2014 IEEE InternationalConference on Communications (ICC) (pp. 786-792). IEEE.
15. Jansen, W.A., 2011, January. Cloud hooks: Security and privacy issues in cloud computing. In 2011 44th Hawaii International Conference on System Sciences (pp. 1-10). IEEE.
16. Wan, Z., 2012. June liu, and robert h. deng, senior member, ieee, hasbe: A hierarch-ical at-tribute-based solution for flexible and scalable access control in cloud computing in proc. IEEE Transactions on Information Forensics and security, 7(2).
17. Mon, E.E. and Naing, T.T., 2011, October. The privacy-aware access control system using attribute-and role-based access control in private cloud. In 2011 4th IEEE International Con-ference on Broadband Network and Multimedia Technology (pp.

447-451). IEEE.

18. Hohenberger, S. and Waters, B., 2013, February. Attribute-based encryption with fast de-cryption. In International workshop on public key cryptography (pp. 162-179). Springer, Ber-lin, Heidelberg.

19. Dong, Y. and Lei, Z., 2019. An access control model for preventing virtual machine hopping attack. Future Internet, 11(3), p.82.

20. Lee, C., Federated Access Control in Heterogeneous Intercloud Environment: BasicModels and Architecture Patterns.

21. Goyal, V., Pandey, O., Sahai, A. and Waters, B., 2006, October. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98).