International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

Optimal Framework for Level Based Access Control for VM Auditing on Cloud

S Rekha Garikamukkala[1*], Dr. V.Ravi Sankar[2]
[1]Research Scholar,Computer Science and Engineering,Gitam(Deemed to be University),Hyderabad,India
Sr.Assistant Professor,CVR College of Engineering,Ibrahimpatnam, Hyderabad
sunitha.garikamukkala@gmail.com
[2]Associate Professor,Computer Science and Engineering,Gitam(Deemed to be University), Hyderabad,India
ravisankar.vadali@gitam.edu

Abstract— The growth in the cloud computing have motivated and enable lot of application developer to deploy the applications on cloud. The major challenge of hosting on cloud is the service provider or the application provider must comply to a good number of rules. These compliance reports are time to time validated and checked by external auditors. The auditing process for the cloud services are critical and the access controls must be enabled. Due to the higher complexity and less flexibility of the virtual machines, most of the cases this access control mechanism is compromised. This work proposes four algorithms to identify and enhance the LBAC mechanism for cloud services with access updates based on time variant characteristics analysis and predictive analysis with selective cryptographic methods. The proposed model produces significantly improved results to overcome three major issues in the cloud service management as selective LBAC, static privileges and open access control for the auditors.

Keywords: Dynamic Time Variant; Access Control; Predictive Identification; Selective Encryption; Selective Decryption; Access Allocation.

I. INTRODUCTION

Multi-tenancy, according to Z. Birnbaum et al. [1], is one of the most appealing properties of cloud computing because it enables elastic, efficient, and on-demand resource provisioning and allocation for both customers and service providers. This design, on the other hand, has new consequences for security. As a result of side-channel and escape-to-hypervisor attacks, VMs operating on the same physical computer might be compromised. Many false alarms occur while utilising signature-based intrusion detection technologies or system call anomaly analysis to avoid intrusive activity and malicious programmes. These researchers provide a paradigm for behavioural auditing of client VMs and the detection of potentially malicious processes at the highest semantic level. Our early findings have confirmed the new approach's efficacy and efficiency.

Conserving energy results in generating power. The relevance of energy in our daily lives cannot be overstated. The demand for energy is at an all-time high. Either increasing energy production or reducing energy use will suffice to meet the rising demand. It is critical to save energy since generating energy is a costly endeavour. In order to find ways to save energy, an electrical energy audit examines the patterns of power usage. Automation is required since energy audits are time consuming and labour expensive. With the goal of incorporating automation into the energy audit and the adoption of distributed energy production, the OEAERMS was created as shown by A. Ganapathy et al. [2], OEAREMS contributes to a better knowledge of how electrical energy is used and to raising awareness about energy conservation.

Using a shared pool of customisable computer resources, Cloud computing enables users to save their data remotely in the cloud, according to S. Shetty et al. [3]. The cloud computing system and network's security is critical to the security of data that is outsourced to the cloud. The assessment of data security on the network between the cloud provider and its customers is still a difficult problem, despite various attempts to secure data on the cloud computing system. Insights from the cloud computing system and network audit will be provided on the security and performance of virtual machines (VMs) and the operating system across multiple data centres, as well as the intra-cloud network managed by cloud providers and the wide-area network between cloud users and cloud providers (WLAN). This is why network traffic analysis for cloud auditing is essential so that consumers may turn to a third-party auditing firm to check the cloud service provider's data security. Cloud computing network traffic analysis requires the following major technologies: IP geolocation of network devices between cloud providers and their customers, monitoring of data security on the cloud network route, and online mining of enormous audit records created by cloud network traffic.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

Henceforth, after setting the context of the research, in the next two sections, the fundamentals of LBAC and VM auditing processes are analyzed.

II. FOUNDATIONAL METHOD FOR LEVEL BASED ACCESS CONTROL

After setting the context in the previous section of this work, this section is dedicated to understand the fundamentals of level-based access control mechanism.

Assuming that, the complete user base is identified as UB[], where each user is identified as U_X. These users are primarily the access requesters. This can be represented for n number of users in the collection as,

$$UB[] =< U_1, U_2, U_3, ...U_n > \quad (1)$$

Further, each user has specific characteristics set as CH_X[], where each characteristics can be identified as C_X. This can be formulated form number of characteristics as,

$$U_X \rightarrow CH_X[] =< C_1, C_2, C_3, ...C_m > \quad (2)$$

The combined characteristics can produce the user access privilege, UAP as,

$$UAP_X = f\{CH_X[]\} \quad (3)$$

Where, f is the function to calculate the access permissions requested based on the set of allocated and allowed resources with request permissions.

In the other hand, the set of available resources or services can be denoted as SB[], where each service can be identified as S_X. Thus, for k number of total services, this can be formulated as,

$$SB[] =< S_1, S_2, S_3, ...S_k > \quad (4)$$

Again, each service is collection of few fundamental characteristics as Service Origin as SO, Service Profile as SP and most importantly Service Authentication as SA. The SA defines the permissive access privileges to that specific service. This can be represented as,

$$S_X =< SO, SP, SA > \quad (5)$$

Finally based on the user access privilege, UAP and the service authentication, SA, the level-based access control mechanism will be performed. The detailed logic of this process is to identify the UAP and match the SA to extract the services for the user with access levels. This can be formulated as,

$$\{S'[], AL\} = \prod_{UAP_X :: SA_X} SB[] \quad (6)$$

Here S' denotes the selected services for access and AL denotes the permitted access levels.

After this foundational knowledge, the recent research outcomes will be analyzed further in the light of this basic knowledge.

III.FOUNDATION METHOD FOR VM AUDITING

The service auditing process closely relies on the virtual machines. The virtual machines are at the core of this process. Once the level-based access controls are defined, the auditor assignments towards the virtual machines should be performed in order to assign the virtual machines to the auditors for auditing process. The foundational process for VM auditing is furnished here.

With the prior knowledge of Equation 2, it is clear that, multiple users or auditors have their set of characteristics. Each characteristics are further utilized and a collection of mean characteristics, MA[], are formulated as,

$$MA_X[] = Mean\{\bigcup_i CH_X[i]\} \quad (7)$$

The similar process for the virtual machines must also be performed. Now, the virtual machines information is extracted from the service information. The service information can be obtained from the Equation 5 as stated in the previous section of this work. Thus, the virtual machine collection, VM_X[], associated with any service can be formulated as,

$$S_X =< SO, SP, SA > \rightarrow VM_X[] \quad (8)$$

Further, the virtual machine collection is comprised of multiple characteristics such as computational capacity, C, memory capacity, M, storage capacity, S and network bandwidth, N. This can be formulated as,

$$VM_X[] = \sum_{j=i}^{p} < C_X, M_X, S_X, N_X > [j] \quad (9)$$

For a j number of virtual machines in the collections.

Finally, the auditor characteristics must be utilized for assigning the virtual machines to the auditors. As,

$$U_X :: VM_Y[] = \prod_{MA_X[]} \sum_{j=i}^{p} < C_X, M_X, S_X, N_X > [j] \quad (10)$$

Thus, $VM_Y[]$ is the set of virtual machines which are assigned to U_X auditor.

Henceforth, in the light of the understanding of level-based access control and virtual machine auditing process, in the next section of this work, the recent research outcomes are analyzed.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

IV.PARALLEL RESEARCH OUTCOMES

The understanding obtained from the previous few sections of this work, ensures the deeper understanding of the recent parallel research outcomes, which are critically analyzed in this section of this work.

In this study, R. Houlihan et al. [4] propose a unique approach to auditing untrusted cloud. Contracts between cloud service providers (CSPs) and their customers specify in quantifiable terms what resources the CSPs will deliver to the customers. They have an incentive to cheat on the SLA since they are profit-oriented. The CSP may serve more users on the same hardware and make more money by giving them less resources than what is stated in the SLA. It is easy for the cloud service provider (CSP) to feign compliance with the SLA since the monitoring and verification of the SLA is often conducted on the cloud system itself. Introduce a methodology that makes use of a third-party auditor to avoid such cheating in parallel researcher results (TPA). Parallel researchers are solely interested in the results of CPU cheating in this study. Cheating by a CSP may be detected by using a popular CPU-intensive computation, transpose matrix multiplication (TMM), which can be exploited by parallel researchers. Researchers have shown that our system is capable of detecting CPU cheating even in modest amounts using real-world trials.

Security auditing enables cloud tenants to check that the cloud architecture is in accordance with desired security features, such as whether a tenant's virtual network is adequately isolated from other tenants. A cloud provider may be hesitant to provide highly sensitive information, such as the underlying cloud infrastructure's full topology, to a third-party auditor while doing an audit. It's possible that auditing findings intended for one tenant may accidentally divulge private information about other tenants; for example, a misconfiguration might make another tenant's VM accessible. It's a fresh problem that hasn't garnered a lot of attention. Many of the available anonymization solutions would either not safeguard the data adequately or make it impossible to audit. This article proposes SegGuard.

The dynamic nature of the virtual infrastructure in a cloud computing environment is one of its distinguishing features. Current Virtual Machines (VMs) move to a new host or network segment, while new VMs are created and existing VMs are destroyed. Because of cloud-specific features like rapid infrastructure changes, traditional incidence tracking systems aren't up to the task. An audit system for the cloud is being developed by F. Doelitzscher et al. [6] that intends to promote confidence in cloud infrastructures by bringing greater transparency to both the user and the cloud provider on what is going on. Demonstration illustrates how autonomous agents detect changes in infrastructure, automatically reassess the cloud's security state, and tell the user via an audit report in the case of a change.

Malicious chargeback software and privacy disclosure are the most common concerns to the security of smartphones. These attacks leverage the flaws in the prior authorization scheme, and they may even ask for hardware to snoop on privacy in the background. The current Android operating system does not allow users to monitor and audit system resources, hence a dynamic supervisory mechanism of process behaviour based on Dalvik VM is offered as a solution. Modifications and extensions are made to the Android system framework and application layers, and system-specific underlying services are leveraged to provide a dynamic oversight of Dalvik VM's process behaviour. This technique allows for real-time monitoring and analysis of every process using system resources as well as the behaviour of any programme in use. It lowers the degree of security risks at the system level and identifies the processes that are using system resources at that level of security. It safeguards private information, critical data, and sensitive system activity by detecting and intercepting it before it occurs or takes place. According to D. Zhu et al. [7], our technique has been shown to be accurate, effective, and resilient.

Utilizing cloud computing log digital investigations, “forensic evidence from a virtual machine (VM) host operating system may be used to investigate a suspected crime, using the hypervisor event logs. A possible Web Services-centric approach may be required for such log-supported investigations, but due to the heterogeneous complexity of an enterprise's private cloud, let alone the distributed public cloud, forensic reconstruction of evidence on VM hosts systems is required in cloud digital log forensics. An SOA audit framework for this sort of forensic investigation must be able to recreate transactions that span different VM hosts, platforms, and applications.” Cloud log forensics SOA framework needs for successful digital investigation exams are examined in this research. S. Thorpe et al. [7] demonstrate how cloud-based log-centric SOAs may benefit from investigative and forensic auditing tools and procedures that will need this architecture.

It has become an on-demand utility since cloud computing has commodified computer, storage, and networking resources. A lack of transparency in cloud platforms has influence on cloud application performance by J. Schiffman et al. [9]. Thus, the CV provides a low-cost mechanism for cloud clients to ensure that their instances are operating as expected.

It is an online optimization approach that analyses the success of an optimization on a specific code area. If implemented correctly, it has the ability to dramatically enhance performance and eliminate performance decrease owing to compiler optimizations. It is impossible to draw statistically

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

meaningful conclusions about performance without a large enough number of timings for a given piece of code. This study improves the overall efficacy of a performance auditing system by enabling for a finer granularity of timings to be obtained than previously possible in existing systems. There are many applications outside performance audits for our method, which solves the basic issue of associating program's high-level behaviour with its binary instructions. A Java VM implementation and assessment by J. Lau et al. [10] is presented in this paper.

Today, cloud computing is a major force in meeting all of a company's on-demand IT demands. As contrasted with any of its early competitors, the cloud offers substantial mechanisms for adequate resource sharing, maximum resource use, and genuine elasticity. As a result of these security issues, many firms are hesitant to use this next-generation computing. Customers and their data are the lifeblood of today's corporate computers, which extends identity management capabilities to the Cloud VM level, is examined in detail by M. K. Srinivasan et al. [11].

Recently, the issue of protecting VMs against a hacked or even malevolent hypervisor has been a major focus of attention. Due to the fact that suspend/resume and migrate procedures offered by an IaaS platform are sometimes difficult to tell apart, most prior systems were open for rollback attack. Some of the earlier systems simply disabled these functions to protect against rollback attacks, while others need a lot of user input in order to protect themselves. For the first time, an approach that strikes an appropriate balance between security and usability has been proposed by Yubin Xianet al. [12].

As the IT industry grows and changes on a dime, cloud computing is becoming more and more prevalent. When compared to any of its early rivals, cloud computing provides a whole new computing paradigm that allows for the most efficient use of resources. 'Pay-as-you-use' business model appeals to corporations in addition to its technological merits. Many firms are reluctant to use this new computer technology because of its high level of security concerns. Customers and their data are the lifeblood of today's corporate computers. There is a significant number of security issues because of the public and multi-tenant nature of the cloud which is designed and implemented by M. K. Srinivasan et al [13] using user-centric identity management.

Data races, deadlocks, non-deterministic failures, and complicated performance difficulties continue to plague multi-core programming. EXCITE-VM, described by H. Litz et al. [14], “is a system that enables snapshot isolation transactions on shared memory to help programmers and boost the performance of concurrent applications. If an application thread doesn't explicitly create a new snapshot, it won't see the committed modifications of other threads until it does so. By separating each thread from the transitory, uncommitted writes of other threads, snapshot isolation allows low overhead lockless read operations and enhances fault tolerance”.

Customers are unable to see the underlying physical infrastructure of today's cloud infrastructures because of their opaque service offerings. Cloud-based essential business applications with data location limits may have difficulty satisfying compliance requirements. Data owners should be able to keep tabs on the whereabouts of their data when it is spread across many nations through federated cloud infrastructures. For data location monitoring, P. Massonet et al [15] demonstrate how an already existing federated Cloud monitoring architecture may be leveraged without sacrificing Cloud isolation. Cloud infrastructure provider (IP) monitors VMs on behalf of customer, service provider (SP), and provides infrastructure level monitoring information to the SP. In the suggested method, coordination is necessary between these two parties. The SP may build the audit logs necessary for compliance auditing using the monitoring information. An e-Government case study with legal data placement limits validates the suggested logging architecture.

S. Barjatiya et al. [16] discuss Blue Shield's concept and execution in this paper. Multi-tenant cloud workloads may be hardened by using Blue Shield. In a cloud environment, the Blue Shield design dramatically reduces the dangers encountered by the tenants. Blue Shield's EIS has been tested in a proof-of-concept environment. When it comes to dealing with security concerns, there are many ways that are currently being used. When moving to a Blue Shield-based cloud, the existing security apps installed in a non-cloud environment don't need any changes. With the proposed architecture in place, virtual machines in the same VLAN are protected from one other.

Virtual machines (VMs) and containers (containers that share the operating system kernel) have been used to isolate cloud tenants since their inception. The isolation and security of data maintained by specific apps is becoming more important as the number of these applications grows. A single platform is needed when the government, which consists of several departments and agencies, delivers services to its people and must be able to share data with other apps in a way that goes beyond the usual cloud-isolation limits. Data management is at the heart of these challenges. There is no control over where data travels after it leaves the custody of its owner once cloud-hosted apps and cloud-services apply traditional access control, which is application and principal/role specific and implemented at policy enforcement points. System-wide flow control is provided by Information Flow Control (IFC), which is based on data's attributes. When it comes to enforcing owners' data flow policies and defending against malicious or malfunctioning

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

software, cloud-deployed IFC has a lot of promise. As a result, IFC's audit log is transparent and gives system-wide visibility of data flows. In addition, this helps individuals in charge of data management accomplish their responsibilities by giving proof of compliance and aiding in the detection of policy flaws and misconfigurations. We provide our IFC concept, IFC architecture, and IFC implementation in a paper by T. F. J. M. Pasquier et al. [17]. This includes an OS-level implementation of IFC, as well as an IFC-enabled middleware.

Cloud computing is a cutting-edge technology that effectively offers users with infrastructure and a platform. Cloud computing also allows for a more thorough examination of security-related concerns and difficulties. Securing cloud computing has been investigated in terms of its many features and aspects such as third-party control, third-party integrity, and third-party audit and compliance. Securing data at both the user and cloud level is part of the Secured Cloud Model. An authentication module for users is supplied, and a cloud-based security mechanism is in place to protect data from cyberattacks. Using a single sign-on system makes it easy to log into the cloud without having to juggle many sets of credentials. According to A. Ochani et al. [18], homomorphic encryption is used to encrypt data stored in the cloud.

When a CDN service (i.e., a Content Distribution Network) is implemented in the cloud, QoS audits may detect QoS violations that occur as a result of resource exhaustion and outages. For an application that relies on the CDN's internal mechanisms to provide a certain level of service, it's important to know how effectively those mechanisms have been developed to meet those requirements (i.e., low latency and overhead). This 'gold standard' is used to compare the actual behaviour of S with that predicted by computer models of S. S's QoS meta-data and CDN adaption mechanisms are externalised using declarative specifications in order to allow a management module H to reason about QoS breaches. H's QoS provisioning for S, K. Ravindran et al. [19] explain the software and system engineering difficulties that occur.

Further, based on the crucial review of the parallel research outcomes, in the next section of this work, the identified research problems are furnished.

V. PROBLEM FORMULATION

After the detailed discussion of the recent and parallel research outcomes in the previous section of this work, in this section, the recent research bottlenecks are listed.

Firstly, the current research outcomes demonstrates that the access to the services are highly static. In the light of the Equation 6, assuming that the user U_X, have requested for the service S_Y, at the time instance t1.

Thus, the available services, $S'[]$, can be identified as following.

$$\{S'[], AL\} = \prod_{UAP_X ::SA_X} SB[] \tag{11}$$

Further, if the request from the same user changes at time instance t2, then the same $S'[]$ services are reassigned as the Equation 11 does not consider the changes of service request. The solution to this problem is elaborated in the next section of this work.

Secondly, the assigned privileges to the services are also highly static. Similar to the previous case, continuing from Equation 6, the access levels, AL , is also static and not taking into consideration the change in request levels.

$$\{S'[], AL\}(t1) \neq \{S'[], AL\}(t2) \tag{12}$$

Finally, during the assignment of the virtual machines to the auditors, the complete virtual machines are assigned to the auditor. This is a higher risk factor and must be mitigated.

Further, the proposed solutions to these persistent research problems are furnished in the next section of this work.

VI.PROPOSED SOLUTIONS – MATHEMATICAL MODEL

After the detailed analysis of the parallel recent research outcomes and the identification of the persistent research problems in the previous section of the work, in this section, the proposed solutions are furnished using the mathematical models.

Firstly, the problem of static access levels is solved using a two-phase solution. The first phase of the solution calculates the moving average or mean of the access level requests and based on the change in the request, the access permissions are granted.

Continuing from the Equation 3, the access level requests from the users or the auditors are formalized. Assuming that, the first request from the auditor, A_X, is made at the time instance t1. Thus, the access level, $UAP_X(t1)$, can be formulated as,

$$UAP_X(t1) = f\{\bigcup_i CH_X[i](t1)\} \tag{13}$$

Again, assuming that the same user made the second access request at the time t2. Thus, the new access level must be calculated as,

$$UAP_X(t2) = f\{\bigcup_i CH_X[i](t2)\} \tag{14}$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

At this point in time, the difference in the access levels must be realized as $\lambda_X(t1,t2)$,

$$\lambda_X(t1,t2) = UAP_X(t1) \rightarrow UAP_X(t2) \qquad (15)$$

Further, the mean of the access – level, $M\lambda_X(t1,t2)$, requests are to be calculated to incorporate the change requirements as,

$$M\lambda_X(t1,t2) = \sum_{k=1}^{(t2-t1)} \lambda_X(t1,t2)\{k\} \Big/ k \qquad (16)$$

Again, the selected services with appropriate access levels are to be assigned to the auditor as,

$$\{S'[], AL\} = \prod_{M\lambda_X(t1,t2)::SA_X} SB[] \qquad (17)$$

The second phase of the solution deploy a regression model to predict the upcoming requested access levels and ensure the same towards the users for the services.

Continuing from Equation 2 and Equation 3,

$$\Re\{UAP_X(t+1)\} = \beta_0 + \beta_1.C_1(t) + \beta_1.C_2(t) + \beta_1.C_3(t)..... + \beta_1.C_m(t) \qquad (18)$$

Further, the selected access levels can be pre-granted as,

$$\{S'[], AL\} = \prod_{M\lambda_X(t1,t2)\bigcap\Re\{UAP_X(t+1)\}::SA_X} SB[] \qquad (19)$$

The second and the third identified problem is proposed to be solved using a deep encryption method. In this encryption method, the virtual machines are proposed to be locked using a dual key setup where the first key will be deployed to lock the header of the virtual machine and the second key will be deployed to lock the complete virtual machine. The first key is to be assigned to the auditors for only accessing the header of the virtual machines and the second key will be assigned to the owner of the virtual machines to gain complete access. The details are furnished here.

Assuming that, any virtual machine, VM_X, is separated into two parts as VMH_X and VMD_X, with the header and the complete virtual machine components respectively. This work proposes to encrypt the virtual machines with RSA algorithm and generate two pair of keys as,

$$\{e,n\} \leftarrow RSA\{VMH_X{}^e (\text{mod } n)\} \qquad (20)$$

And,

$$\{e,m\} \leftarrow RSA\{VMD_X{}^e (\text{mod } m)\} \qquad (21)$$

Here, the key pairs as $\{e,n\}$ and $\{e,m\}$ are to be assigned to the auditors and the data owners.

Henceforth, based on the proposed mathematical models, in the next section of this work, the proposed algorithms are furnished.

VII. PROPOSED ALGORITHMS

After the detailed analysis of the proposed solutions of the existing research problems, in this section of the work, the proposed algorithms based on the mathematical models are furnished here.

Firstly, the proposed Dynamic Time Variant Access Level Identification (DTV-ALI) Algorithm is furnished.

Algorithm - I: Dynamic Time Variant Access Level Identification (**DTV-ALI**) Algorithm
Inputs: • Set of Auditors / Users as A[] • Set of Services S[] ***Output:*** • Access granted services as S1[]
Process: Step - 1. Load the live auditor set as A[] Step - 2. For each auditor as A[i] and time instance t a. Extract the characteristics set as C[](t) for A[i] using Equation 2 b. Calculate the access level as UAP(t)[i] using Equation 14 c. Identify the different of the requested access level as Del_UAP(t,t-1)[i] using Equation 15 d. Calculate the mean change as MDel_UAP[i] using Equation 16 Step - 3. Load the set of services as S[] Step - 4. For each service in the set as S[j] a. Extract the characteristics set as SCX[] using Equation 5 b. Grant the access to the identified services as S1[] for all auditors using Equation 17 Step - 5. Return S1[]
Outcome: • The proposed algorithm ensures to change the access level based on time. • The timely access is granted to the auditors

Secondly, the proposed Predictive Access Level Identification (PA-LI) Algorithm is furnished.

Algorithm - II: Predictive Access Level Identification (**PA-LI**) Algorithm
Inputs: • Set of access levels as UAP(t)[]

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

• Access granted services as S1[] ***Output:*** • Predicted access granted services as S2[]
Process: Step - 1. Load the access level information as UAP(t)[] Step - 2. For each access levels as UAP(t)[k] a. Calculate the predicted access levels as R.UAP(t+1)[] Step - 3. For each service in the set as S[l] a. Grant the new selected services as S2[] using Equation 18 Step - 4. Return S2[]
Outcome: • The increase in time complexity due to the DTV-ALI algorithm is reduced with this predictive algorithm

Thirdly, the proposed Selective Encryption and Access Allocation (SE-AA) Algorithm is furnished.

Algorithm - III: Selective Encryption and Access Allocation (**SE-AA**) Algorithm
Inputs: • Virtual Machines as VM[] ***Output:*** • Encrypted Virtual Machine Headers as VMH[] • Encrypted Virtual Machines as VMD[]
Process: Step - 1. Load the set of virtual machine as VM[] Step - 2. For each element in VM[] as VM[p] a. Generate the key pairs as (e,n) and (e,m) b. VMH[] = RSA-Encryption{VM[],(e,n)} c. VMD[] = RSA-Encryption{VM[],(e,m)} Step - 3. Return {VMH[], (e,n)} and {VMD[], (e,m)}
Outcome: • The parts of the virtual machines are encrypted, hence the access is restricted for the auditors

Finally, the proposed Selective Decryption and Access Allocation (SD-AA) Algorithm is furnished.

Algorithm - IV: Selective Decryption and Access Allocation (**SD-AA**) Algorithm
Inputs: • Encrypted Virtual Machine Headers as VMH[] • Encrypted Virtual Machines as VMD[] ***Output:*** • Virtual Machines as VM[]
Process: Step - 1. Load the virtual machine parts as VMH[] and VMD[] Step - 2. For each element in VMH[] and VMD[] as VMH[p], VMD[p] Step - 3. Load the key pairs as (e,n) and (e,m) Step - 4. VMH[] = RSA-Decryption{VMH[],(e,n)} Step - 5. VMD[] = RSA-Decryption{VMD[],(e,m)} Step - 6. Return VM[]
Outcome: • The decrypted merged virtual machine is restored for hosting the services

Further, based on the proposed algorithms, in the next section of this work, the obtained results are analyzed.

VIII. RESULTS AND DISCUSSIONS

After the detailed discussions on problem identification, proposed solutions in terms of mathematical models and algorithms, in this section of the work, the obtained results are furnished and discussed.

The obtained results are highly satisfactory and are furnished with discussion.

Firstly, the testing setup is discussed with dataset information. The dataset used in this simulation is the widely accepted PlanetLab dataset [20] and the details are furnished here [Table – 1].

Table 1. Initial dataset setup

Parameters	***Values***
Number of Services	200
Number of Total VMs	500
Average Number of VMs	2
Number of Total Auditors	130
Total Simulation Duration (Hours)	150
Average access duration / Auditor (Mins)	17

Here it is to be observed that, the dataset is highly populated and number of services are on the higher side. Thus, this dataset is perfect for such analysis. The characteristics are analyzed graphically here [Fig – 1].

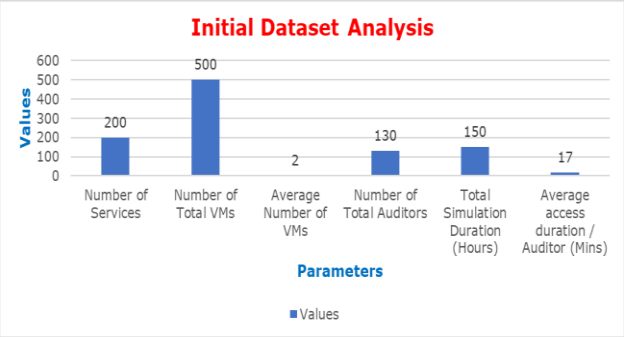

Figure 1. Initial dataset analysis

Secondly, the service descriptions are furnished with virtual machine mapping [Table – 2]. As stated in the previous table, the total number of virtual machines are 500. However, only 10 are randomly listed here further.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

Table 2. Sample service descriptions

ServiceID	*Number of VMs*	*Read Frequency*	*Update Frequency*	*Life Time (ms)*
SA-109	4	19	15	65.48
SA-122	5	15	15	81.98
SA-136	1	21	16	68.36
SA-200	1	22	10	86.08
SA-101	5	18	10	71.09
SA-103	4	14	18	91.71
SA-127	4	25	11	98.65
SA-155	5	23	16	88.95
SA-163	2	22	21	97.54
SA-141	2	21	25	67.77

The distribution of the virtual machines with the read and update frequency for each service are highly random as per the dataset. Thus, the further analysis is highly critical and the applicability of the proposed model will be tested to its best extend. The outcomes are also visualized graphically here [Fig – 2].

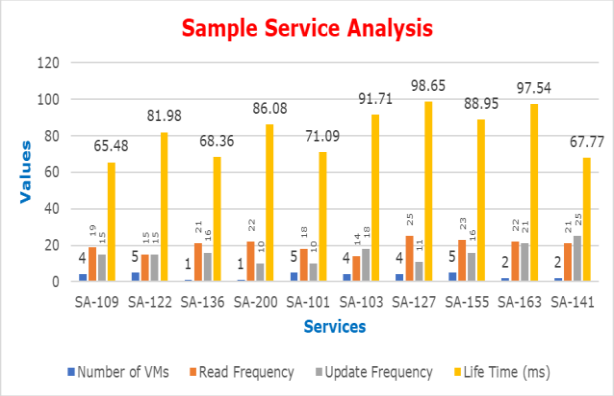

Figure 2. Sample service analysis

Thirdly, information of virtual machines is analyzed [Table – 3]. Here the sample of 10 virtual machines are again analyzed.

Table 3. Sample virtual machine analysis

ServiceID	*VM_ID*	*Read Frequency*	*Update Frequency*	*VM_Size (TB)*
SA-109	VM-225	19	15	3
SA-122	VM-226	15	15	5
SA-136	VM-380	21	16	4
SA-200	VM-164	22	10	5
SA-101	VM-155	18	10	4
SA-103	VM-329	14	18	3
SA-127	VM-231	25	11	5
SA-155	VM-147	23	16	5
SA-163	VM-292	22	21	5
SA-141	VM-298	21	25	6

It is natural to realize that, the virtual machine read and update frequencies are always in line with the total service level frequencies. The obtained analysis is further visualized graphically here [Fig – 3]. Also, the higher size of the virtual machines makes it critical for cryptographic operations, which are demonstrated at the later stage of this work.

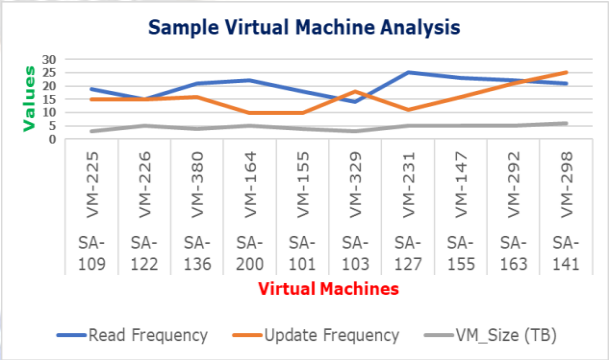

Figure 3. Sample virtual machine analysis

Fourthly, the auditor characteristics are analyzed. For this again a smaller sample is taken with 10 auditor characteristics [Table – 4].

Table 4. Sample auditor characterisitcs analysis

Auditor_ID	*VM Requested*	*Read Frequency*	*Update Frequency*
2080	VM-225	16	14
4028	VM-226	12	13
2463	VM-380	18	13
3676	VM-164	21	18
2920	VM-155	15	8
2804	VM-329	18	16
2408	VM-231	22	10
2091	VM-147	21	15
4555	VM-292	21	28
4799	VM-298	19	22

The results are also visualized graphically here [Fig – 4].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

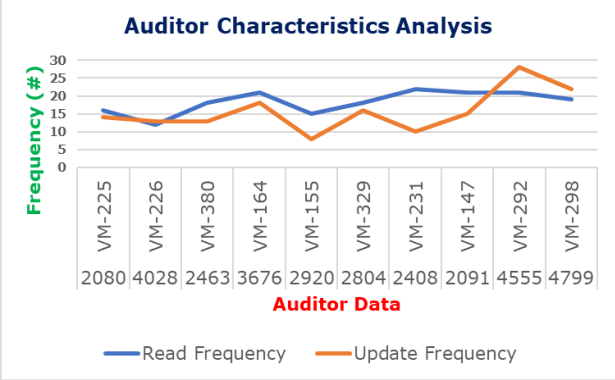

Figure 4. Auditor characterisitcs analysis

After the phase, based on the auditor read and update frequencies, the requested virtual machines are assigned.

Fifthly, the level-based access control results are discussed.

Table 5. Access control results

Auditor_ID	*VM Requested*	*Read Frequency*	*Update Frequency*	*VM_ID Assigned*	*Read Frequency*	*Update Frequency*	*Access Level – Read*	*Access Level - Update*
2080	VM-225	16	14	VM-225	19	15	Granted	Not Granted
4028	VM-226	12	13	VM-226	15	15	Granted	Not Granted
2463	VM-380	18	13	VM-380	21	16	Granted	Not Granted
3676	VM-164	21	18	VM-164	22	10	Granted	Not Granted
2920	VM-155	15	8	VM-155	18	10	Granted	Not Granted
2804	VM-329	18	16	VM-329	14	18	Not Granted	Granted
2408	VM-231	22	10	VM-231	25	11	Granted	Not Granted
2091	VM-147	21	15	VM-147	23	16	Granted	Not Granted
4555	VM-292	21	28	VM-292	22	21	Granted	Not Granted
4799	VM-298	19	22	VM-298	21	25	Granted	Granted

Further the results are visualized graphically here [Fig – 5].

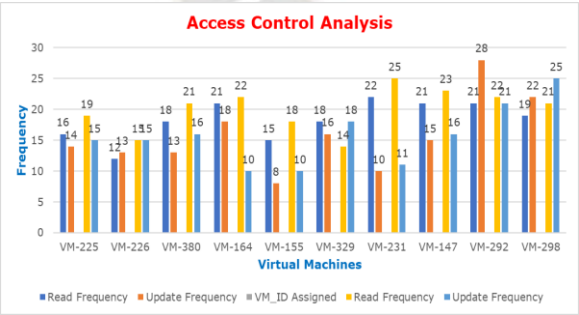

Figure 5. Access control results analysis

From the obtained results it is natural to realize that few of the auditors' requested frequencies are more the permissible range of the virtual machines. Thus, those access requests are not granted.

Sixth, the updated access control results are furnished. During this phase, if the requested frequencies are higher than the mean threshold, then the access to the virtual machines are re-altered and further granted as few samples are demonstrated here [Table – 6].

Table 6. Updated access level results

Auditor_ID	*VM Requested*	*Read Frequency*	*Update Frequency*
2080	VM-225	Granted	Not Granted
4028	VM-226	Granted	Updated - Granted
2463	VM-380	Granted	Not Granted
3676	VM-164	Granted	Updated - Granted
2920	VM-155	Granted	Not Granted
2804	VM-329	Updated - Granted	Granted
2408	VM-231	Granted	Not Granted
2091	VM-147	Granted	Not Granted
4555	VM-292	Granted	Not Granted
4799	VM-298	Granted	Granted

Here few of the samples are showcased, where based on the virtual machine dynamic thresholds, the access levels are updated.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

Seventh, the time complexity analysis for the selective encryption and decryption are produced [Table – 7].

Table 7. Cryptographic time complexity analysis

VM_ID	*VM_Size (TB)*	*Encryption Time (ms)*	*Decryption Time (ms)*
VM-225	3	97.132	298.06
VM-226	5	81.615	243.435
VM-380	4	72.003	410.18
VM-164	5	73.434	428.745
VM-155	4	71.147	240.088
VM-329	3	99.57	161.718
VM-231	5	40.723	152.088
VM-147	5	99.585	485.81
VM-292	5	61.54	265.128
VM-298	6	46.874	207.696

As already mentioned, after the initial partitioning of the virtual machines, the standard RSA algorithm is deployed for encryption and decryption of the virtual machines. The results are visualized graphically here [Fig – 6].

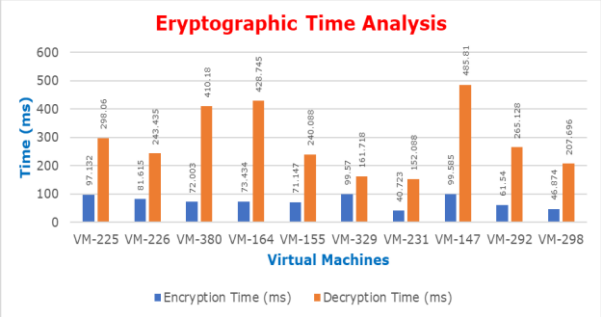

Figure 6. Eryptographic time analysis

Significant to observe that the time complexity is very high due to the higher size of the virtual machines. In the other work by the same author have significantly produced few algorithms to critically reduce the time complexity by proposing yet novel model for gigantic sized virtual machine encryptions.

Further, in the light of the obtained results, final research conclusion is presented in the next section of this work.

IX. CONCLUSION

The rapid growth of cloud computing has compelled and enabled a large number of application developers to deploy their applications on cloud platforms. The most significant challenge of cloud computing is that the service provider or application provider must adhere to a large number of rules and regulations. External auditors validate and check these compliance reports on a regular basis to ensure they are accurate. The auditing process for cloud services is critical, and access controls must be enabled in order to be effective. In most cases, this access control mechanism is compromised as a result of the increased complexity and reduced flexibility of virtual machines, as previously stated. In this paper, we propose four algorithms to identify and improve the LBAC mechanism for cloud services with access updates. These algorithms are based on time variant characteristics analysis, predictive analysis, and selective cryptographic methods to identify and improve the LBAC mechanism. To overcome three major issues in cloud service management, such as selective LBAC, static privileges, and open access control for auditors, the proposed model achieves significantly better results than the existing model.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Z. Birnbaum, B. Liu, A. Dolgikh, Y. Chen and V. Skormin, "Cloud Security Auditing Based on Behavioral Modeling," *2013 IEEE Ninth World Congress on Services*, Santa Clara, CA, USA, pp. 268-273, 2013.

[2] A. Ganapathy, G. Soman, Godwin Manoj VM and R. Lekshamana, "Online Energy Audit and Renewable Energy Management System," *2016 International Conference on Computing Communication Control and automation (ICCUBEA)*, Pune, India, pp. 1-6, 2016.

[3] S. Shetty, "Auditing and Analysis of Network Traffic in Cloud Environment," *2013 IEEE Ninth World Congress on Services*, Santa Clara, CA, USA, pp. 260-267, 2013.

[4] R. Houlihan, X. Du, C. C. Tan, J. Wu and M. Guizani, "Auditing cloud service level agreement on VM CPU speed," *2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, Australia, pp. 799-803, 2014.

[5] M. Oqaily et al., "SegGuard: Segmentation-Based Anonymization of Network Data in Clouds for Privacy-Preserving Security Auditing," in *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2486-2505, 1 Sept.-Oct. 2021.

[6] F. Doelitzscher, C. Fischer, D. Moskal, C. Reich, M. Knahl and N. Clarke, "Validating Cloud Infrastructure Changes by Cloud Audits," *2012 IEEE Eighth World Congress on Services*, Honolulu, HI, USA, pp. 377-384, 2012.

[7] Johri, P. ., Dhingra, M. ., Babu M., D. ., Sule, B. ., Kumar Pandey, A. ., & Karale, A. V. . (2023). Reuse Attack Prevention Through Randomization Traversal Algorithm with the Code Reduction Technique for Operating System Security. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 29–34. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2528

[8] D. Zhu, Z. Fan and N. Pang, "A Dynamic Supervisory Mechanism of Process Behaviors Based on Dalvik VM," *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, Jabalpur, India, pp. 1203-1210, 2015.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7412
***Article Received**: 04 May 2023 **Revised:** 29 June 2023 **Accepted:** 24 July 2023*

[9] S. Thorpe, T. Grandison, A. Campbell, J. Williams, K. Burrell and I. Ray, "Towards a Forensic-Based Service Oriented Architecture Framework for Auditing of Cloud Logs," *2013 IEEE Ninth World Congress on Services*, Santa Clara, CA, USA, pp. 75-83, 2013.

[10] Verma, D. N. . (2022). Access Control-Based Cloud Storage Using Role-Fully Homomorphic Encryption Scheme. Research Journal of Computer Systems and Engineering, 3(1), 78–83. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/46

[11] J. Schiffman, Y. Sun, H. Vijayakumar and T. Jaeger, "Cloud Verifier: Verifiable Auditing Service for IaaS Clouds," *2013 IEEE Ninth World Congress on Services*, Santa Clara, CA, USA, pp. 239-246, 2013.

[12] Mr. Dharmesh Dhabliya, Ms. Ritika Dhabalia. (2014). Object Detection and Sorting using IoT. International Journal of New Practices in Management and Engineering, 3(04), 01 - 04. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/31

[13] J. Lau, M. Arnold, M. Hind and B. Calder, "A Loop Correlation Technique to Improve Performance Auditing," *16th International Conference on Parallel Architecture and Compilation Techniques (PACT 2007)*, Brasov, Romania, pp. 259-269, 2007.

[14] M. K. Srinivasan, K. Sarukesi and P. Revathy, "Architectural design for iCloudIDM Layer-II (iCloudIDM-LII) Subsystem of eCloudIDS generic security framework," *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Mysore, India, pp. 1668-1674, 2013.

[15] Yubin Xia, Yutao Liu, H. Chen and B. Zang, "Defending against VM rollback attack," *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012)*, Boston, MA, USA, pp. 1-5, 2012.

[16] Elena Petrova, Predictive Analytics for Customer Churn in Telecommunications , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[17] M. K. Srinivasan, K. Sarukesi and P. Revathy, "eCloudIDS Tier-1 iCloudIDM Layer-I (iCloudIDM-LI) Subsystem Design and Implementation through User-centric Identity Management Approach for Secure Cloud Computing Environment," *2013 IEEE 14th International Conference on Mobile Data Management*, Milan, Italy, pp. 206-211, 2013.

[18] H. Litz, B. Braun and D. Cheriton, "EXCITE-VM: Extending the virtual memory system to support snapshot isolation transactions," *2016 International Conference on Parallel Architecture and Compilation Techniques (PACT)*, Haifa, Israel, pp. 401-412, 2016.

[19] P. Massonet, S. Naqvi, C. Ponsard, J. Latanicki, B. Rochwerger and M. Villari, "A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures," *2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum*, Anchorage, AK, USA, pp. 1510-1517, 2011.

[20] S. Barjatiya and P. Saripalli, "BlueShield: A Layer 2 Appliance for Enhanced Isolation and Security Hardening among Multi-tenant Cloud Workloads," *2012 IEEE Fifth International Conference on Utility and Cloud Computing*, Chicago, IL, USA, pp. 195-198, 2012.

[21] Anna, G., Jansen, M., Anna, J., Wagner, A., & Fischer, A. Machine Learning Applications for Quality Assurance in Engineering Education. Kuwait Journal of Machine Learning, 1(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/109

[22] T. F. J. Pasquier, J. Singh, D. Eyers and J. Bacon, "Camflow: Managed Data-Sharing for Cloud Services," in *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 472-484, 1 July-Sept. 2017.

[23] A. Ochani and N. Dongre, "Security issues in cloud computing," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, pp. 783-787, 2017.

[24] Basaligheh, P. (2021). A Novel Multi-Class Technique for Suicide Detection in Twitter Dataset. Machine Learning Applications in Engineering Education and Management, 1(2), 13–20. Retrieved from http://yashikajournals.com/index.php/mlaeem/article/view/14

[25] K. Ravindran, K. Fayzullaev and Y. Wardei, "Model-based techniques for QoS assessment of cloud-hosted CDN services," *2016 IEEE/ACM 24th International Symposium on Quality of Service (IWQoS)*, Beijing, China, pp. 1-6, 2016.

[26] PlanetLab. http://www.planet-lab.org/.