Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 07 July 2026
Revised 12 Aug 2026
Accepted 31 Aug 2026

Natural Resources for Human Health 2026, Vol. 6 (20s): 1552–1570

KEYWORDS:
Resource Management; CloudSim Plus; Network Behavior; Bandwidth; Latency

Security-Aware Cloud Environment Modelling and Resource Profiling for Intelligent Cloud Resource Management

Veena Vijayan V K [1], Dr. Periyasami [2]

[1]Research Scholar, Department of Computer Science and Application, Park's College (Autonomous), Chinnakarai, Thiruppur, veenapuradam@gmail.com, 0009-0005-3332-2705

[2] Department of Computer Science and Application, Park's College (Autonomous), Chinnakarai, Thiruppur, drperi1975@gmail.com

ABSTRACT: The quick extension of cloud computing has yielded in emergingly diverse methodologies, adaptable workloads, and complicated interaction ecosystems, generating difficulties for effective and secure resource management. Traditional cloud resource management methodologies primitively consider computational resource accessibility and usage, while security-relevant characteristics are generally treated independently. The proposed Integrated Security-Aware Cloud Resource Profiling Framework that combines computational, workload, network, and security characteristics into a unified cloud resource profile. The proposed approach models diverse cloud frameworks utilizing CloudSim Plus and includes network behavior via NS-3. Diverse workloads are characterized as per the memory, processing, bandwidth, execution, priority, latency, and security essentials. VMs and physical hosts are consequently profiled based on resource capacity, workload allotment, utilization, security characteristics and operational conditions is performed at workload, VM, and host levels utilizing access nature, resource threats, interaction trends, policy compliance and security events. The developed frame accomplished 98.3%, 97.2%, 96.1% and 96.7% of accuracy, precision, recall, and F1-score respectively. For security profiling with 18.5%, 97.8% and 12.4ms of resource usage, profiling accuracy, and mean network latency respectively. The resulting hybridized security-aware cloud model facilitates a systematic base for consequent smart resource allotment and orchestration.

1. INTRODUCTION

For delivering scalable computational, storage, and networking services cloud computing has become a fundamental computing paradigm via transferred and virtualized frameworks (Tuli et al., 2022). The progressive growth of cloud-based usability has resulted in emergingly diverse computing ecosystems in which physical hosts, network resources, Virtual Machines (VMs) and workloads exhibit several resource needs and functional characteristics (Luo & Li, 2026). In such ecosystems, workloads may differ notably in terms of memory intake, CPU demand, bandwidth essentials, priority, execution time, latency sensitivity, and security needs. Subsequently, efficient cloud management needs progressive characterization of resource accessibility and workload nature of maintain effective usage and reliable service delivery (Dong, 2023). Simulation-based cloud modelling facilitates a significant methodology for indicating such diverse ecosystems and analysing resource-management techniques prior implementation in physical frameworks. The emerging dynamism and diversity of cloud ecosystems have proposed multiple resource-management difficulties (Gao et al., 2022). Traditional resource allotment methodology may primitively consider dynamic resource accessibility without adequately representing workload dynamics, physical-host status, VM behavior, and communication characteristics simultaneously. Fluctuations in workload intensity can outcome in resource contention, underusage, host overload, and ineffective VM allotment (Montazerin & Shameli-Sendi, 2025). In addition, network

characteristics namely communication delay, bandwidth accessibility, congestion and traffic behavior can impact the performance of cloud ecosystem model should characterize computational and communication resources together rather than treating them as independent factors (Wang et al., 2025). In this context, accurate workload characterization and resource profiling are required for understanding the functional state of diverse cloud architecture. Security is an equally significant dimension due to several workloads and VMs may exchange common physical framework (Zhu et al., 2026). Virtualization and resource transferring can propose risks correlated with access nature, communication trends, abnormal resource consumption, policy violation, and security events (Bhonde & Devane, 2024). Subsequently, computational capability alone cannot determine the appropriateness of a resource for a specific workload. Security status must be noted alongside resource accessibility and functional nature, motivating the requirement for security-aware profiling throughout workloads, VMs, and physical hosts (Souza et al., 2023).

Earlier researches have examined cloud simulation, VM placement, resource allotment, workload prediction, and security-aware resource management. However, these fields are generally addressed independently (Thabet et al., 2023). Resource management methodologies often underscore usage, placement, workload dynamism or migration, while security-based methods primitively concentrate on attack estimation, secure VM allotment or isolation. Simultaneously, simulation architectures support cloud and edge frameworks modelling but may not facilitate a combined representation of computational, security and network conditions throughout several resource levels (Ma et al., 2026). Thus, an important research gap retained in combinedly modelling workload, VM, physical host, network, resource-usage, and security features under a single clod profile. To surpass these limitations, proposes Integrated Security-Aware Cloud Resource Profiling Framework (ISACRP) methodology for diverse cloud infrastructures. The architecture models the cloud ecosystem utilizing CloudSim Plus and network nature utilizing NS-3. Diverse physical hosts and VMs are configured as per their resource capabilities, while workloads are characterized utilizing memory, bandwidth, processing, execution, latency, priority, and security needs. VM and physical-host profiling consequently records resource capability, workload allotments, usage, functional status, and security characteristics, while network profiling notes latency, traffic nature, bandwidth, and congestion. The architecture further includes multi-level security profiling at workload, VM, and physical host levels by analysing access nature, communication trends, resource anomalies, security events and policy compliance. These profiles are combined to create a unified security-aware cloud resource profile comprising workload characteristics, host accessibility, VM conditions, network status, resource usage, and security risk details. The architecture is analysed utilizing accuracy, F1-score, precision, recall, profiling accuracy, resource usage, and network latency to assess security categorization and functional performance. The key contributions of the proposed ISACRP model are as follow,

- A diverse cloud environment modelling architecture combines VMs, physical hosts, and network resources utilizing CloudSim Plus and NS-3.
- A multilevel security-aware profiling methodology characterizes workloads, physical hosts, and VMs based on resource behavior and security status.
- A hybridized security-aware cloud profile integrates workloads, host, VM, resource usage, network, and security details to support future smart resource management.

Natural Resources for Human Health
eISSN: 2583-1194

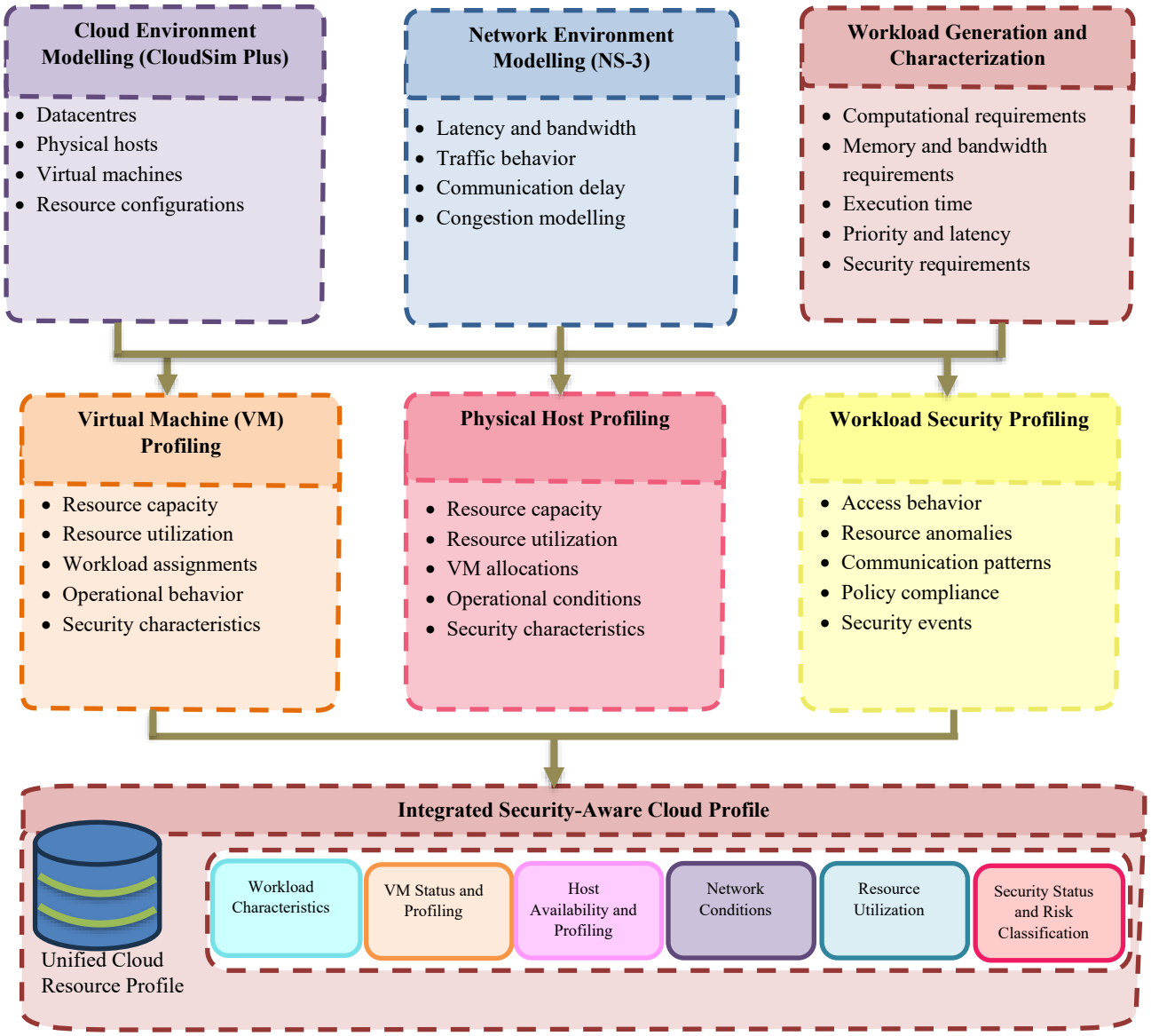


Figure 1. Multi-Level Cloud State Characterization and Details Workflow

The sequential flow from architecture configuration and interaction modelling to workload characterization and resource-state assessment is presented in Figure 1. It records VM, physical host, and workload-level characteristics, incorporating functional, behavioral and security-relevant features. The gathered details are consolidated to exhibit resource conditions, usage, network status, and associated risk conditions. This pipeline establishes the systematic details essential for substantial cloud resource-management processes.

The remainder of this paper is structures as follow Section 2 discusses the related works, Section 3 explains the proposed ISACRP methodology, Section 4 presents the empirical results and comparative analysis. Finally, Section 5 concludes the methodology and presents future research directions.

2. RELATED WORK

Latest investigation on cloud and edge calculating has emergingly concentrated on resource management, simulation reliability, security-aware resource allotment and virtualization. An architecture called SimTune was proposed (Tuli et al., 2022) for

decreasing the simulator-reality gap in edge-cloud resource handling by refining minimal fidelity simulation variables utilizing a surrogate model. The model results illustrated enhancements in energy intake and reaction time, emphasizing the significance of real-world simulation ecosystems for analysing resource-management techniques. In a contrast pathway, security-aware multi-tenant Service Function Chain (SFC) implementation was investigated (Gao et al., 2022) including manual-isolation concerns into resource placement. Their hypergraph-oriented methodology point outed the combined needs of resource intake and security, illustrating that security restrictions must be noted alongside traditional resource effective objectives.

Security-aware VM placement has also obtained focus as cloud frameworks become emergingly revealed to co-location and virtualization-relevant attacks. A secure VM placement technique was proposed (Thabet et al., 2023) utilizing Monte Carlo simulation and hypothesis testing to estimate security levels and regulate insecure placements. The technique illustrated the feasibility of hybridizing security estimation into VM placement while managing acceptable performance of energy. An agent-based cloud simulation model was introduced (Dong, 2023) in which cloud factors are indicated as autonomous agents able of communicating asynchronously. The architecture was utilized to investigate service placement, migration, energy intake, server consolidation, resource usage, and Service Level Agreement violations throughout same and diverse cloud environments. A python-based simulation architecture called EdgeSimPy was introduced (Souza et al., 2023) for modelling network devices, edge servers, mobility, applications, power intake and application compositions. Its modular design avails resource-management policies to be evaluated within heterogeneous edge-computing situations. A priority-based security-aware VM allotment policy was introduced (Bonde and Devane, 2024) a multidimensional attack score based on network, virtual-machine-surveil, physical-machine characteristics and hosted-VM. The findings represents that security-aware prioritization can decrease the attack level of cloud datacentres with restricted additional energy overhead.

Resource prediction and adaptive resource management have consequently become significant for managing adaptable cloud workloads. A variations-aware VM placement methodology that predicts future resource needs was proposed (Montazerin and Shameli-Sendi, 2025) utilizing time series details and Long Short-Term Memory or Gated Recurrent Unit models. The findings illustrated decrease in VM migrations and placement break downs compared with traditional placement techniques, representing the value of uninterruptedly surveilling resources characteristics rather than depending only on dynamic resource accessibility. Simultaneously, the elastic virtual resource management infrastructure was proposed (Wang et al., 2025) which combines surveilling, evaluation, planning and execution with deep reinforcement learning for adaptive CPU, memory, and bandwidth allotment. The outcome presents that learning-oriented resource management can enhance execution performance and resource usage within adaptably fluctuating workloads. Multiple investigations have also pint out the computational complications and systematical featurization of VM placement. A relax-and-round refining method for online NUMA-aware VM placement was proposed (Hu et al., 2025) targeting to accomplish effective placement while conserving resource restrictions in large-scale cloud environments. Through a topology-aware VM placement (Ma et al., 2026) expanded this pathway, including multi-layer datacentre topology and future resource demand into placement decisions. Their value-oriented methodology noted both current and potential future resource usage, illustrating the significance of architecture topology and long short-term resource accessibility in cloud resource management. Simulation based methodologies facilitate a significant base for analysing such resource-management techniques prior implementation. More recently, an improved multi-access edge computing simulator called MECSim was proposed (Islam and Ghose, 2026) supporting diverse architecture, multi-datacentre ecosystems, dependent operations, energy management, cost and profit modelling, replication, caching, and transient-failure simulation. These enhancements illustrate the increasing requirement for simulation methodology caliber of indicating diverse computational, communication, reliable and energy characteristics.

Table 1. Comparative Analysis of Prior Methods in Cloud Resource and Security Management

Author(s) & Year	Study Focus	Technique/Model Used	Key Contribution	Limitations
Tuli et al., 2022	Focused on resource management in hybrid edge-cloud computing	Low-fidelity surrogate model, high-fidelity simulator	The model tuning can improve resource management performance, energy, and response time, also	The simulation errors may affect the resulting models, requires further validation across various

			helps co-simulation methods	infrastructures, scalability limits of simulator tuning.
Gao et al., 2022	Addresses secure and resource-efficient, effective placement of multitenant SFC	Non-uniform weighted hypergraph construction, hypergraph matching algorithm	Integrated with security constrains based on physical isolation, the proposed approach lower resource consumption	further validation needs for real world deployment and scalability, introduces computational complexity.
Zhai et al., 2022	Focused on security and delay-efficient SFC deployment in network function virtualization	Security-constraint and Function-Mutex-constraint Consolidation (SFMC), Security-Aware SFC deployment, Viterbi algorithm	improved resource utilization, long-term revenue-to-cost ratio, load balancing and acceptance ratio.	real deployment validation is still required, model depends on security level, resource availability, selected constrains and network load, scalability result is very large number.
Nawrocki et al., 2022	Security-aware task allocation in Mobile Cloud Computing	Machine Learning, Mobile cloud security simulation environment	it can conclude with data confidentiality, processing time, resource utilization and energy consumption, the results showed improved security and computational tasks.	Further validation needs for real-world mobile-cloud environments, the resource depends on the mobile-device, communication conditions, user-defined security requirements.
Liang et al., 2022	Focused on Energy-efficient and performance-aware resource management in Cloud Data Centers (CDCs)	High-applicability heterogeneous CDC resource management algorithm based on Trusted VM Migration (HTVM2), one-dimensional and multidimensional trusted VMs	HTVM2 framework supports both one-dimensional and multidimensional VM migration, it can improve VM migration success rate, load balancing, and energy efficiency,	Further validation requires to other applicable distributes or edge-computing environments, VM can introduce migration overhead and resource/network costs.
Bhattacharya et al., 2022	Focused on modelling and prediction of heterogeneous cloud application performance and resource utilization	Two resource-utilization prediction algorithms, CPU, disk, VM live migration	Build a prediction framework for estimating and evaluating virtualized-resource usage and performance trends, the model showed good curve fitting, also supporting prediction fast.	It may limited generalization to higher diverse cloud applications, Cache coherence can affect accuracy and system configuration is sensitive issue.
Dong 2023	Focused on cloud resource management simulation for	Agent-based cloud simulation model, major cloud components	The agent-based modeling can accurately reflect cloud status, the simulator can used to	The behavior not fully capture for real-large scale cloud framework; accuracy depends on the

	service, placement, migration and consolidation		assess resource-management strategies and energy-consumption models.	models used to represent cloud components and energy consumption.
Souza et al., 2023	Focused on Application provisioning and resource management in Edge-computing	EdgeSimPy, within modular architecture, network devices, user mobility, application consumption, power consumption	Gives a broader simulation framework, it can support real-application traces, case studies involving large-scale edge-computing scenarios.	The framework depends on the simulation, the accuracy based on the underlying models for mobility, application, networking, power consumption.
Bhonde and Devane 2024	developed Security-aware VM allocation in CDCs, within vulnerable VMs placed on the Physical Machine (PM)	VM allocation policy, network, Virtual Machine Migration (VMM) / hosted VMs, and PM dimensions	The model reduces the overall data-center threat, with increase in energy consumption for network, hosted VMs/VMM, and PM respectively.	The application needs further validation across different cloud environments, attack scenarios, and data-center scale, introduces a security may cause increase energy consumption.
Islam and Ghose 2026	Focused on resource and simulation in heterogeneous Multi-access Edge Computing (MEC), and addressed energy, economic factors, reliability	Multi-access Edge Computing Simulator, multi-data-center clusters, DVFS-enabled devices, dependent-task modeling, transient-failure simulation, caching, and task replication	Provides a broad simulator, offloading and scheduling, the model achieved an average reduction in simulation time compared with EdgeCloudSim,	the model may not fully observe all condition of real deployments, increased complexity, further validation requires across various hardware, workloads, network conditions, and failure patterns.
Elsedimy et al., 2025	Developed a Multi-objective VM placement in CDCs, within load balancing, performance degradation and power consumption	Quantum Particle Swarm Optimization–based Multi-Objective VM Placement (QPSO-MOVMP), Pareto-optimal VM placement solutions, physical machines	The results showed better power-consumption and performance degradation, and providing better-distributed Pareto solutions than the comparison method.	The real-world cloud deployment needs further validation, it may increase computational overhead, and the security network traffic, migration cost, hardware requires further validation.

The chosen prior researches as per their investigators focus, adopted approaches, key innovations and restrictions overview is presented in Table 1. It presents diverse techniques to point out workload management, resource handling, cloud simulation, network status, VM placement, and security issues. The recognized restriction underscores the aspects that are resolved collaboratively in the developed methodology.

Overall, the existing investigations illustrate significant advancements in cloud simulation, diverse resource modeling, VM placement, dynamic resource allotment, workload prediction, and security-aware resource management. However, these aspects are repeatedly addressed as isolate factors. Simulation-based models primitively underscore framework and resource characteristics, whereas security focuses majorly on placement restrictions, attack estimation, or VM allotment. Simultaneously,

resource management methodologies generally concentrate on CPU, memory, bandwidth, migration or usage without building a unified representation of workload features, VM conditions, physical-host conditions, network characteristics, and security risk. This generates a methodological gap for a hybridized security-aware cloud profiling architecture capable of combinedly characterized workloads, VMs, physical hosts, network conditions, resource usage, and security status. The proposed ISACRP resolved the difficulties by designing a unified cloud environment model in which computational, communication, operational and security characteristics are consequently profiled, facilitating a systematic base for significant smart resource allotment and orchestration. This straight away aligns with the proposed ISACRP objective of introduced a security aware cloud model that combines diverse resources, workload essentials, network status, and security characteristics.

3. PROPOSED INTEGRATED SECURITY-AWARE CLOUD RESOURCE PROFILING FRAMEWORK (ISACRP)

The formulated ISACRP infrastructure establishes a progressive pipeline for modelling and profiling a diverse cloud environment by hybridizing workloads, computational resources, VMs, network conditions, security characteristics, and physical hosts. The pipeline starts with cloud infrastructure activation and progresses via network modelling, workload characterization, VM profiling, physical-host profiling, multi-level security profiling, security risk categorization, and profile hybridization. The output created at every stage is utilized as the input for the consequent stage, ultimately yielding a unified security aware cloud environment model. CloudSim Plus is utilized for cloud framework modelling, while NS-3 is utilized to model network nature and communication conditions.

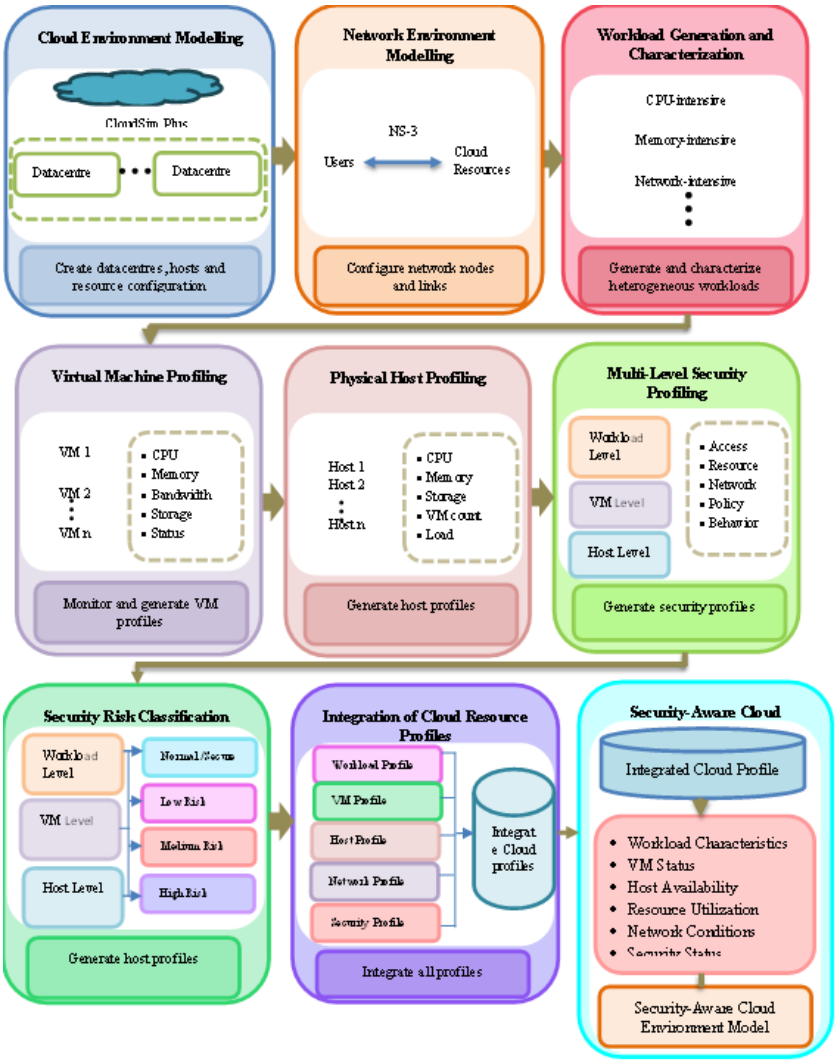


Figure 2. Overview of Workflow of Proposed ISACRP

Figure 2 presents the pipeline of proposed ISACRP architecture comprises of nine sequential levels namely cloud environment modelling, network environment modelling, heterogeneous workload creation and characterization, virtual machine profiling, physical host profiling, multi-level security profiling, security risk categorization, hybridization of workload, VM, host, network, and security profiles into a combined cloud profile, and formulation of the security-aware cloud ecosystem model. The yielding model combinedly presents workload characteristics, host resource accessibility, VM conditions, resource usage, security conditions, network status, risk categorization for security-aware cloud resource management.

The pipeline starts by setting up the cloud simulation ecosystem and building diverse physical host and datacentres. Every physical host is configured with different CPU, memory, storage, and bandwidth capabilities to represents the heterogeneity of resource accessible in real-world cloud frameworks. The datacentre layer handles the physical host, while the host layer facilitates the computational resources needed for VM deployment. VM allotment and scheduling methodology are activated to introduce the connection between workloads, VMs, and physical hosts. For a physical host H_j, the accessible resource capability $R_j^{available}$ is determined as,

$$R_j^{available} = R_j^{capacity} - R_j^{allocated} \tag{1}$$

Where,

$R_j^{capacity}$ = the total capacity of the resource

$R_j^{allocated}$ = the amount currently allotted to active VMs

Once the computational frame is established, the communication ecosystem is modelled utilizing NS-3. Network nodes and communication connections are configured to indicate communication between workloads, VMs, users, hosts, and cloud resources. The network environment records bandwidth accessibility, communication delay, packet transmission nature, traffic intensity, and congestion status. These features are associated with the corresponding workloads and cloud resources so that network nature can be noted together with computational conditions. The communication delay for a transmitted packet is indicated as,

$$D_i = t_i^{arrival} - t_i^{send} \tag{2}$$

Where,

t_i^{send} = packet transmission time

$t_i^{arrival}$ = packet arrival time.

The average communication delay is computed as,

$$D_{avg} = \frac{1}{N}\sum_{i=1}^{N} D_i \tag{3}$$

Where,

N = the total number of observed packets

Next, heterogeneous workload requests are created with several memory, computational, execution, communication, latency, security and priority essentials. Every workload is characterized as per the memory needs, CPU demand, execution length, bandwidth essentials, priority, latency sensitivity, arrival nature and essential security level. Based on these characteristics, workloads can represent CPU-intensive, network-intensive, memory-intensive, latency sensitive, or security-sensitive usability. For workload W_i, the workload profile is presented as,

$$W_i = \{CPU_i, Mem_i, BW_i, Exec_i, P_i, L_i, S_i\} \tag{4}$$

Where,

CPU_i = computational requirements

Mem_i =memory requirements

BW_i= bandwidth requirements

$Exec_i$=execution requirement

P_i=priority

L_i=latency sensitivity

S_i=required security level

Once the workload features are established, the accessible VMs are profiled as per to their current resource and functional conditions. The profiling process records CPU capacity and usage, processing elements, assigned and used memory, bandwidth allotment and usage, storage allotment, workload allocation, execution status, and current security condition. These characteristics facilitate an adaptable representation of the state of every VM. The resource usage of a VM is denoted as,

$$U_{VM} = \frac{R_{used}}{R_{allocated}} \times 100 \quad (5)$$

Where,

R_{used}= amount of resource currently consumed

$R_{allocated}$= amount of resource allocated to the VM

For multiple resource dimensions, the mean usage can be indicated as,

$$U_{VM}^{avg} = \frac{U_{CPU}+U_{Memory}+U_{Bandwidth}}{3} \quad (6)$$

The yielding VM profile represents whether the VM has sufficient capacity, is underusage, is highly used, or is experiencing abnormal resource behavior. The VM level details is then aggregated at the physical-host level to determine the functional state of each host. Memory usage, CPU usage, storage accessibility, bandwidth accessibility, active VM count, host load, workload intensity, operational conditions and remaining capacity are investigated. The connections between active VMs and their underlying physical host is utilized to determine the overall resource status of every host. The host usage is computed as,

$$U_H = \frac{R_{consumed}}{R_{capacity}} \times 100 \quad (7)$$

Where,

$R_{consumed}$= resource consumed by active VMs

$R_{capacity}$= total host capacity

The remaining resource capacity is defined by,

$$R_H^{remaining} = R_H^{capacity} - R_H^{consumed} \quad (8)$$

Where,

$R_H^{remaining}$= Remaining resource capacity of host H,

$R_H^{capacity}$= Total accessible resource capacity of host H, and

$R_H^{consumed}$= Amount of resources currently consumed by the workloads running on host H

These values enable to be characterized as per their resource accessibility and current load conditions. After establishing the computational and operational profiles, security profiling is executed at three levels namely workload, VM, and physical host. At the workload level, access behavior, communication trends, resource utilization, policy compliance and security necessities. At the VM level, resource anomalies, authorization and access nature, communication deviations, unexpected workload behavior, policy compliance, and isolation conditions are considered. At the physical-host level, resource anomalies, access

events, policy compliance, network deviations, unusual VM activity and security events are investigated. The security profile of an entity E_i can be represented as,

$$S_i = \{A_i, R_i, N_i, P_i, B_i, E_i\} \quad (9)$$

Where,

A_i= access characteristics,

R_i= Resource requirement of workload i,

N_i= resource behavior,

P_i= network behavior,

B_i= behavioral characteristics, and

E_i= observed security events.

The security characteristics gathered from workloads, VMs, and physical hosts are then analyzed to recognize deviations from expected behavior. Unauthorized access behavior, Abnormal resources consumption, unusual communication trends, security events and policy violations are noted during categorization. Based on the observed characteristics, every entity is allotted a suitable security status namely normal/secure, low risk, medium risk, or high risk. The classification process can be indicated as,

$$C_i = f(A_i, R_i, N_i, P_i, B_i, E_i) \quad (10)$$

Where,

C_i= security classification,

$f(\cdot)$= the classification process applied to the collected security characteristics.

The workload, VM, network profiles and physical-host are consequently combined with security categorizations to build a unified representation of the cloud environment. The hybridized profile integrates the resource accessibility of physical hosts, the computational needs of workloads, the current status Of VMs, resource usage, security conditions, and network status. The overall cloud profile can be denoted as,

$$P_{Cloud} = \{W, VM, H, N, R, S\} \quad (11)$$

Where,

W= workload characteristics,

VM= VM status,

H= physical-host conditions,

N= network characteristics,

R= resource availability and utilization, and

S= security information

The hybridization procedure creates a connection between resource accessibility and security status. Subsequently, a resource is denoted not only by its computational capacity but also by its utilization, current workload assignment, security status, and communication conditions. The last stage yields the security the security-aware cloud environment model from the integrated profiles. The resulting model comprises VM status, workload characteristics, resource usage, physical-host accessibility, network conditions, associated risk categorization and security status. This model facilitates a consolidated representation of the current functional and security state of the diverse cloud architecture. the created model assists as the base for substantial smart resource-management methodology. It allows future assignment and orchestration processes to consider workload necessities,

network status, accessible computational resources, security risks, and usage levels comprehensively rather than depending on resource accessibility alone.

Performance evaluation is conducted utilizing precision, F1-score to evaluate categorization and security profiling, while profiling accuracy, resource usage, and network latency are utilized to assess the functional characteristics of the modelled cloud environment. These metrics are implemented after security-aware cloud model has been created and therefore indicate analyzation criteria rather than factors of the proposed approach. The performance of the developed ISACRP architecture is analyzed utilizing security categorization and operational metrics. The following standard analysis measures are implemented to quantify the effectiveness and reliability of the created security-aware cloud profile,

- **Precision**

$$Precision = \frac{TP}{TP+FP} \tag{12}$$

Where,

TP= True Positive, and

FP= False Positive

- **F1-score**

$$F1\text{-}Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{13}$$

Where,

$Recall = \frac{TP}{TP+FN}$, $FN = False\ Negative$

- **Resource Utilization**

$$Resource\ Utilization = \frac{R_{used}}{R_{available}} \times 100 \tag{14}$$

Where,

R_{used}= utilized resource capacity, and

$R_{available}$= the available resource capacity

- **Profiling Accuracy**

$$Profiling\ Accuracy = \frac{N_{correctly\ profiled}}{N_{total}} \times 100 \tag{15}$$

Where,

$N_{correctly\ profiling}$ = number of correctly characterized resources, and

N_{total}= total number of profiled resources

- **Network Latency**

$$Network\ Latency = \frac{1}{N}\sum_{i=1}^{N} (t_i^{arrival} - t_i^{send}) \tag{16}$$

Where,

N= number of observed transmissions,

t_i^{send}= the transmission time, and

$t_i^{arrival}$= corresponding arrival time

Natural Resources for Human Health
eISSN: 2583-1194

Algorithm: Multi-Level Resource and Security Assessment

Input: Heterogeneous cloud infrastructure, workload requests, VM configurations, physical-host configurations, network parameters, and security characteristics.
Output: Integrated Security-Aware Cloud Environment Profile.
Begin

// Initialize CloudSim Plus and NS-3 network environments
// Configure heterogeneous physical hosts and VMs
// Configure network nodes, links, bandwidth, and latency
// Generate workload requests
For each workload W_i do
    Extract CPU, memory, bandwidth, execution, priority, latency, and security requirements
    Characterize W_i and assign it to a suitable VM
End For
For each VM_j do
    Monitor CPU, memory, bandwidth, storage, and workload status, Calculate VM resource utilization
    If $VM\ utilization\ <\ Lower_Threshold$ then
        Set VM status = Underutilized
    Else if $VM\ utilization\ >\ Upper_Threshold$ then
        Set VM status = Highly Utilized
    Else
        Set VM status = Normally Utilized
    End If
    Generate VM profile
End For
For each Physical Host H_K do
    Aggregate VM resource information
    Monitor host utilization, load, bandwidth, and remaining capacity
    If $host\ utilization\ >\ Overload_Threshold$ then
        Set host status = Overloaded
    Else if $host\ utilization\ >\ High_Load_Threshold$ then
        Set host status = Highly Utilized
    Else
        Set host status = Available
    End If
    Generate physical-host profile
End For
For each workload, VM, and physical host do
    Analyze access, resource, network, and behavioral characteristics
    Check policy compliance and security events
    If abnormal behavior is detected then
        Assign corresponding security-risk condition
    Else
        Assign security status as normal
    End If
End For
Integrate workload, VM, host, network, and security profiles
Generate and return the security-aware cloud environment profile

End

4. RESULTS AND DISCUSSION

The analysis presents the empirical setup and parameter configuration utilized to model the heterogeneous cloud ecosystem, succeeded by the performance assessment of the proposed ISACRP methodology utilizing the defined security and operational metrics. The received outcomes are interpreted to investigate the efficiency of the proposed ISACRP architecture within the

noted simulation conditions. A comparative analysis with being techniques is also facilitated, followed by an overall assessment of the proposed infrastructure and its importance for security-aware cloud resource management.

The simulation ecosystem is designed utilizing CloudSim Plus for diverse cloud architecture modelling and NS-3 for network nature simulation as presented in Table 2. Several physical hosts and VMs are configure with fluctuating memory, CPU, storage, and bandwidth capacities. Heterogeneous workloads are created with several memory, processing, latency, bandwidth, security, and priority requirements. Network latency, traffic behavior, latency, and security needs. Network latency, bandwidth, traffic behavior, communication delay, and congestion are monitored, while resource usage and security status are profiled.

Table 2. Simulation and Configuration Details of Proposed ISACRP

Parameter	Configuration
Cloud Simulator	CloudSim Plus
Network Simulator	NS-3
Cloud Infrastructure	Heterogeneous datacentres and physical hosts
Physical Host Resources	CPU, memory, storage, and bandwidth
VMs	Different resource capacities and configurations
Workload Type	Heterogeneous cloud workloads
Workload Parameters	Processing, memory, bandwidth, execution length, priority, latency, security
Network Parameters	Latency, bandwidth, traffic behavior, communication delay, congestion
VM Monitoring	Resource allocation, utilization, workload assignment, execution status
Host Monitoring	CPU/memory utilization, bandwidth, storage, active VMs, host load
Security Profiling	Workload, VM, and physical-host levels
Security Characteristics	Access behavior, resource anomalies, communication patterns, policy compliance, security events
Security Categories	Secure/Normal, Low Risk, Medium Risk, High Risk
Implementation	Java and Python
Evaluation Metrics	Precision, F1-score, Resource Utilization, Profiling Accuracy, Network Latency

The developed infrastructure creates a combined profile of diverse cloud resources by integrating VM status, workload features, network behavior, physical host status, and security attributes. The security profiling performance is analysed utilizing accuracy, recall, precision, and F1-score, while the functional performance is assessed utilizing profiling accuracy, resource utilization, and network latency as represented in Table 3 and Figure 3. The effectiveness of the security categorization approach is indicated by the obtained precision and F1-score value of 98.7% and 98.75% respectively. Additionally, the operational characteristics of the simulated cloud environment is demonstrated utilizing resource utilization, profiling accuracy, and network latency of 32.6%,98.8% and 10ms respectively. Overall, the created profile facilitates a consolidated representation of resource accessibility and security conditions for significant intelligent resource management decisions.

Table 3. Performance Analysis of the Proposed ISACRP Model

Performance Metrics	Values
Precision	98.7%
F1-Score	98.75%
Resource Utilization	32.6%
Profiling Accuracy	98.8%
Network Latency	10ms

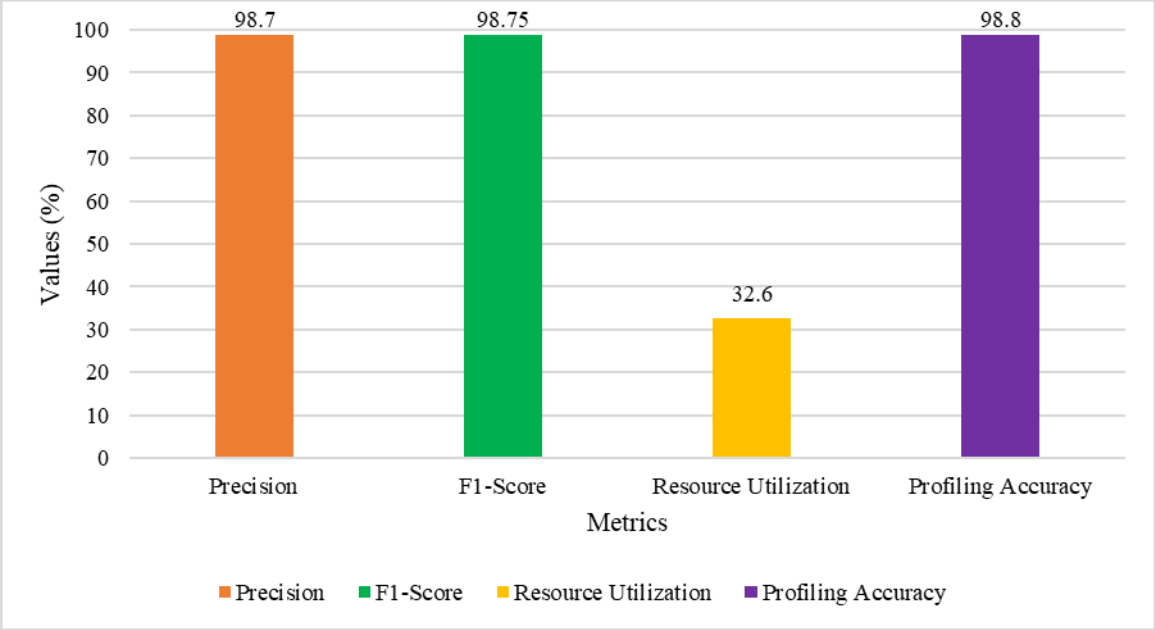


Figure 3. Visual Presentation of Performance of Developed ISACRP Methodology

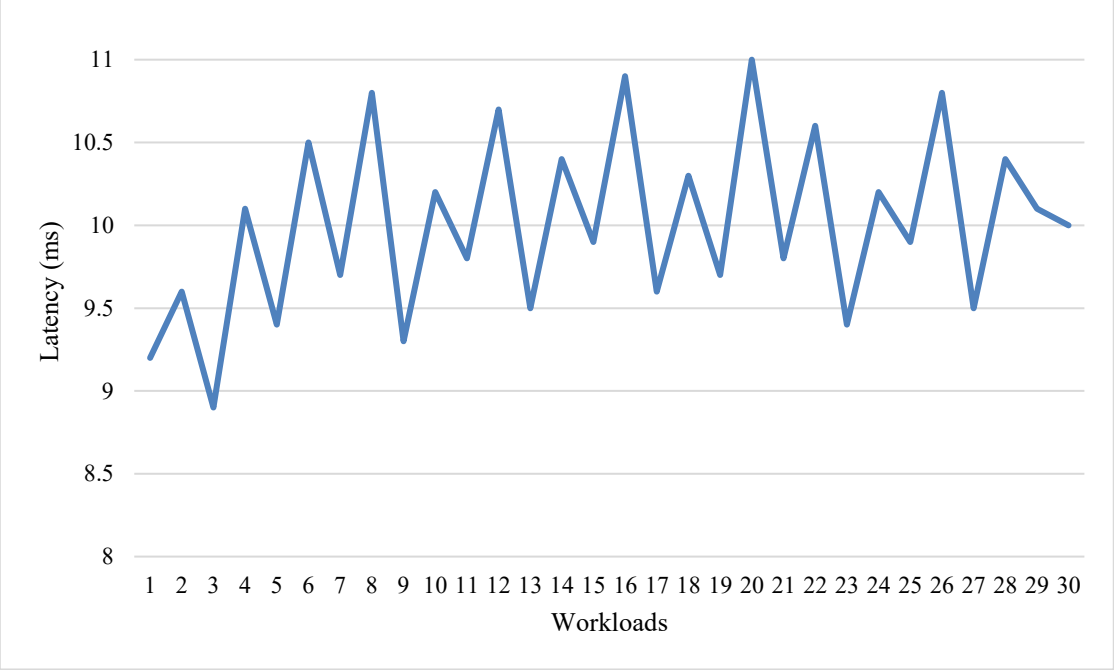


Figure 4. Network Latency Fluctuations within Different Workload Levels

The fluctuations in network latency across 30 workload examples are demonstrated in Figure 4. The latency varies between approximately 8.9 and 11.0ms, mirroring variations in communication delay within several workload status. The observed changes represent the dynamic network nature associated with workload execution, while maintaining a relatively consistent latency range.

Earlier methodologies facilitate complementary vision on resource profiling, cloud–IoT management and cloud security in contrast to developed ISACRP model. Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection (LTPCID) was introduced (Wardana et al., 2024) for developing a lightweight, secure, trustworthy, and privacy-preserving collaborative intrusion detection system for diverse IoT ecosystems. Security Performance of Smart Metering Systems (SPSMS),

proposed (Zhu et al., 2026) that focused on enhancing security performance via big-data-based evaluation of intelligent metering systems. DIKWP-based artificial consciousness for IoT-enabled smart systems (DIKWP) was proposed (Duan & Guo, 2025) for IoT-enabled smart healthcare that allows adaptive, secure, explainable, and purpose-based decision-making. Integration and Innovation of Cloud Computing and the Internet of Things (IICC), formulated (Luo and Li, 2026) reveals the hybridization of cloud computing and IoT technologies for enterprise production and functional management. Comprehensively, these studies emphasize the relevance of integrated cloud environments, security, and resource profiling, while facilitating distinct base for indicating several functional characteristics.

Table 4. Comparative Analysis of Performance between Existing and ISACRP Models

Models	Precision (%)	F1-score (%)	Resource Utilization (%)	Profiling Accuracy (%)	Network Latency (ms)
LTPCID	97.55	97.67	95.3	97.36	33.6
SPSMS	95.1	94.6	97.8	94.6	12
DIKWP	95	95.5	52.5	97.5	50
IICC	90.78	89.3	78.91	92.5	71.76
ISACRP (Proposed)	98.7	98.75	32.6	98.8	10

The comparative analysis of the current and developed ISACRP models utilizing standard performance metrics such as precision, F1-score, resource utilization, profiling accuracy, and network latency as represented in Table 4. these metrics comprehensively record categorization quality, resource effectiveness, profiling efficiency, and communication performance.

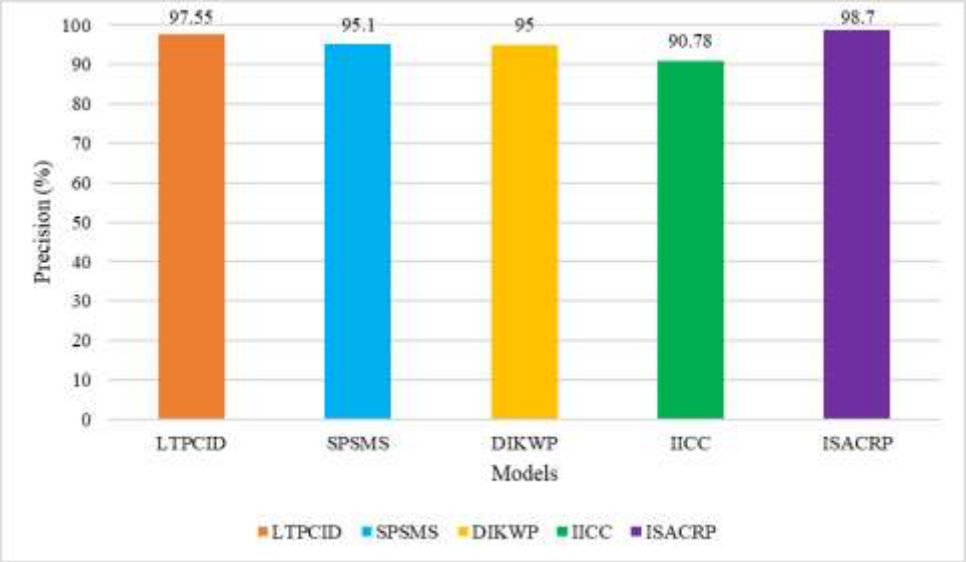


Figure 5. Comparative Analysis of Precision between Exiting and ISACRP Model

The comparative analysis of precision between existing and ISACRP model is visualized in Figure 5. Higher precision represents more reliable recognition f the intended security or resource conditions with fewer false-positive categorizations. The graphical representation underscores the fluctuations in precision throughout the considered methodologies.

Natural Resources for Human Health
eISSN: 2583-1194

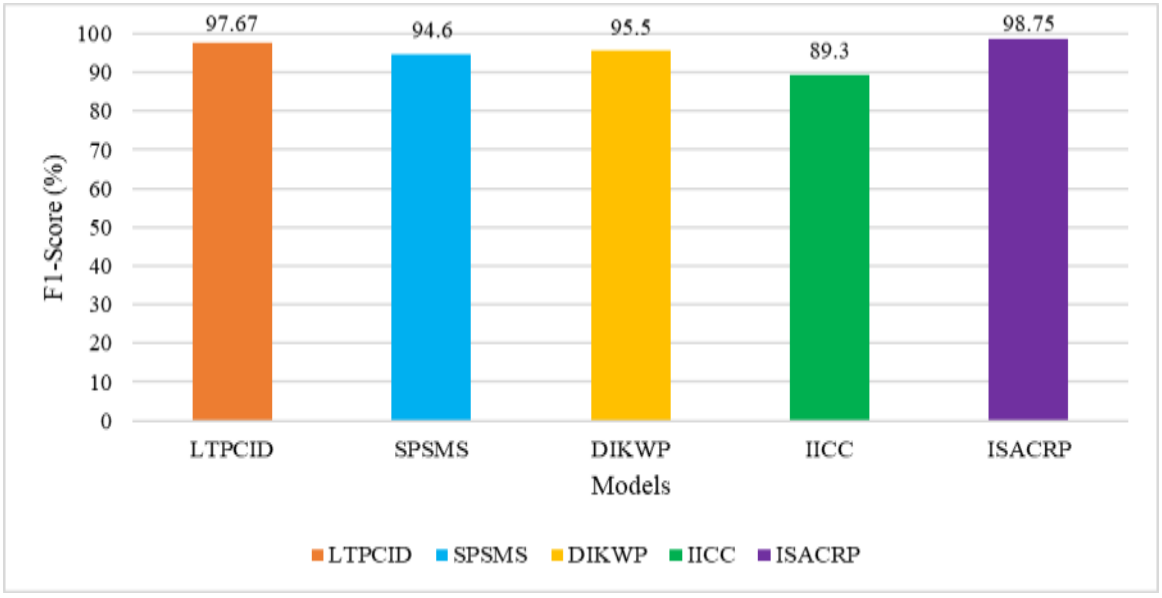


Figure 6. Comparative Analysis of F1-Score between Exiting and ISACRP Model

The comparative analysis of F1-score between existing and ISACRP model is visualized in Figure 6. the F1-score mirrors the balance between precision and recall, facilitating an overall representation of categorization efficiency. The graphical representation underscores the variation in F1-score throughout the considered methodologies.

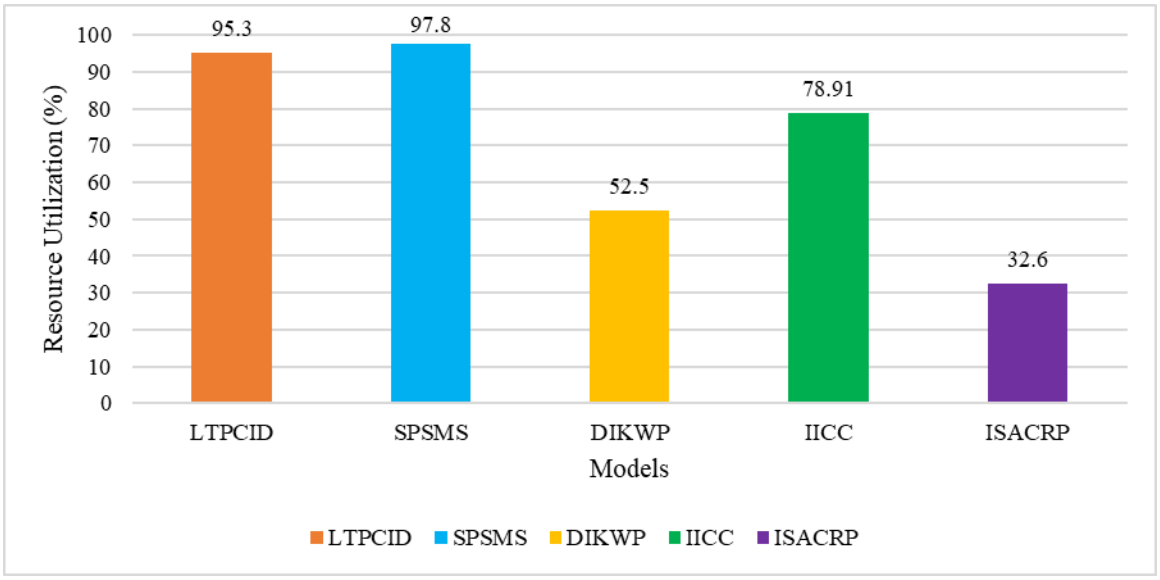


Figure 7. Comparative Analysis of Resource Utilization between Exiting and ISACRP Model

The comparative analysis of resource utilization between existing and ISACRP model is visualized in Figure 7. Resource usage is quantified by combining the usage of CPU, memory, storage, and bandwidth, thereby indicating the extent to which accessible framework resources are efficiently engaged at the time of workload execution.

Natural Resources for Human Health
eISSN: 2583-1194

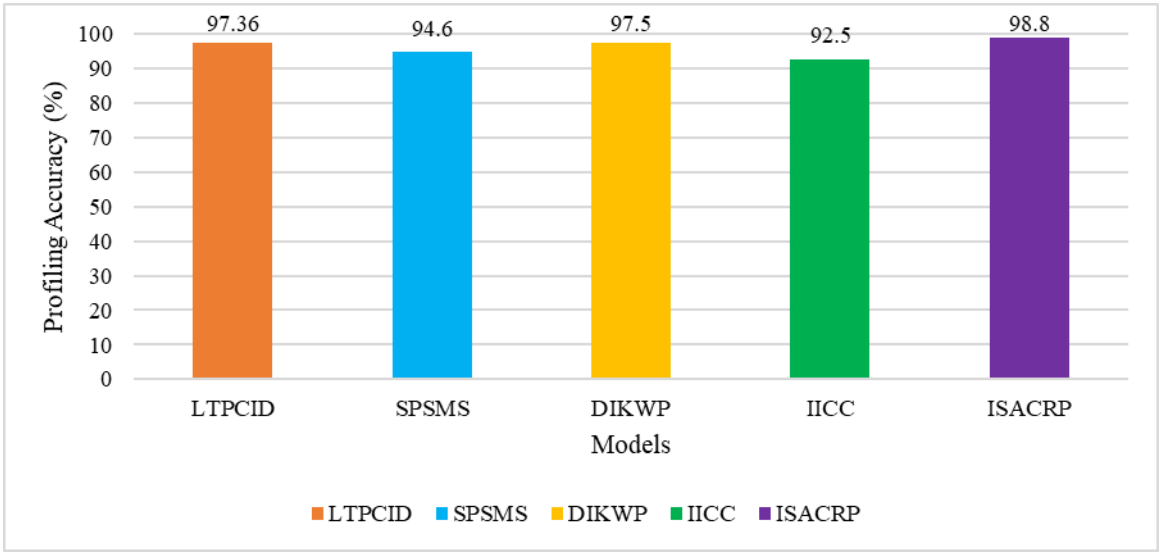


Figure 8. Comparative Analysis of Profiling Accuracy between Exiting and ISACRP Model

The comparative analysis of profiling accuracy between existing and ISACRP model is visualized in Figure 8. Profiling accuracy mirrors the correctness with which the functional characteristics and resource states of cloud attributes are recognized and indicated under their corresponding profiles.

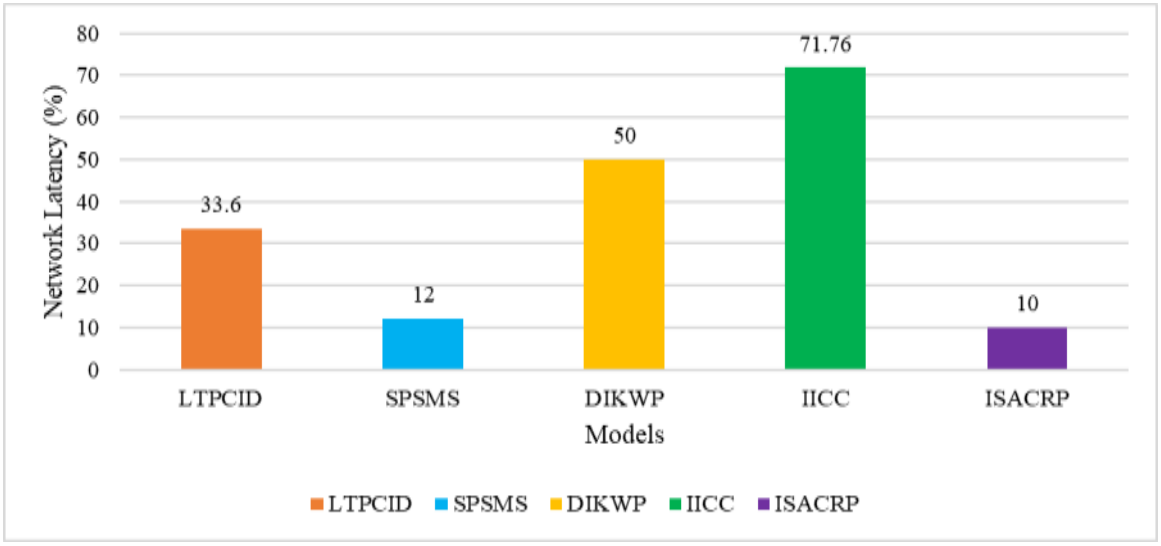


Figure 9. Comparative Analysis of Network Latency between Exiting and ISACRP Model

The comparative analysis of network latency between existing and ISACRP model is visualized in Figure 9. Network latency indicates the communication delay correlated with data transmission throughout the modelled network ecosystem and is defined in milliseconds (ms). The noted fluctuation among the analyzed models mirrors differences in communication effectiveness and responsiveness during workload execution, with lower latency representing decreased communication delay.

Overall, the proposed ISACRP architecture facilitates a hybridized methodology for modelling and profiling diverse cloud environments by integrating computational resources, network conditions, security characteristics, and workloads. The multi-level profiling of VMs, workloads, and physical hosts allows both functional resource conditions and security risks to be represented under a unified cloud profile. The analysis utilizing security classification and functional metrics illustrates the usability of the architecture for characterizing cloud resource conditions. The generated profile facilitates a systematic base for future smart resource allocation and security-aware orchestration.

5. CONCLUSION

The proposed ISACRP architecture resolves the challenges correlated with diverse cloud resources, network variability, adaptable workloads and security risks in virtualized cloud ecosystems. The developed ISACRP model introduced a simulated cloud framework utilizing CloudSim Plus, including diverse datacentres, physical hosts, resource configurations, and VMs. Network characteristic was modeled utilizing NS-3 to characterize latency, bandwidth accessibility, traffic nature, communication delay and congestion. Additionally, diverse workloads were evaluated as per their memory, bandwidth, computational, execution, priority, latency, and security essentials. A major contribution of the infrastructure is the combination of multi-level security profiling throughout workloads, physical hosts and VMs. Security-relevant characteristics, incorporating access nature, resource anomalies, communication trends, policy compliance, and security events, were included into the resource profiling procedures. The outcoming details was hybridized into a unified security-aware cloud profile comprising workload nature, host accessibility, network conditions, resource usage, security conditions, and risk classifications. The efficiency of the developed ISACRP architecture is analyzed utilizing accuracy, precision, recall, F1-score, resource utilization, profiling accuracy, and latency. the higher metrics value illustrates the performance of the developed profiling architecture. The outcoming security-aware cloud model facilitates a systematic base for consequent intelligent resource allotment and orchestration, where both resource accessibility and security status can be noted at the time of future cloud management decisions.

ACKNOWLEDGEMENTS

This is not applicable.

AUTHOR CONTRIBUTIONS

Veena Vijayan V K: responsible for conceptualizing the study and developing its methodology and carried out the data curation and implementation, performed the analysis, prepared the visualizations, and contributed to the preparation, writing, and editing of the manuscript.

Dr. Periyasami: provided research supervision and methodological guidance throughout the study and also contributed to the validation and interpretation of the results, guided the software implementation, and reviewed and edited the manuscript.

CONFLICT OF INTEREST

The authors have no conflicts of interest to declare.

ETHICS STATEMENT

Ethical approval was not required for this study.

DATA AVAILABILITY STATEMENT

Data supporting the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] Tuli, S., Casale, G., & Jennings, N. R. (2022). SimTune: Bridging the simulator reality gap for resource management in edge-cloud computing. *Scientific reports*, *12*(1), 19158.

[2] Luo, F., & Li, Z. (2026). Integration and Innovation of Cloud Computing and the Internet of Things in Enterprise Production and Operations Management. *Journal of Engineering, Project & Production Management*, *16*(1), 1.

[3] Dong, D. (2023). Agent-based cloud simulation model for resource management. *Journal of Cloud Computing*, *12*(1), 156.

[4] Gao, J., Feng, L., Yu, P., Zhou, F., Wu, Z., Qiu, X., ... & Zhu, Y. (2022). Resource consumption and security-aware multi-tenant service function chain deployment based on hypergraph matching. *Computer Networks*, *216*, 109298.

[5] Montazerin, F., & Shameli-Sendi, A. (2025). Enhancing virtual machine placement efficiency in cloud data centers through fluctuations-aware resource management. *Computers and Electrical Engineering*, *122*, 109885.

[6] Wang, D., Li, Y., Zhang, W., Yu, Z., Tian, Y. C., & Li, K. (2025). EVRM: Elastic Virtual Resource Management framework for cloud virtual instances. *Future Generation Computer Systems*, *165*, 107569.

[7] Zhu, J., Zhao, L., Wang, N., & Huang, Z. (2026). Improving the Security Performance of Smart Metering Systems Based on Big Data. *Procedia Computer Science*, *279*, 891-899.

[8] Bhonde, A., & Devane, S. R. (2024). Priority-based security-aware virtual machine allocation policy. *International Journal of Information and Computer Security*, *23*(1), 40-56.
[9] Souza, P. S., Ferreto, T., & Calheiros, R. N. (2023). EdgeSimPy: Python-based modeling and simulation of edge computing resource management policies. *Future Generation Computer Systems*, *148*, 446-459.
[10] Thabet, M., Berrima, M., & Hnich, B. (2023). A secure optimal placement strategy based on Monte Carlo simulation and hypothesis testing. *Future Generation Computer Systems*, *138*, 89-103.
[11] Ma, D., Cao, X., Hu, J., Xia, T., Zhou, Y., Liu, K., ... & Gao, F. (2026). Topology-aware virtual machine placement for improving cloud servers resource utilization. *Future Generation Computer Systems*, 108361.
[12] Hu, J., Liu, K., Zhang, Y., Sun, X., Zhai, Q., Cao, X., ... & Gao, F. (2025). A relax-and-round optimization algorithm for online NUMA-aware virtual machine placement. *Expert Systems with Applications*, *271*, 126653.
[13] Islam, A., & Ghose, M. (2026). MECSim: A comprehensive simulation platform for multi-access edge computing. *Journal of Systems Architecture*, 103706.
[14] Wardana, A. A., Kołaczek, G., & Sukarno, P. (2024). Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things. *Applied Sciences*, *14*(10), 4109.
[15] Duan, Y., & Guo, Z. (2025). DIKWP-driven artificial consciousness for IoT-enabled smart healthcare systems. *Applied Sciences*, *15*(15), 8508.