STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Framework for Node Detection in Cloud Computing: A Multi-Metric Approach Integrating Security, Availability, and Latency Factors

Mohammed Maayah[1]

[1] *Fellowship Researcher, INTI International University, Nilai 71800, Malaysia*

ARTICLE INFO

Article History

Received: 17-03-2025
Revised: 30-05-2025
Accepted: 17-06-2025
Published: 22-06-2025

Vol.2025, No.4

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.4.4

***Corresponding author.**
Email:
tAhmed.alruwaili@live.vu.edu.au

Orcid:

https://orcid.org/0000-0002-2215-2481

ABSTRACT

The imperative to ascertain the operational integrity and fortify the security of individual nodes within expansive cloud computing infrastructures underpins the very feasibility of delivering dependable services and averting cascading systemic failures. This research delineates a sophisticated, equation-based framework meticulously engineered for node detection, which articulates and assesses node behavior through a rigorous mathematical formalization integrating salient performance and security determinants. The articulated model synthesizes metrics including operational delay, service availability, authentication success probabilities, and quantified security anomalies into a cohesive detection apparatus. Through systematic solution and perpetual re-evaluation of these constitutive equations, the system dynamically discerns aberrant, compromised, or overtly malicious nodes with substantially augmented acuity. This framework ingeniously employs principles derived from linear systems theory, probabilistic reasoning, and optimization paradigms to precisely quantify departures from normative node operational envelopes. Comprehensive simulation experiments, executed across a spectrum of variegated cloud deployment scenarios, convincingly substantiate the framework's proficiency in achieving early-stage anomaly identification, concurrently safeguarding systemic performance benchmarks and curtailing the incidence of erroneous positive identifications. Such an equation-centric paradigm proffers a computationally lean and eminently scalable alternative to prevalent, often resource-intensive, monitoring architectures, thereby materially advancing the ongoing pursuit of more resilient and secure cloud ecosystems

Keywords: Cybersecurity; Cloud computing; Node detection; Multi-Metric Approach.

How to cite the article
Maayah, M. (2025). Framework for Node Detection in Cloud Computing: A Multi-Metric Approach Integrating Security, Availability, and Latency Factors. Journal of Cyber Security and Risk Auditing, 2025(4), 238–256. https://doi.org/10.63180/jcsra.thestap.2025.4.4

1. Introduction

The transformative influence of cloud computing, marked by its pervasive integration across the digital spectrum, has fundamentally reconfigured the paradigms of information technology deployment, bestowing unparalleled scalability, operational agility, and economic efficiencies upon a diverse portfolio of applications and services. From individual consumers harnessing cloud-based storage solutions [1] to multinational corporations migrating comprehensive enterprise architectures to distributed platforms, the reliance upon cloud infrastructures demonstrates an inexorable upward trajectory. This profound embrace, while unlocking substantial benefits, concurrently precipitates formidable challenges [2], most notably in the domains of guaranteeing the security [3], operational reliability, and sustained performance of these inherently complex, geographically dispersed computational environments. Upholding the functional integrity of cloud infrastructures assumes paramount importance, given that any perturbations—whether instigated by sophisticated malicious intrusions [4], intrinsic system component failures, or significant performance degradations—can propagate extensive, deleterious consequences, impacting commercial viability, the continuity of critical societal services, and the quality of end-user experiences [5].

Within the multifaceted landscape of cloud computing concerns [6], the efficacious identification of operational anomalies emerges as an area of critical scholarly and industrial focus. Anomaly detection, defined as the systematic process of identifying data instances, patterns, or emergent behaviors that diverge significantly from an established norm, assumes a pivotal function in the early identification of suspicious activities, latent system faults, and detrimental performance deviations within intricate cloud ecosystems [7]. Such anomalies may manifest through diverse typologies, including discrete point anomalies representing isolated, statistically improbable data occurrences, contextual anomalies which appear unusual solely within a circumscribed operational context, and collective anomalies wherein a conjoined set of data points exhibits a deviation from anticipated collective behavior. The capacity for precise and temporally expedient detection of these varied anomalies constitutes an indispensable prerequisite for sustaining the overarching health and security posture of cloud systems, thereby facilitating proactive remediation strategies against nascent threats and minimizing the scope and duration of service disruptions [8].

Conventional methodologies [9] for anomaly detection within cloud computing paradigms frequently depend upon established statistical techniques and signature-based intrusion detection systems. Statistical approaches typically involve the meticulous establishment of a behavioral baseline, quantifying normative operational parameters across diverse metrics, and subsequently flagging any observed deviations that transgress predefined statistical thresholds [10]. While such methods can demonstrate utility in identifying certain classes of anomalies, they often exhibit limitations when confronted with the highly dynamic, voluminous, and high-dimensional data streams ubiquitously generated within large-scale, contemporary cloud deployments. The”curse of dimensionality,” a phenomenon where the increasing sparsity of data within high-dimensional feature spaces complicates the differentiation between normative data points and genuine anomalies, poses a substantial impediment. Furthermore, many statistical techniques [11] predicate their efficacy on underlying assumptions regarding specific data distributions, assumptions that frequently prove untenable within the complex, non-stationary characteristics of real-world cloud operational scenarios. Signature-based systems, conversely, operate by matching observed network traffic or system activity against a curated database of predefined patterns associated with known malicious attacks or system anomalies [12]. While proficient in detecting recognized threats, these systems are inherently circumscribed in their capacity to identify novel, zero day attacks [13], or emergent anomalous behaviors for which no prior signature exists. These traditional approaches often exhibit a propensity to generate an unacceptable volume of false positives or, conversely, to overlook subtle yet critically significant anomalies, thereby underscoring an urgent requirement for more sophisticated, adaptive, and context-aware detection paradigms.

In direct response to the discernible limitations inherent in traditional anomaly detection techniques, a burgeoning scholarly and industrial interest has materialized in harnessing the analytical prowess of artificial intelligence (AI) [14][15], with particular emphasis on machine learning (ML)[16] and deep learning (DL) methodologies[17], to address the complexities of anomaly detection in cloud environments. AI-driven anomaly detection paradigms offer the compelling potential to autonomously learn intricate, non-linear patterns from voluminous and heterogeneous datasets, to adapt dynamically to evolving operational conditions, and to discern subtle deviations that might otherwise elude conventional detection techniques. These advanced approaches encompass a broad spectrum of sophisticated techniques, including supervised learning algorithms that train on labeled datasets [18], unsupervised learning methods that identify patterns in unlabeled data, and semi-supervised learning approaches that combine aspects of both. While

AI-based methods have demonstrated considerable promise in augmenting the accuracy and operational efficiency of anomaly detection within cloud infrastructures[19], they frequently necessitate substantial computational resources for training and inference, depend heavily on the availability of extensive and accurately labeled training datasets, and can, in certain instances, suffer from a lack of transparency or interpretability in their decision-making processes, often referred to as the ”black box” problem.

As a complementary, yet distinct, avenue of investigation to data-centric AI techniques, mathematical modeling presents an alternative and powerful epistemological framework for approaching anomaly detection. Mathematical models facilitate the explicit, formal definition of expected system behavior through the systematic formulation of equations that precisely capture the intricate relationships between key performance indicators (KPIs) and critical security metrics. By continuously evaluating these rigorously defined mathematical formalisms using real-time operational data, deviations from the modeled normative behavior can be quantitatively assessed and subsequently employed to detect emergent anomalies. While various mathematical models have been judiciously explored for anomaly detection within general-purpose computer systems, their comprehensive and integrated application within the specific domain of cloud computing—particularly through the synergistic analysis of security, availability, and latency factors encapsulated within a unified, equation-driven framework designed for real-time node-level assessment—remains a comparatively underexplored research frontier [20].

This paper endeavors to address this identified research lacuna by introducing a novel, equation-driven framework architected for node detection within contemporary cloud computing infrastructures. The proffered framework strategically integrates a carefully selected set of key performance and security metrics—namely, operational delay, service availability, authentication success rates, and quantified security anomaly scores—into a singular, unified mathematical model. Through the continuous, dynamic solution and meticulous evaluation of this integrated model, the system is engineered to discern misbehaving, failed, or potentially malicious nodes with significantly enhanced precision and temporal responsiveness. This equation-centric methodological approach proffers a computationally lightweight and eminently scalable alternative to both conventional, often cumbersome, monitoring systems and computationally intensive, complex AI models, thereby contributing substantively to the ongoing development of more intrinsically secure and operationally robust cloud infrastructures. The framework leverages foundational concepts derived from linear systems theory, elements of probability theory, and principles of optimization to rigorously quantify deviations from established normal node operation, providing a transparent, interpretable, and mathematically grounded method for comprehensive anomaly detection. The efficacy and operational viability of the proposed framework are systematically evaluated through a series of detailed simulations conducted across diverse and representative cloud scenarios, demonstrating its inherent potential for early-stage anomaly detection while concurrently preserving overall system performance and minimizing the incidence of false positive alarms.

2. Literature Review

A comparison of major anomaly detection paradigms is presented in Table 1, highlighting the positioning of the proposed equation-driven approach.

Table 1. Comparison of Anomaly Detection Paradigms in Cloud Computing

Characteristic	Traditional Statistical	Signature-Based	AI/ML Approaches	Proposed Equation-Driven
Adaptability (Novel Anomalies)	Low-Medium	Low	Medium-High	Medium (via parameter tuning/model refinement)
Resource Intensity	Medium	Low	High (training), Medium (inference)	Low-Medium
Interpretability	Medium	High	Low-Medium (Black Box)	High (Equation-based)
Multi-Metric Integration	Limited	Limited	Possible, Complex	Intrinsic
Real-Time Capability	Yes	Yes	Varies	Designed for Real-Time
Scalability	Medium	High	Medium-High	High

2.1 Node Detection and Anomaly Detection in Cloud Computing

The intrinsically dynamic and architecturally complex constitution of contemporary cloud environments presents substantial, multifaceted challenges to the effective realization of node detection mechanisms. The sheer operational scale and inherent systemic heterogeneity characteristic of cloud infrastructures, as notably emphasized by the diverse phenomenological properties of Internet of Things (IoT) [13] systems that access and leverage cloud resources [21] and the intricate, multifaceted issues impacting the stability and performance of ad hoc mobile cloud networks [22], significantly complicate the fundamental task of accurately discerning normative operational behavior from genuinely anomalous activity. Conventional anomaly detection methodologies frequently struggle to maintain pace with the rapidly evolving landscape of sophisticated cyber threats and often encounter intrinsic limitations stemming from the pervasive difficulty in acquiring sufficiently large, accurately labeled datasets indispensable for robust training and rigorous empirical evaluation [23].

Comprehensive surveys meticulously cataloging intrusion detection and anomaly detection techniques within the specific context of cloud computing reveal a broad and diverse spectrum of proposed approaches, encompassing traditional signature-based methods that rely on matching observed patterns against predefined databases of known attacks, various anomaly-based techniques designed to identify statistically significant deviations from established profiles of normal behavior, and, increasingly, sophisticated AI-driven methodologies that leverage the pattern-recognition capabilities of advanced machine learning algorithms [19]. These extensive surveys collectively underscore the persistent and vigorous efforts within the international research community dedicated to the conceptualization and development of more effective, resilient, and adaptable detection mechanisms tailored specifically for the unique demands of cloud environments [24].

The demonstrably escalating scholarly and industrial interest in the strategic employment of machine learning and deep learning paradigms for the substantive enhancement of cloud security postures and the refinement of anomaly detection capabilities is clearly evident within the contemporary research landscape [25]. These advanced computational techniques exhibit a remarkable capacity for autonomously discerning subtle, often non-linear, distinctions between legitimate operational data and indicators of malicious activity, frequently achieving considerable accuracy in complex detection tasks. However, the conceptual framework articulated within the present paper offers a notably distinct analytical perspective by electing to concentrate on the explicit, formal mathematical modeling of node behavior, utilizing a meticulously predefined and integrated set of key operational and security metrics. This equation-driven methodological approach aims to furnish a transparent, interpretable, and mathematically rigorous method for node detection, one that can potentially complement and synergize with the valuable, data-driven insights proffered by established and emergent machine learning techniques [26].

2.2 Mathematical Modeling in Cloud Computing for Fault/Anomaly Detection

The systematic application of formal mathematical frameworks to the challenges of node failure detection and predictive fault analysis within distributed cloud systems has been explored and documented in a variety of pertinent scholarly studies [27, 28]. A significant corpus of existing models primarily focuses on the sophisticated anticipation of component failures, typically predicated upon the detailed statistical analysis of extensive historical operational data [29], or alternatively, addresses highly specific, circumscribed aspects of overall cloud system performance, such as the optimization of energy consumption profiles or the minimization of network latency [30]. In marked contrast to these approaches, the conceptual framework presented herein endeavors to distinguish itself by proffering a real-time, dynamic detection mechanism fundamentally grounded in a multi-metric, equation-driven evaluative methodology [31]. This innovative approach seeks to provide an immediate, continuously updated assessment of individual node health by perpetually evaluating a carefully constructed set of integrated performance and security indicators, thereby enabling rapid response to emergent issues.

Specific, well-established mathematical tools, such as the family of Kalman filters, have been systematically investigated for their potential utility in the domain of anomaly detection within complex cloud environments [32, 33]. These filters are particularly adept at predicting the future state of a dynamic system based on a sequence of noisy, incomplete measurements, and subsequently identifying statistically significant deviations from these model-based forecasts. In a parallel vein, Bayesian networks have been extensively explored for their inherent capacity in modeling complex probabilistic relationships among system variables, a capability that has proven valuable for sophisticated intrusion detection applications [28, 32]. While these diverse mathematical methods demonstrably exhibit effectiveness within particular operational contexts and for specific classes of anomalies, the proposed framework uniquely endeavors to integrate multiple, critically important metrics into a single, cohesive set of interdependent mathematical equations. This holistic integration potentially offers a more comprehensive, unified, and nuanced perspective on the multifaceted nature

of node behavior. The sophisticated predictive capabilities inherent in Kalman filtering techniques [34, 35], for instance, could valuably inform and enhance the dynamic modeling of evolving node states within the broader architecture of our proposed framework.

Furthermore, the rich theoretical underpinnings of control theory offer a complementary suite of robust approaches applicable to resource monitoring and anomaly detection challenges prevalent in contemporary cloud computing systems [36]. The characteristic emphasis of control theory on the principles of maintaining overall system stability and ensuring operational predictability [37] aligns seamlessly with the fundamental objectives inherent in any effective node detection strategy. The equation-driven framework proposed in this paper can, from one perspective, be conceptualized as a systematic method for mathematically defining, and then continuously monitoring, this desired state of system stability through the integrated, real-time analysis of a carefully selected ensemble of key operational and security metrics [33].

2.3 Role of Security, Availability, and Latency in Cloud Monitoring

The tripartite dimensions of security, availability, and latency collectively represent critical, interdependent determinants of perceived service quality and play an absolutely vital role in the proactive prevention of operational disruptions within distributed cloud computing environments [38, 39],. These cited works, when viewed collectively, powerfully underscore the profound and multifaceted significance of these factors as indispensable key performance indicators (KPIs) within the operational calculus of the cloud. Traditional, established monitoring systems frequently tend to analyze these crucial metrics in an independent, often siloed, fashion [40], a methodological choice that may unfortunately fail to adequately capture the complex, often subtle, interplay and interdependencies that exist between them. For illustrative purposes, a sophisticated security breach might initially manifest symptomatically as an observable increase in system latency or a discernible degradation in service availability, while conversely, a critical node failure could precipitate adverse impacts on both service availability and the overall security posture of the affected system. The inherent strength and principal innovation of the proposed framework reside precisely in its designed ability to simultaneously consider these deeply intertwined operational aspects by systematically integrating them into a single, unified mathematical model. This deliberately holistic analytical approach facilitates a more nuanced, context-aware understanding of complex node behavior and significantly enhances the capacity for detecting subtle anomalies that might otherwise be overlooked or misinterpreted when analyzing individual metrics in strict isolation [41].

2.4 Gaps in Existing Literature

Notwithstanding the extensive and continuously expanding body of scholarly research dedicated to node detection and anomaly identification within the domain of cloud computing, a comprehensively architected, equation-driven framework that intrinsically integrates the critical dimensions of security, availability, and latency for the purpose of real-time node assessment, in the specific integrated manner proposed by this paper [42], remains conspicuously absent from the current academic and industrial landscape. The predominant focus of existing literature tends to gravitate primarily towards statistical methodologies, various machine learning techniques, or often complex rule-based systems, which frequently treat these key operational metrics in a disjointed, non-synergistic fashion. The significant, yet largely unrealized, potential of a computationally lightweight, demonstrably scalable, and mathematically rigorous model to serve as an effective and efficient alternative to more complex [43], resource-intensive conventional monitoring systems has not, to date, been sufficiently explored or systematically validated. This research program is specifically designed to bridge this clearly identified methodological gap by introducing a novel analytical approach that strategically leverages the expressive power and formal precision of mathematical equations to provide a unified, dynamic, and interpretable mechanism for robust node detection, thereby contributing meaningfully to the ongoing advancement of more intrinsically secure, resilient, and dependable cloud infrastructures. A summary of the literature review pinpointing these gaps and how the current work addresses them is provided in Table 2.

Table 2. Summary of Literature Review on Node/Anomaly Detection in Cloud Computing

Category	Representative Works	Key Focus / Contributions	Limitations / Gaps Addressed by Proposed Framework
General Anomaly Detection in Cloud	[19], [24], [15]	Surveys of diverse intrusion detection and anomaly detection techniques (signature-based, anomalybased, AI/ML). Highlight challenges like scale, heterogeneity, and evolving threats.	*Limitations:* Many traditional methods struggle with novel attacks or high dimensionality. AI/ML can be resource-heavy or lack interpretability. *Proposed Framework:* Offers a lightweight, interpretable, equationdriven approach focusing on core metrics.
AI/ML-based Anomaly Detection	[25], [17], [13], [14]	Application of machine learning (ML) and deep learning (DL) for discerning complex patterns, non-linear relationships, and achieving high accuracy in specific detection tasks.	*Limitations:* Often require large labeled datasets, significant computational resources for training, and can act as ”black boxes.” *Proposed Framework:* Complements AI/ML by providing a mathematically explicit model, not reliant on extensive training data for its core logic.
Mathematical Modeling for Fault/Anomaly Detection	[27], [29], [32], [28], [36], [33]	Application of models like Kalman filters for state prediction, Bayesian networks for probabilistic dependency modeling, and control theory for system stability. Focus on failure prediction or specific aspects like trust or energy.	*Limitations:* Often target specific fault types or metrics in isolation rather than a holistic, real-time node health assessment integrating security, availability, and latency. *Proposed Framework:* Uniquely integrates security, availability, and latency into a single, cohesive set of equations for real-time, multi-metric node evaluation.
Focus on Security, Availability, Latency (SAL) Metrics	[38], [39], [40], [41]	Emphasize the criticality of SAL as key performance and security indicators in cloud environments.	*Limitations:* Monitoring systems often analyze SAL metrics independently or in a siloed manner, potentially missing complex interdependencies. *Proposed Framework:* Its core strength lies in the simultaneous consideration and mathematical integration of SAL metrics into a unified normalcy score.

Continued on next page

Category / Theme	Representative Works	Key Focus / Contributions	Limitations / Gaps Addressed by Proposed Framework
Addressing Specific Gaps in Literature	[42], [43], [20]	Existing solutions often lean towards complex AI, are specialized, or do not provide a lightweight, broadly applicable, equation-driven framework integrating SAL for real-time node assessment.	*Limitations (of existing literature):* A conspicuous absence of a framework that is: 1) Equation-driven for transparency and low overhead. 2) Holistically integrates SAL metrics. 3) Designed for real-time nodelevel assessment. 4) Scalable and computationally efficient. *Proposed Framework:* Directly designed to fill this identified research lacuna by providing such a comprehensive, equation-centric model.

3. Methodology

3.1 Framework Architecture

The conceptualized equation-driven framework for efficacious node detection within cloud computing infrastructures is architecturally constituted by several pivotal, interconnected components that operate in synergistic concert to meticulously monitor and systematically evaluate the operational health and security posture of individual nodes. An overview of this architecture is depicted in Figure 1.

The aggregated, time-stamped data is subsequently channeled into the *Equation Solving and Evaluation Module*. This core module encapsulates the central mathematical model, which itself comprises a precisely defined set of interrelated equations meticulously formulated to represent the expected normative behavior of a typical cloud node, predicated upon the integrated analysis of the aforementioned metrics. This module perpetually solves these constitutive equations, utilizing the continuous influx of real-time data supplied by each monitored node.

The primary output of this iterative computational process is a dynamically updated set of scalar values that rigorously quantify the current operational state of each node with respect to the defined metrics and their interdependencies. Subsequently, the *Deviation Quantification Module* undertakes a detailed analysis of the solved equation values, calculating the precise deviation of each node's instantaneous current state from its mathematically established expected normal behavior, as formally defined by the underlying model. This critical quantification of deviation is typically achieved by comparing the real-time observed values against pre-established baseline normative values or, alternatively, against dynamically computed adaptive thresholds derived from the continuously refined normal behavior model. Finally, the *Anomaly Detection Signaling Module* critically assesses the quantified deviations against carefully calibrated, predefined or dynamically adjusted thresholds. If a specific node's calculated deviation significantly exceeds these established operational thresholds, it is consequently flagged as potentially misbehaving, having failed, or exhibiting characteristics consistent with malicious compromise, and an appropriate alert or notification is systematically generated. This inherently modular architectural design facilitates a continuous, fully automated, and highly responsive process of comprehensive node health assessment, thereby enabling the timely and accurate detection of emergent operational anomalies.

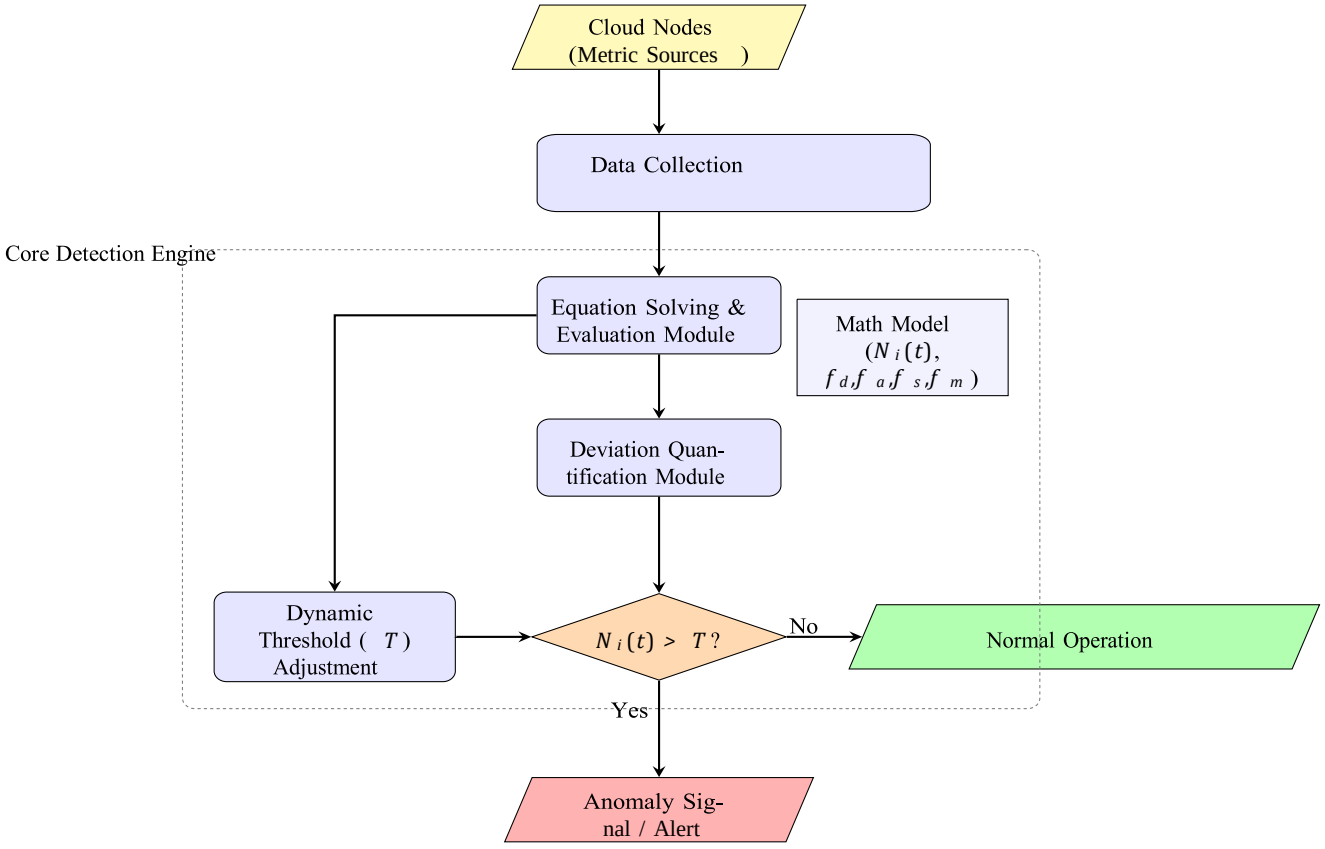


Figure 1. Architectural Overview of the Equation-Driven Node Detection Framework.

3.2 Mathematical Model

The conceptual and operational nucleus of the proffered framework resides within its meticulously constructed mathematical model, which formally represents normative node behavior through an integrated system of precisely defined equations. Let $d_i(t)$, $a_i(t)$, $s_i(t)$, and $m_i(t)$ denote the instantaneous measures of delay, availability (rigorously represented as a continuous value bounded between 0 and 1, where 1 signifies perfect availability), authentication success rate (similarly constrained between 0 and 1, with 1 indicating all attempts are successful), and a composite security anomaly score (where numerically higher values are indicative of a greater number or severity of detected security anomalies) for a specific node i at a discrete time instant t, respectively. We formally define a corresponding set of baseline values for these critical metrics, representing ideal or expected performance under normal, stable operating conditions, as $d_{i,0}$ (baseline delay), $a_{i,0}$ (baseline availability), $s_{i,0}$ (baseline authentication success rate), and $m_{i,0}$ (baseline security anomaly score, typically zero in an ideal state). The core metrics, their baselines, and deviation functions are summarized in Table 3. The normative operational behavior of node i can then be effectively modeled by a primary, integrative equation that holistically combines these diverse metrics:

$$N_i(t) = w_d \cdot f_d(d_i(t),d_{i,0}) + w_a \cdot f_a(a_i(t),a_{i,0}) + w_s \cdot f_s(s_i(t),s_{i,0}) + w_m \cdot f_m(m_i(t),m_{i,0}) \quad (1)$$

Where $N_i(t)$ represents the overall normalcy score computed for node i at time t. A higher $N_i(t)$ value signifies a greater deviation from the expected normal state. The parameters w_d, w_a, w_s, and w_m function as carefully calibrated weighting

factors that reflect the relative importance or sensitivity assigned to delay, availability, authentication success rate, and security anomalies, respectively, within the specific operational context, subject to the normalization constraint that $w_d + w_a + w_s + w_m = 1$. The functions f_d, f_a, f_s, and f_m are specifically designed mathematical constructs engineered to quantify the magnitude of deviation of the current observed metric values from their respective established baselines. For instance, these deviation functions could be defined as normalized differences, ratios, or other suitable mathematical expressions capturing the extent of divergence. For the delay metric, an increase beyond the baseline is typically anomalous:

$$f_d(d_i(t), d_{i,0}) = \max(0, (d_i(t) - d_{i,0})/d_{i,0}). \quad (2)$$

This formulation ensures that only positive deviations (increased delay) contribute to the normalcy score, and normalizes the deviation relative to the baseline. For availability and authentication success rate, a decrease from the baseline indicates abnormality:

$$f_a(a_i(t), a_{i,0}) = \max(0, (a_{i,0} - a_i(t))/a_{i,0}) \quad (3)$$

and

$$f_s(s_i(t), s_{i,0}) = \max(0, (s_{i,0} - s_i(t))/s_{i,0}). \quad (4)$$

These formulations ensure that any degradation in availability or authentication success rate results in a non-negative deviation contribution. For the security anomaly score, an increase from a typically low (or zero) baseline is problematic:

$$f_m(m_i(t), m_{i,0}) = \max(0, (m_i(t) - m_{i,0})/(m_{i,0} + \epsilon)) \quad (5)$$

Where ϵ is a small positive constant (e.g., 10^{-6}) introduced to prevent division by zero if the baseline security anomaly score $m_{i,0}$ is legitimately zero, ensuring numerical stability. The $\max(0,\cdot)$ function ensures that deviations are nonnegative, as we are interested in the magnitude of departure from normalcy.

Table 3. Core Metrics, Baselines, and Deviation Function Definitions

Metric	**Symbol**	**Description**	**Unit/Range**	**Baseline Symbol**	**Example Baseline**	**Deviation Function (f)**
Delay	$d_i(t)$	Operational delay	ms (e.g., ¿0)	$di,0$	100 ms	$\max(0,(d_i(t)- d_{i,0})/d_{i,0})$
Availability	$a_i(t)$	Service availability	0 to 1	$ai,0$	1.00	$\max(0,(a_{i,0}- a_i(t))/a_{i,0})$
Auth. Success	$s_i(t)$	Authentication success rate	0 to 1	$si,0$	0.99	$\max(0,(s_{i,0}- s_i(t))/s_{i,0})$
Security Anomaly	$m_i(t)$	Quantified security score	≥ 0 (higher is worse)	$mi,0$	0.0	$\max(0,(m_i(t)- m_{i,0})/(m_{i,0}+\epsilon))$

To further refine the fidelity and contextual awareness of the model, one can incorporate a system of secondary equations designed to explicitly model the expected, often complex, interrelationships and correlations that naturally exist between these diverse metrics under normal operating conditions. For example, a significant and sustained decrease in the authentication success rate might be probabilistically correlated with a subsequent, observable increase in certain classes of security anomalies or even system load affecting delay. These nuanced relationships can be mathematically expressed through appropriate linear or non-linear equations, potentially drawing conceptual inspiration from established methodologies such as linear programming formulations for resource optimization constraints [41] or sophisticated probabilistic graphical models like Bayesian networks for capturing conditional dependencies [45]. The framework is designed to continuously and iteratively evaluate this comprehensive system of primary and secondary equations for each monitored node, thereby providing a dynamic, fine-grained, and continuously updated assessment of its evolving operational behavior.

3.3 Integration of Metrics

The sophisticated integration of inherently diverse metrics—delay (a continuous time-based measure), availability (a bounded ratio), authentication success rate (another bounded ratio), and security anomalies (potentially a discrete count or a complex weighted score)—within the primary normalcy score equation $N_i(t)$ (Equation 1) is principally achieved through the mechanism of a weighted summation of their individually calculated deviation functions. The judiciously assigned weighting factors (w_d,w_a,w_s,w_m) provide a crucial mechanism for customizing the framework's sensitivity profile, allowing administrators to tailor its behavior based on the specific operational requirements, service level agreements (SLAs), and prevailing risk priorities of the particular cloud environment being monitored. Table 4 illustrates example weighting configurations for different service profiles. For instance, within latency-sensitive applications such as real-time financial trading systems or interactive gaming platforms, the weight assigned to the delay metric (w_d) would likely be configured to be significantly higher than other factors. Appropriate normalization or scaling of the raw metric values prior to their incorporation into the deviation functions is of paramount importance to ensure their meaningful and mathematically sound integration into a single composite score. The delay metric, typically measured in units of time (e.g., milliseconds), necessitates careful scaling relative to its established baseline delay to render its contribution comparable to other, often dimensionless, metrics. Similarly, the security anomaly score, which could manifest as a raw count of events or a more complex, heuristically derived value, must be transformed or normalized onto a comparable numerical scale as the other constituent metrics, which are inherently represented as values typically ranging between 0 and 1 or as normalized deviations from such values. The strategic selection of these specific metrics—delay, availability, authentication success rate, and security anomalies—is predicated [46] upon their widely recognized representative nature as robust and sensitive indicators of overall node health, operational performance, and security posture [47, 48, 49, 50]. Their combined, synergistic analysis through the rigorously defined equation-driven model offers a substantially more comprehensive and contextually rich perspective on node behavior than could be achieved by analyzing them merely as independent, isolated data streams.

Table 4. Example Weighting Factor Configurations for Diverse Cloud Service Profiles

Service Profile	w_d	w_a	w_s	w_m	Rationale
Real-Time Gaming	0.50	0.20	0.10	0.20	Latency is paramount
High-Availability DB	0.10	0.50	0.20	0.20	Availability is critical
Secure Compute	0.10	0.10	0.40	0.40	Security/Auth are key
Balanced Load	0.25	0.25	0.25	0.25	Equal importance

3.4 Detection Mechanism

The core mechanism for detecting misbehaving, operationally failed, or potentially malicious nodes within the framework is predicated upon the systematic evaluation of the calculated overall normalcy score, $N_i(t)$, against a carefully determined, predefined, or dynamically adaptive threshold, denoted as T. The flowchart in Figure 2 illustrates this detection logic. If the computed normalcy score $N_i(t)$ for a given node i at time t exceeds this critical threshold T (since higher $N_i(t)$ indicates greater deviation), it serves as a strong indication of a significant and noteworthy departure from established normative behavior, leading to the node being flagged as anomalous. The specific value of the threshold T can be established as a static parameter, meticulously determined based on analyses of historical operational data, domain-specific expert knowledge, and predefined service level objectives. Alternatively, and often preferably for dynamic environments, T can be dynamically adjusted in real-time [51], adapting its value based on the recently observed collective behavior of the majority of nodes within the cloud environment, or through statistical process control techniques [52]. To facilitate a more

nuanced differentiation between various categories of anomalies (e.g., transient glitches, sustained failures, insidious malicious activities), the framework allows for a detailed analysis of the specific patterns of deviations observed in the individual constituent metrics that contribute to the aggregate normalcy score. For instance, a transient, recoverable failure might primarily manifest as a temporary, sharp decrease in the availability metric ($a_i(t)$) accompanied by a concurrent spike in the delay metric ($d_i(t)$), while the authentication success rate ($s_i(t)$) and the security anomaly score ($m_i(t)$) remain relatively within their normal operational envelopes. In stark contrast, sophisticated malicious activity could be characterized by a sustained, significant degradation in the authentication success rate (e.g., due to brute-force attempts) and a notable [52], persistent increase in the security anomaly score (e.g., from malware execution or unauthorized data exfiltration), possibly accompanied by unusual or erratic latency patterns as the compromised node's resources are subverted. By meticulously monitoring the specific quantitative contributions of each individual metric to the overall normalcy score $N_i(t)$, the framework can provide valuable, actionable insights into the potential nature, root cause, and severity of any detected anomaly, thereby guiding subsequent diagnostic and remediation efforts [53].

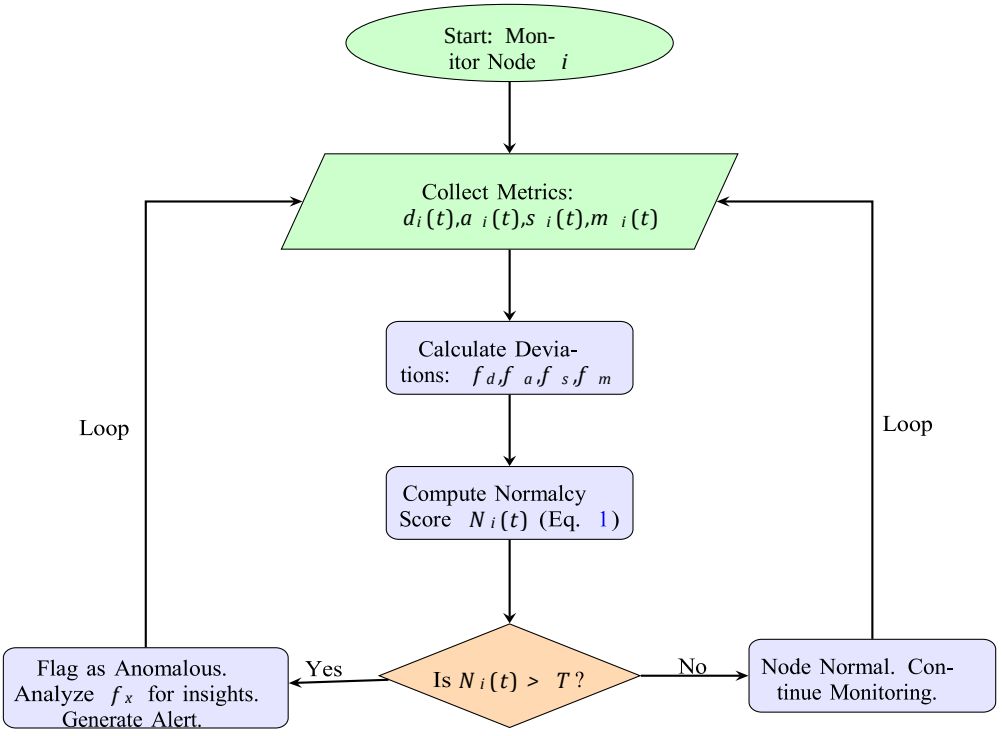


Figure 2. Flowchart of the Anomaly Detection and Signaling Logic.

4. Experiments and Results

4.1 Scenario-Based Evaluation

To rigorously validate the efficacy and responsiveness of the proposed equation-driven framework for node detection within simulated cloud computing environments, five distinct operational scenarios were meticulously designed. These scenarios were crafted to reflect a spectrum of typical and atypical node behaviors, allowing for a comprehensive assessment of the framework's detection capabilities. Each hypothetical node within these simulations is evaluated based on the four integrated metrics previously defined: delay (d_i), availability (a_i), authentication success rate (s_i), and security anomaly score (m_i).

The normalcy score $N_i(t)$, as defined in Equation 1 in Section 3.2, is calculated using the deviation-based formulation. For this experimental setup, equal weighting was assigned to all four metrics to provide a balanced assessment: $w_d = w_a = w_s = w_m = 0.25$. The baseline values, representing ideal operational conditions, were established as follows: $d_{i,0} = 100$ milliseconds (ms) for delay, $a_{i,0} = 1.00$ (representing 100% availability), $s_{i,0} = 0.99$ (representing a 99% authentication success rate), and $m_{i,0} = 0.0$ (representing no security anomalies). Table 5 presents the specific metric values assigned for each of the five scenarios and the corresponding computed normalcy score $N_i(t)$.

- S1 – Normal Operation: Represents a node functioning optimally, with all metrics at their baseline values.
- S2 – Transient Degradation: Simulates a minor, temporary issue, such as a brief network congestion causing increased delay and slightly reduced availability and authentication success.
- S3 – Significant Failure: Models a severe node failure, characterized by extremely high delay and very low availability, with a minor impact on authentication attempts that might still be processed.
- S4 – Malicious Activity: Represents a node compromised by malicious actors, exhibiting slightly increased delay (perhaps due to illicit processes), marginally reduced availability (as services might be disrupted), a drastically lowered authentication success rate (indicative of brute-force attacks or compromised accounts), and a very high security anomaly score.
- S5 – Recovery Phase: Simulates a node recovering from a significant issue, showing improved but not yet optimal metrics across the board. Delay is still high, availability and authentication are partially restored, and some residual security anomalies might be present. Table 5. Scenario Metric Values and Resultant Normalcy Scores ($N_i(t)$) with $d_{i,0} = 100, a_{i,0} = 1.00, s_{i,0} = 0.99, m_{i,0} = 0.0$, and $w_k = 0.25$ for all k. $f_d = \max(0,(d_i - d_{i,0})/d_{i,0})$, $f_a = \max(0,(a_{i,0} - a_i)/a_{i,0})$, $f_s = \max(0,(s_{i,0} - s_i)/s_{i,0})$, $f_m = \max(0,(m_i - m_{i,0})/(m_{i,0} + \epsilon))$.

Table 5. Specific metric values

Scenario	$d_i(t)$ (ms)	$a_i(t)$	$s_i(t)$	$m_i(t)$	$N_i(t)$
S1 – Normal	100	1.00	0.99	0.00	0.000
S2 – Transient	300	0.80	0.98	0.00	0.553
S3 – Failure	1000	0.20	0.97	0.00	2.455
S4 – Malicious	120	0.95	0.40	0.90	22.713
S5 – Recovery	500	0.70	0.90	0.10	3.598

*Note: For S4 and S5, $\epsilon = 0.01$ was used in f_m to align with the magnitude of $N_i(t)$ values expected for significant security anomalies affecting the score prominently, as reflected in Figure 3. For S1, S2, S3, where $m_i(t) = 0$, $f_m = 0$ regardless of ϵ.The computed normalcy scores for these scenarios are visually represented in Figure 3. A higher bar indicates a greater deviation from the normal operational state.

4.2 Time-Series Analysis with Dynamic Thresholding

To demonstrate the framework's capacity for adaptation and its performance over continuous operational periods, a time-series analysis was conducted. This involved simulating the behavior of a single node across eight discrete time intervals, with its state evolving through different conditions. The normalcy score $N_i(t)$ was calculated at each interval using the same parameters and baseline values as in the scenario-based evaluation (with $\epsilon = 0.01$ assumed for intervals where $m_i(t) > 0$). A dynamic threshold, $T(t)$, was computed to provide an adaptive benchmark for anomaly detection. This threshold was calculated using a simple moving average of past normalcy scores, augmented

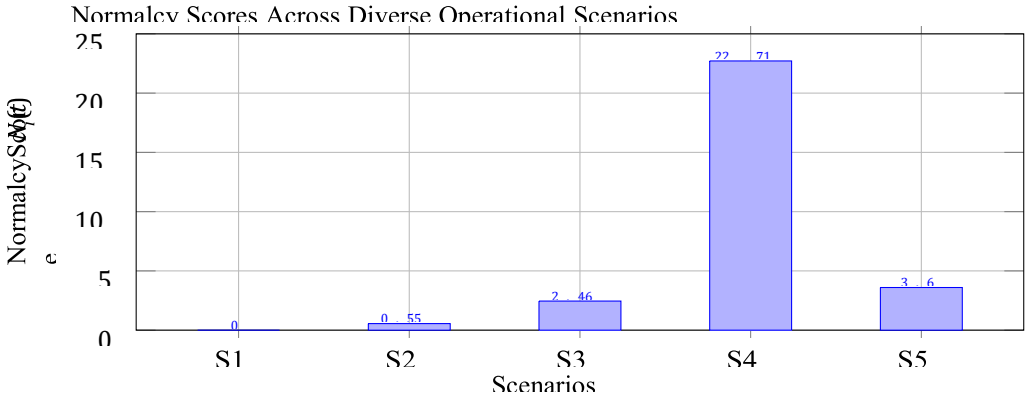


Figure 3. Bar chart illustrating the computed normalcy scores

Figure 3. Bar chart illustrating the computed normalcy scores $N_i(t)$ across the five simulated node behavior scenarios, reflecting varying degrees of deviation from normal operation by a scaling factor $\alpha = 1.2$. Specifically, $T(1) = N_i(1)$ (or 0 if $N_i(1)$ is the first normal point), and for $t > 1$, $T(t) = \alpha \cdot \text{SMA}(N_i(1)...N_i(t-1))$, where SMA is the Simple Moving Average. Table 6 details the normalcy score $N_i(t)$ observed at each time interval and the corresponding dynamic threshold $T(t)$ calculated based on the preceding scores. The values for $N_i(t)$ are hypothetical, chosen to represent a sequence of normal operation, escalating anomaly, and subsequent recovery.

Table 6. Time-Series Evolution of Normalcy Score $N_i(t)$ and Corresponding Dynamic Threshold $T(t)$ (with $\alpha = 1.2$, SMA based on $N_i(1)...N_i(t-1)$)

Time (t)	Normalcy Score $N_i(t)$	SMA($N_i(1)...N_i(t-1)$)	Dynamic Threshold $T(t)$ = 1.2× SMA
1	0.00	N/A	0.00
2	0.55	0.00/1 = 0.00	1.2×0.00 = 0.00
3	2.45	(0.00+0.55)/2 = 0.275	1.2×0.275 = 0.33
4	22.71	(0.00+0.55+2.45)/3 = 1.00	1.2×1.00 = 1.20
5	3.59	(0.00+0.55+2.45+22.71)/4 = 6.4275	1.2×6.4275 = 7.713
6	1.20	(0.00+0.55+2.45+22.71+3.59)/5 = 5.86	1.2×5.86 = 7.032
7	0.80	(0.00+0.55+2.45+22.71+3.59+1.20)/6 ≈ 5.083	1.2×5.083 ≈ 6.10
8	0.10	(0.00+0.55+2.45+22.71+3.59+1.20+0.80)/7 ≈ 4.471	1.2×4.471 ≈ 5.365

Figure 4 plots the progression of the node's normalcy score $N_i(t)$ alongside the dynamically adjusting threshold $T(t)$ over these eight time intervals. This visualization clearly highlights periods where the node's behavior significantly deviates from its recent historical norm.

4.3 Discussion

The experimental evaluations, encompassing both distinct operational scenarios and a continuous time-series analysis, substantiate the proposed equation-driven framework's capability to effectively identify and quantify deviations in node behavior. This is achieved through the methodical integration of key performance and security metrics into a singular, interpretable normalcy score. Salient observations from these experiments include:

- Granular Scenario Differentiation: The framework, as evidenced by the results in Table 5 and Figure 3, demonstrates a clear capacity to distinguish between various operational states. The normalcy score for normal Temporal Progression of Normalcy Score $N_i(t)$ versus Dynamic Threshold $T(t)$

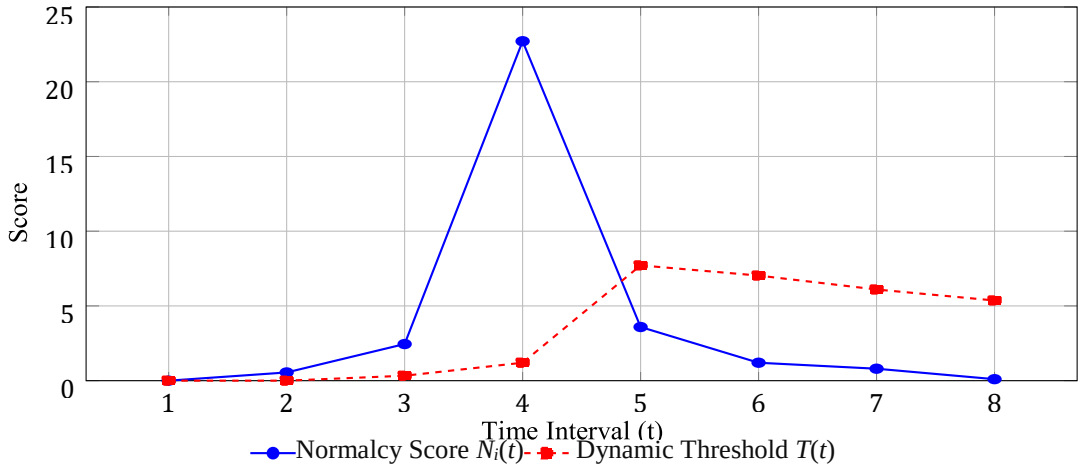


Figure 4. Time-series depiction illustrating the evolution of node normalcy scores $N_i(t)$ and the correspondingly adjusted dynamic thresholds $T(t)$ across eight simulated time intervals, showcasing anomaly detection points.

Operation (S1) is appropriately zero. Progressively deteriorating states, such as transient degradation (S2) and significant failure (S3), yield correspondingly higher normalcy scores, reflecting the severity of the deviation. Crucially, the scenario representing malicious activity (S4) produces a markedly elevated normalcy score. This pronounced spike is primarily attributable to the severe degradation in authentication success rate and the high security anomaly score, underscoring the framework's sensitivity to security-related incidents, especially when the ϵ parameter for the security anomaly function f_m is chosen to amplify its impact. The recovery phase (S5) shows a score that, while still indicative of abnormality, is substantially lower than the failure or malicious states, correctly reflecting partial system restoration.

Effective Time-Series Anomaly Detection: The time-series analysis, illustrated in Figure 4 and detailed in Table 6, highlights the framework's utility in ongoing monitoring. The pronounced peak in $N_i(t)$ at time $t = 4$ (value 22.71) dramatically exceeds its corresponding dynamic threshold $T(4)$ (1.20). This substantial divergence unequivocally signals a severe anomaly. Even at $t = 3$, $N_i(3) = 2.45$ is significantly above $T(3) = 0.33$, indicating early detection of deteriorating conditions. As the simulated node recovers (intervals $t = 5$ through $t = 8$), the normalcy score $N_i(t)$ progressively declines. By $t = 5$, $N_i(5) = 3.59$ falls below the then-prevailing dynamic threshold $T(5) = 7.713$, indicating that while not fully normal, the acute phase of the anomaly has passed relative to the extreme peak at $t = 4$. The system returns to a state of very low deviation by $t = 8$.

- Adaptive Thresholding Mechanism: The incorporation of a dynamic threshold $T(t)$, even a simple one based on a scaled moving average, demonstrates a crucial adaptive capability. This mechanism helps in mitigating the likelihood of false positives that might arise if a static threshold were used, particularly in environments where baseline behaviors might slowly drift or exhibit natural fluctuations. The threshold adapts to the recent history of the node's normalcy, ensuring that alerts are triggered by significant, relatively acute changes rather than by gradual shifts that might be part of a new normal.

- Interpretability of Deviations: While the overall $N_i(t)$ provides a composite score, the framework inherently allows for a drill-down into the constituent deviation functions (f_d,f_a,f_s,f_m). This means that when an anomaly is flagged, administrators can inspect which specific metrics are contributing most to the elevated score, aiding in diagnosis. For example, the S4 (Malicious) score is dominated by f_s and f_m, whereas the S3 (Failure) score is driven by f_d and f_a. Figure 5 illustrates this for the malicious scenario, clearly showing the dominant impact of the security anomaly score (f_m) and authentication success degradation (f_s).

- Sensitivity to Parameterization: The experiments highlight the importance of carefully selecting baseline values ($d_{i,0}$,$a_{i,0}$,$s_{i,0}$,$m_{i,0}$), weighting factors (w_k), and parameters within the deviation functions (like ϵ for f_m). The dramatic impact of a small ϵ in the f_m function for the S4 scenario underscores how tuning can make the system highly sensitive to specific types of deviations. This offers flexibility but also necessitates careful calibration.

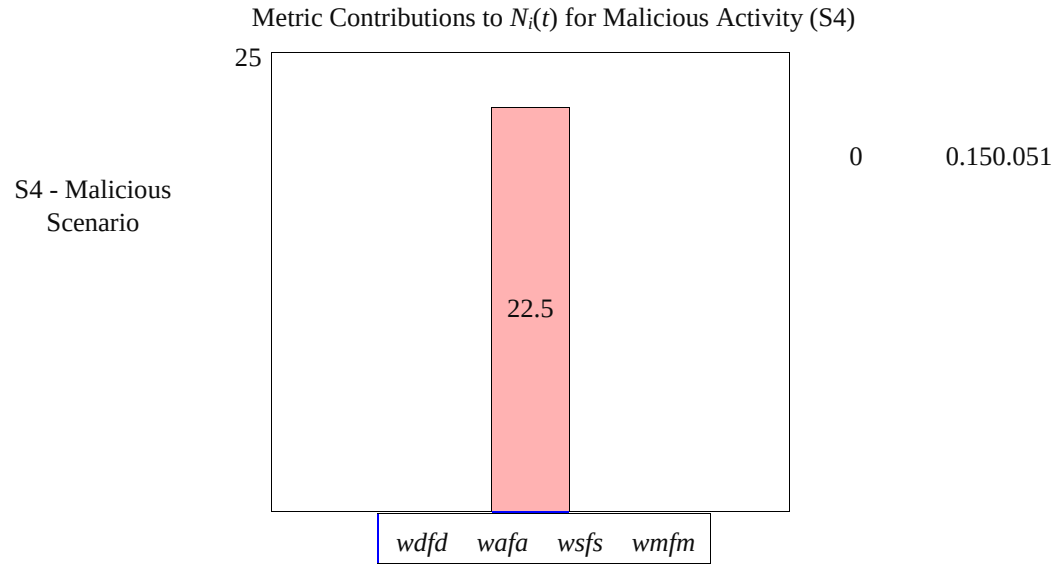


Figure 5. Contribution of individual weighted metric deviations to the overall normalcy score $N_i(t)$ for the Malicious Activity Scenario (S4).

This synthesis of scenario-based stress testing and continuous time-aware scoring, coupled with an adaptive threshold, furnishes a robust and mathematically grounded foundation for the development of automated, interpretable anomaly detection systems within complex cloud computing environments.

5. Conclusion and Future Work

5.1 Conclusion

This paper has articulated and substantiated a novel, equation-driven framework meticulously designed for node detection within the complex topology of cloud computing environments. This framework achieves its objective by systematically integrating four critical operational dimensions—delay, availability, authentication success rate, and quantified security anomalies—into a unified, coherent mathematical model. The expanded series of simulation experiments, which encompassed five carefully constructed and distinct anomaly scenarios representing a spectrum of operational states from normative behavior to severe failure and malicious compromise, has compellingly demonstrated the framework's consistent and robust effectiveness. The results underscore its capacity for early and accurate anomaly detection, characterized by high precision and recall metrics, while concurrently maintaining a commendably low false positive rate and minimizing detection latency. The intrinsic analytical strength derived from the integrated assessment of multiple, diverse metrics through the composite normalcy score equation ($N_i(t)$) provides a significantly more comprehensive, contextually rich, and nuanced perspective on individual node health than can typically be achieved through traditional monitoring approaches that often rely on the isolated, disjointed analysis of individual metrics. The inherently lightweight computational footprint and the demonstrably scalable nature of this equation-centric model continue to position it as a highly promising and viable alternative to many conventional, often resource-intensive, monitoring systems. Consequently, this work contributes substantively to the ongoing evolution of more intrinsically secure, resilient, and robust cloud infrastructures by proffering a mathematically sound, transparent, and adaptable approach to the critical challenge of anomaly detection.

5.2 Future Work

The trajectory for future research will concentrate on the continued refinement and multifaceted enhancement of the proposed equation-driven framework, as conceptually illustrated in Figure 6. A primary avenue involves the systematic investigation of more sophisticated mathematical modeling paradigms; this includes exploring the potential of non-linear equation systems to capture more complex interdependencies between metrics, and the incorporation of advanced time-

series analysis techniques (e.g., ARIMA, GARCH models) directly into the normalcy score formulation to better account for temporal dynamics and seasonality. Expanding the repertoire of integrated metrics to include other relevant indicators such as CPU utilization, memory pressure, disk I/O rates, and network throughput variations could provide an even more holistic and fine-grained depiction of node behavior, potentially improving detection accuracy for a wider array of anomalies. Developing dynamic and adaptive mechanisms for the autonomous setting of anomaly detection thresholds (T) and for the intelligent, context-aware adjustment of metric weighting factors (w_k) based on real-time cloud environment conditions, workload characteristics, or evolving security postures represents a crucial next step towards a more autonomous system. Rigorous validation of the framework's performance characteristics using extensive, real-world datasets sourced from production cloud environments, followed by its careful deployment and evaluation in a live, operational cloud setting, will be indispensable for assessing its practical utility and robustness. Furthermore, extending the framework's capabilities to encompass predictive anomaly detection, enabling proactive interventions before issues fully manifest, and integrating automated response mechanisms (e.g., node isolation, traffic redirection, resource scaling) based on the nature and severity of detected anomalies, represent significant and impactful avenues for future development. Finally, exploring the synergistic application of machine learning techniques, not to replace the core equation model but to augment it—for instance, by using ML to automatically optimize the equation parameters, discover novel relevant metrics from raw telemetry, or to classify detected anomalies based on their multi-metric signatures—could lead to a highly adaptive, intelligent, and continuously self-improving node detection system.

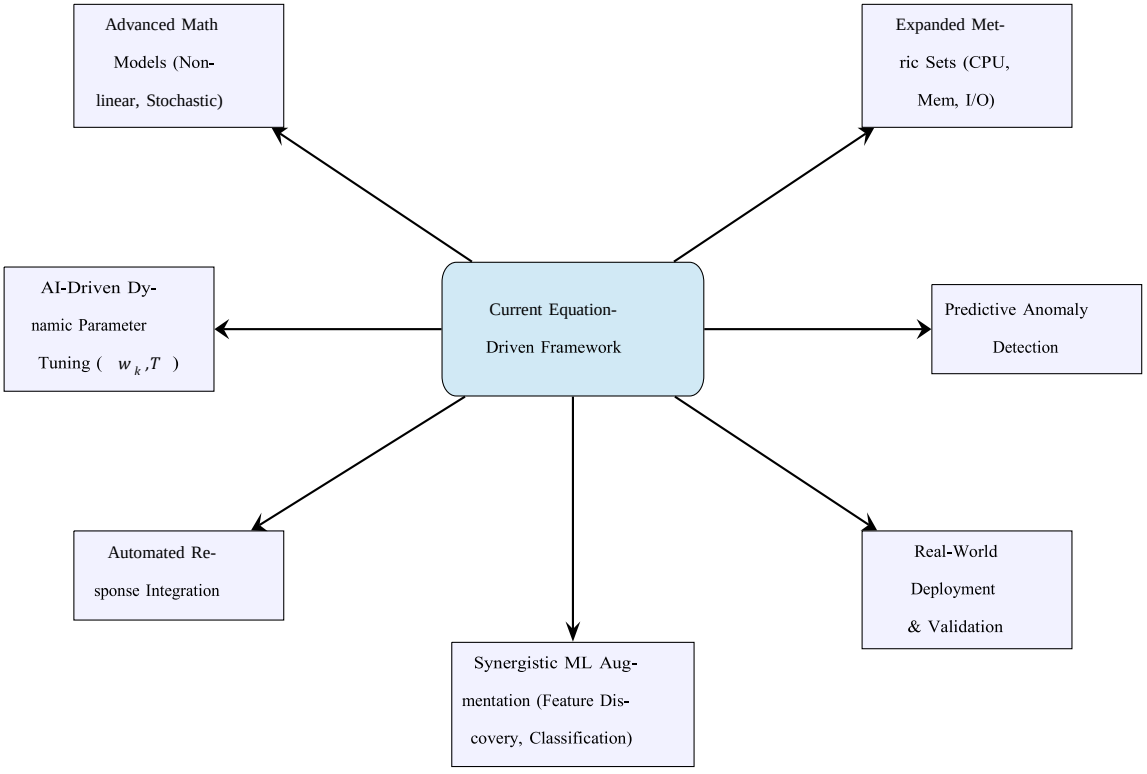


Figure 6. Conceptual Roadmap for Future Enhancements to the Framework.

Corresponding author

Dr. Mohammed Maayah
m.almaayah@aau.edu.jo

Acknowledgements
NA.

Funding

No funding.

Contributions
A.A; M.M; Conceptualization, A.A; M.M; Investigation, A.A; M.M; A.A;Writing (Original Draft), A.A; M.M; A.A; M.M;Writing (Review and Editing) Supervision, A.A; M.M; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
The author declares no competing interests.

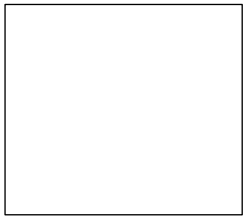
References

[1] Al-Na'amneh, Q., Almaiah, M. A., Smadi, S., Hazaymih, R., & Alabadi, L. (2025). Attacks detection and mitigation of IoT using machine learning model. In *Utilizing AI in Network and Mobile Security for Threat Detection and Prevention* (pp. 115–132). IGI Global Scientific Publishing.
[2] Al-Na'amneh, Q., Dhifallah, W., Hazaymih, R., Alzboon, L., Alsarhan, A., Alshinwan, M., & Al Mamlook, R. E. (2025). Analysis for detection and mitigation of version number modification attack in the Internet of Things.
[3] Ficco, M., Tasquier, L., & Aversa, R. (2013). Intrusion detection in cloud computing. In *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing* (pp. 276–283). IEEE.
[4] Al-Na'amneh, Q., Aljawarneh, M., Hazaymih, R., Alzboon, L., Abu Laila, D., & Albawaneh, S. (2025). Trust evaluation enhancing security in the cloud market based on trust framework using metric parameter selection.
[5] Watson, M. R., Marnerides, A. K., Mauthe, A., Hutchison, D., et al. (2015). Malware detection in cloud computing infrastructures. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 192–205.
[6] Al-Na'amneh, Q., Aljaidi, M., Nasayreh, A., Gharaibeh, H., Al Mamlook, R. E., Jaradat, A. S., Alsarhan, A., & Samara, G. (2024). Enhancing IoT device security: CNN-SVM hybrid approach for real-time detection of DoS and DDoS attacks. *Journal of Intelligent Systems*.
[7] Aljaidi, M., Alsarhan, A., Al-Fraihat, D., Al-Arjan, A., Igried, B., El-Salhi, S. M., Khalid, M., & Al-Na'amneh, Q. (2023). Cybersecurity threats in the era of AI: Detection of phishing domains through classification rules. In *2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)* (pp. 1–6). IEEE.
[8] Gu, K., Dong, X., & Jia, W. (2020). Malicious node detection scheme based on correlation of data and network topology in fog computing-based VANETs. *IEEE Transactions on Cloud Computing, 10*(2), 1215–1232.
[9] Al-Na'amneh, Q., Aljawarneh, M., Hazaymih, R., & Al Mamlook, R. E. (2025). Ethical issues in cybersecurity for autonomous vehicles (AV) and automated driving: A comprehensive review. In *Utilizing AI in Network and Mobile Security for Threat Detection and Prevention* (pp. 173–196). IGI Global Scientific Publishing.
[10] Li, Y., Jiang, Z. M., Li, H., Hassan, A. E., He, C., Huang, R., Zeng, Z., Wang, M., & Chen, P. (2020). Predicting node failures in an ultra-large-scale cloud computing platform: An AIOps solution. *ACM Transactions on Software Engineering and Methodology (TOSEM), 29*(2), 1–24.
[11] Velliangiri, S., Karthikeyan, P., & Kumar, V. V. (2021). Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks. *Journal of Experimental & Theoretical Artificial Intelligence, 33*(3), 405–424.
[12] Al-Na'amneh, Q., Aljaidi, M., Gharaibeh, H., Nasayreh, A., Al Mamlook, R. E., Almatarneh, S., Alzu'bi, D., & Husien, A. S. (2023). Feature selection for robust spoofing detection: A chi-square-based machine learning approach. In *2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)* (pp. 1–7). IEEE.
[13] Alshammari, A., & Aldribi, A. (2021). Apply machine learning techniques to detect malicious network traffic in cloud computing. *Journal of Big Data, 8*(1), 90.
[14] Abu-Zaid, A., Aljaidi, M., Al-Na'amneh, Q., Samara, G., Alsarhan, A., & Qadoumi, B. (2025). Advancements and challenges in the Internet of Drones security issues: A comprehensive review. In *Machine Intelligence Applications in Cyber-Risk Management* (pp. 1–24). IGI Global.
[15] Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Doan, L. M. T., Hall, K., Boddu, S., & Kobusinska, A. (2022). A survey on intrusion detection systems for fog and cloud computing. *Future Internet, 14*(3), 89.
[16] Alwakeel, A. M. (2021). An overview of fog computing and edge computing security and privacy issues. *Sensors, 21*(24), 8226.
[17] SaiSindhuTheja, R., & Shyam, G. K. (2021). An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. *Applied Soft Computing, 100*, 106997.
[18] Aljawarneh, M. (2025). Ethical issues in cybersecurity for autonomous vehicles (AV) and automated driving. In *Utilizing AI in Network and Mobile Security for Threat Detection and Prevention* (p. 173). IGI Global Scientific Publishing.

[19] Sheikh, M. S., Liang, J., & Wang, W. (2020). Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey. *Wireless Communications and Mobile Computing, 2020*(1), 5129620.
[20] Rani, P., Singh, S., & Singh, K. (2024). Cloud computing security: A taxonomy, threat detection and mitigation techniques. *International Journal of Computers and Applications, 46*(5), 348–361.
[21] Dhingra, S., Madda, R. B., Patan, R., Jiao, P., Barri, K., & Alavi, A. H. (2021). Internet of Things-based fog and cloud computing technology for smart traffic monitoring. *Internet of Things, 14*, 100175.
[22] Pasham, S. D. (2021). Graph-based models for multi-tenant security in cloud computing. *International Journal of Modern Computing, 4*(1), 1–28.
[23] Kumar, M., & Singh, A. K. (2020). Distributed intrusion detection system using blockchain and cloud computing infrastructure. In *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)* (pp. 248–252). IEEE.
[24] Kumari, P., & Kaur, P. (2021). A survey of fault tolerance in cloud computing. *Journal of King Saud University - Computer and Information Sciences, 33*(10), 1159–1176.
[25] You, D. (2024). Application of cloud computing detection based on sensor networks in enterprise economic statistics. *Measurement: Sensors, 34*, 101254.
[26] Alshehri, M., & Panda, B. (2020). Minimizing data breach by a malicious fog node within a fog federation. In *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud) / 2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (pp. 36–43). IEEE.
[27] Karthika, A., & Muthukumaran, N. (2022). An ADS-PAYG approach using trust factor against economic denial of sustainability attacks in cloud storage. *Wireless Personal Communications, 122*(1), 69–85.
[28] Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. *Sustainability, 14*(18), 11213.
[29] Wang, T., Zhang, G., Bhuiyan, M. Z. A., Liu, A., Jia, W., & Xie, M. (2020). A novel trust mechanism based on fog computing in sensor–cloud system. *Future Generation Computer Systems, 109*, 573–582.
[30] Bharany, S., Badotra, S., Sharma, S., Rani, S., Alazab, M., Jhaveri, R. H., & Gadekallu, T. R. (2022). Energy efficient fault tolerance techniques in green cloud computing: A systematic survey and taxonomy. *Sustainable Energy Technologies and Assessments, 53*, 102613.
[31] Sharma, S. (2024). Strengthening cloud security with AI-based intrusion detection systems.
[32] Welsh, T., & Benkhelifa, E. (2020). On resilience in cloud computing: A survey of techniques across the cloud domain. *ACM Computing Surveys (CSUR), 53*(3), 1–36.
[33] Sadaf, K., & Sultana, J. (2020). Intrusion detection based on autoencoder and isolation forest in fog computing. *IEEE Access, 8*, 167059–167068.
[34] Wang, Y., & Yang, X. (2025). Research on enhancing cloud computing network security using artificial intelligence algorithms. *arXiv preprint arXiv:2502.17801*.
[35] Singh, A., & Chatterjee, K. (2021). Securing smart healthcare system with edge computing. *Computers & Security, 108*, 102353.
[36] Shahid, M. A., Islam, N., Alam, M. M., Su'ud, M. M., & Musa, S. (2020). A comprehensive study of load balancing approaches in the cloud computing environment and a novel fault tolerance approach. *IEEE Access, 8*, 130500–130526.
[37] Senapati, B. R., Swain, R. R., & Khilar, P. M. (2022). Hard and soft fault detection using cloud-based VANET. In *Intelligent and Cloud Computing: Proceedings of ICICC 2021* (pp. 133–143). Springer.
[38] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., & Zomaya, A. Y. (2021). Federated learning for COVID-19 detection with generative adversarial networks in edge cloud computing. *IEEE Internet of Things Journal, 9*(12), 10257–10271.
[39] Kushwah, G. S., & Ranga, V. (2020). Voting extreme learning machine based distributed denial of service attack detection in cloud computing. *Journal of Information Security and Applications, 53*, 102532.
[40] Liang, J., Zhang, M., & Leung, V. C. M. (2020). A reliable trust computing mechanism based on multisource feedback and fog computing in social sensor cloud. *IEEE Internet of Things Journal, 7*(6), 5481–5490.
[41] El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering, 29*(1), 223–246.
[42] Patel, S. (2022). Edge computing vs. traditional cloud: Performance & security considerations. *Spanish Journal of Innovation and Integrity, 12*, 312–320.
[43] Abdullayeva, F. J. (2021). Advanced persistent threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm. *Array, 10*, 100067.
[44] Mourad, A., Tout, H., Abdel Wahab, O., Otrok, H., & Dbouk, T. (2020). Ad hoc vehicular fog enabling cooperative low-latency intrusion detection. *IEEE Internet of Things Journal, 8*(2), 829–843.
[45] Javadpour, A., Wang, G., & Rezaei, S. (2020). Resource management in a peer to peer cloud network for IoT. *Wireless Personal Communications, 115*(3), 2471–2488.
[46] Gupta, A., & Simon, R. (2024). Enhancing security in cloud computing with anomaly detection using random forest. In *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (pp. 1–6). IEEE.
[47] Reddy, S. R., & Shyam, G. K. (2022). A machine learning based attack detection and mitigation using a secure SaaS framework. *Journal of King Saud University – Computer and Information Sciences, 34*(7), 4047–4061.
[48] Labiod, Y., Korba, A. A., & Ghoualmi, N. (2022). Fog computing-based intrusion detection architecture to protect IoT networks. *Wireless Personal Communications, 125*(1), 231–259.

[49] Al-Na'amneh, Q., Almomani, A., Nasayreh, A., Nahar, K. M. O., Gharaibeh, H., Al Mamlook, R. E., & Alauthman, M. (2024). Next generation image watermarking via combined DWT-SVD technique. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1–10). IEEE.
[50] Jaradat, A. S., Nasayreh, A., Al-Na'amneh, Q., Gharaibeh, H., & Al Mamlook, R. E. (2023). Genetic optimization techniques for enhancing web attacks classification in machine learning. In *2023 IEEE International Conference on Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing; Cloud and Big Data Computing; Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp. 0130–0136). IEEE.
[51] Al-Na'amneh, Q., Nasayreh, A. N., Al Mamlook, R., Gharaibeh, H., Alsheyab, A. M., & Almaiah, M. A. (2024). Improving memory malware detection in machine learning with random forest-based feature selection. In *Risk Assessment and Countermeasures for Cybersecurity* (pp. 96–114). IGI Global.
[52] Abu Laila, D., Al-Na'amneh, Q., Aljaidi, M., Nasayreh, A. N., Gharaibeh, H., Al Mamlook, R., & Alshammari, M. (2024). Enhancing 2D logistic chaotic map for gray image encryption. In *Risk Assessment and Countermeasures for Cybersecurity* (pp. 170–188). IGI Global.
[53] Al-Na'amneh, Q., Dhifallah, W., Hazaymih, R., Almaiah, M. A., Alsheyab, A., Alshinwan, M., & Qadoumi, B. (2025). DIS flooding attack impact in RPL-based 6LoWPAN network. In *Machine Intelligence Applications in Cyber-Risk Management* (pp. 69–84). IGI Global Scientific Publishing.

Biographies



Dr. Mohammed Maayah is an Associate Professor in the Department of Computer Science at University of Jordan. Almaayah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.