STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

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

A Quantitative Framework for Dynamic Cyber Risk Assessment in Hybrid Enterprise Networks

Udit Mamodiya[1], Indra Kishor[2], Pellakuri Vidyullatha[3], Rami Shehab[4], Amer Alqatish[5*], Ghada Alradwan[6]

[1]Associate Professor, Faculty of Engineering and Technology, Poornima University, Jaipur 303905, Rajasthan, India
[2] Assistant Prof. Dept. of CSE, Poornima Institute of Engineering and Technology, Jaipur 302022, Rajasthan, India
[3]Professor, Department of CSE, Koneru Lakshmaiah Education Foundation Greenfields, Vaddeswaram, Guntur, AP, India
[4]Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, 31982, Al-Ahsa, Saudi Arabia;
[5]Applied College, King Faisal University, Al-Ahsa, Saudi Arabia
[6]Deanship of Development and Quality Assurance, King Faisal University, 31982, Al-Ahsa, Saudi Arabia

ARTICLE INFO

Article History

Received: 10-01-2026
Revised: 30-04-2026
Accepted: 10-06-2026
Published: 16-06-2026

Vol.2026, No.2

DOI:

Corresponding author.
Email:
aalqatish@kfu.edu.sa

Orcid:
https://orcid.org/0000-0002-8022-4252

ABSTRACT

Cyber risk estimation in hybrid enterprise networks, which integrate cloud-native services with legacy on-premises infrastructure, is increasingly challenging due to their distributed architecture and complex interdependencies. Traditional risk assessment approaches often fail to capture real-time exposure dynamics arising from service-level interactions and context-dependent infrastructure relationships. To address this limitation, this study proposes the Dynamic Enterprise Cyber Risk Estimation with Service Topology (DECRE-ST) framework, an adaptive and quantitative approach for real-time cyber risk estimation in hybrid enterprise environments. The proposed framework models enterprise infrastructure as a weighted interaction graph and incorporates contextual exposure factors to compute dynamic asset risk scores. Experimental validation was performed using enterprise telemetry datasets comprising 120 interconnected assets deployed within simulated hybrid cloud environments. Results demonstrate that the DECRE-ST framework improves risk prediction consistency by 17.6% and reduces estimation variance by 21.3% compared with Bayesian-based dynamic risk estimation models. Furthermore, the framework decreases mean risk estimation latency by 14.2% under fluctuating threat conditions. Ablation analysis further confirms the effectiveness of contextual service dependency modeling, contributing nearly 11% to overall estimation stability. These findings indicate that the DECRE-ST framework provides a more accurate, adaptive, and context-aware approach to cyber risk estimation. By enabling continuous assessment of evolving enterprise environments, the framework supports adaptive security governance and enhances decision-making for organizations operating hybrid cloud infrastructures.

Keywords: Hybrid enterprise networks; Dynamic cyber risk assessment; Context-aware risk modeling; Service dependency analysis; Quantitative risk estimation

How to cite the article

1. Introduction

The growing digitization of the operations of the enterprise has led to a gradual shift of monolithic information systems to distributed computing systems that integrate private infrastructure and public cloud resources. Enterprise applications have become a regular execution in heterogeneous environments, where business critical services could co-exist in on-premises data centres, virtualized cloud instances or containerized micro services clusters running at the network edge [1], [2]. It is represented as a cascading effect that is initiated by inter service interactions and common execution pathways. An error in the configuration of a cloud-based authentication service, such as, can accidentally open vulnerability controls on locally installed enterprise databases and provide latent vulnerability routes where otherwise isolated network segments overlay [3]. This means that the process of assessing cyber risk in hybrid enterprise ecosystem must have a modeling paradigm that can model dynamic system behaviour and not vulnerability snapshots [4].

1.1 Background and Motivation

The modern digital organizations are operational on the concept of hybrid enterprise networks. By combining Software-as-a-Service environments with locally controlled infrastructure, a business can redistribute the computational workloads in the most effective way in consideration of both the performance efficiency and economic limits [5]. Nevertheless, such integration must surely expand the attack surface by adding other ingress points, trust between distributed network domains, and authentication dependencies [6]. The conventional enterprise risk management systems were designed based on a relatively stable infrastructure set-up. These frameworks are normally based on regular vulnerability scanning, compliance scoring systems, and deterministic threat probability estimation to produce audit ready risk indicators [7]. Although these techniques are still applicable to static networked setting, they lose their relevance as system configurations vary to meet the changing workload needs or the dynamic orchestration policies [8]. Inspired by the necessity to balance operational flexibility and cybersecurity resilience, recent studies pursued the means of introducing risk awareness into the enterprise network management policy [9].

1.2 Cyber Risk in Hybrid Enterprise Environments

The notion of cyber risk within the framework of hybrid enterprises cannot be adequately elucidated, using assessment frameworks centered on assets. Extensive connectivity the decentralized variant of hybrid infrastructure introduces complex patterns of interaction among the virtual machines, containerized services, and edge-linked gateways all of which may exhibit various vulnerability characteristics when placed in differing operating environments [10]. In addition, the contextual exposure of the underlying software components may often be altered depending on the portability of the enterprise applications between the execution environments, either load balancing or fault tolerance. An instance of a service that can be deemed secure when deployed on an isolated and private network can be vulnerable to reconnaissance when exposed on a cloud-based orchestration platform [11]. As the network communication channels are extended to facilitate the needs of distributed processing, the possibility of the threat mobility in a lateral direction grows accordingly [12]. Assessment of such risk thus requires an analytical model able to capture not only the individual vulnerabilities but also dynamic interactions in which the compromise events can spread.

1.3 Limitations of Static Risk Assessment Models

It has been observed that the commonly used scoring systems like Common Vulnerability Scoring System (CVSS) are originally designed to support standardized vulnerability prioritization in a relatively stable network environment [13]. Although these models provide convenient information regarding the degree of the severity of established software vulnerabilities, they do not adopt contextual factors that identify the likelihood of exploitation in a hybrid enterprise setting [14]. This weakness is further enhanced by intermittent evaluations by audits which introduce risk indicators which are only valid within a limited time. Even minor changes in the workload distribution, network design or the policy of service orchestration can have an incredible impact on the threat environment between cycles of successive audit [15]. Thus, the security teams which rely solely on the static assessment techniques may not be able to appreciate the systemic impact of the arising vulnerabilities. Besides, deterministic risk scoring schemes are likely to assume that the assets of an enterprise are independent of one another, hence ignoring interdependencies whereby compromise events can be transmitted across service domains [16]. This assumption undermines the accuracy of the risk estimates in the environment where the application architecture is very coupled and shared scheme of authentication.

1.4 Emerging Approaches in Dynamic Risk Modeling

After discovering the limitations of the previously used approaches to the assessment of the state, recent studies have proposed the concept of adaptive risk modelling approaches that incorporate real-time telemetry and network behaviour analysis [17]. Probability based graphical models have been used to estimate the threat propagation paths of distributed enterprise systems [18]. The machine learning approaches have been found to be promising in the detection of suspicious patterns of interactions that would indicate the existence of latent events of compromise [19]. They are methods that seek to model the change over time of exposure to system vulnerability utilizing continuous monitoring data acquired by network sensors and execution logs. Nevertheless, little has been done in integrating dynamic risk modeling in enterprise cybersecurity governance despite these advances. Current frameworks often only work as independent analytical systems whose results cannot easily be implemented in operational processes of decision-making [20]. To seal this gap, risk evaluation mechanisms should be developed which can change the network conditions and keep the audit transparent at the same time.

1.5 Research Gap and Contribution

A critical analysis of the literature available indicates that the current literature mainly assesses risk at the asset level, as opposed to system level, with regards to the majority of enterprise cybersecurity frameworks. Although the studies of dynamic threat detection methods have been explored, there is still no complete integration into quantitative risk assessment models that can be applied in a hybrid enterprise setting [21]. This paper fills the above gap by introducing a quantitative model that treats cyber risk as a time-varying form of network interactions of the enterprise. Nevertheless, unlike traditional methods based on an unchanging set of vulnerability scores, the suggested methodology combines both asset criticality weighting and probabilistic threat propagation analysis to produce adaptive risk estimates.

1.6 Need for the Study

The gap between the functionality and the safety of operations grows as the number of enterprises where multi-cloud deployment strategies are implemented is rising. The security audit practice that does not take into consideration the dynamism in infrastructure behavior can unintentionally mask the latent vulnerability pathways in the distributed network environment [22]. It is hence necessary to develop a risk assessment framework that has the capability to capture real-time system interactions in order to facilitate informed governance decisions and regulatory compliance in hybrid systems in the context of enterprise architecture.

1.7 Research Objectives

The principal objectives of this research are as follows:

- To develop a quantitative cyber risk evaluation model for hybrid enterprise networks
- To incorporate dynamic system interactions into risk estimation processes
- To assess threat propagation pathways across distributed infrastructure layers
- To validate the proposed framework within a hybrid enterprise test environment

1.8 Scope of the Work and Novelty

This paper is limited to risk assessment in enterprise network where an on-site infrastructure is combined with cloud-computing facilities. The suggested framework lays emphasis on the modeling of cyber risk as an inter-service dependency-based and time workload-dependency model. The novelty of the current work is in the fact that cyber risk is viewed as a dynamic system-level characteristic, but not as a fixed asset-level indicator. The proposed framework provides more sensitivity to threat dynamics due to the incorporation of interaction-conscious probabilistic modeling into the risk assessment process. The approach will comprise the gathering of the multi-source telemetry of heterogeneous execution settings and, subsequently, the probabilistic assessment of the threat propagation routes with the assistance of the asset-weighted measures of interactions. The rest of the paper is structured in the following way. Section 2 conducts a related work review on cyber risk quantification. Section 3 provides the proposed risk assessment dynamic methodology. Section

4 outlines the experiment and analysis of the findings. Section 5 provides implications to implementation of enterprise governance systems. Section 6 concludes the paper.

2. Literature Review

Cyber risk analysis of large-scale digital infrastructure in enterprises has received an increasing amount of attention in the past decade. This transformation has been mostly influenced by the incremental movement of enterprise services out of isolated systems of computing and into interconnected systems that integrate private infrastructure with distributed cloud assets. In this type of hybrid deployment, the conventional ideas of perimeter security have increasingly become hard to sustain. Risk is not limited anymore to just one area of operation, rather it tends to be a result of the interactions between loosely coupled service components which are deployed in various trust zones [23]. New studies have tried to resolve this complexity by proposing new modeling techniques that can be used to simultaneously consider technical vulnerabilities and contextual exposure factors.

2.1 Enterprise Cyber Risk Assessment Frameworks

With the development of enterprise networks to offer the ability to perform distributed processing, researchers started to investigate risk assessment techniques that took into consideration service dependencies and communication routes [24]. To describe enterprise systems as graphical systems, network-centric models were introduced in which nodes were the computational assets and edges the communication pathways between them [25]. Using the analysis of attack paths of these graphs, the systemic implications of localized compromise events could be estimated. Nevertheless, most of these models had the assumption that the topology of the network was unchanged with time. Such assumptions do not usually work in environments that are hybrid in nature with dynamic workload migration and automated orchestration. Therefore, topology-based risk estimation frameworks do not have the ability to represent the operationally exposed enterprise assets in changing deployment circumstances [26].

2.2 Risk Propagation Modeling in Distributed Systems

Risk propagation has become one of the key topics in recent studies in cybersecurity. Instead of considering vulnerabilities as standalone phenomena, the propagation models attempt to determine how the compromise events can propagate between interrelated service areas [27]. A number of works have used the probabilistic graphical models to model such dependencies and assess the probability of the escalation of such threats in distributed networks. It has also utilized the application of the Bayesian methods of inference, including, that approximates the probability of an attacker to traverse two or more nodes which are already compromised with a shared authentication system or even a shared data exchange system [28]. These approaches can provide helpful facts concerning the systemic processes of enterprise networks under adversarial conditions. Propagation based models take the form of historical incident statistics or redeemed attack conditions despite being analytically grounded. They can therefore find it difficult to track emergent patterns of threats that arise because of real-time system configuration or workload redistribution. The hybrid enterprise environments in particular may be susceptible to regular deployment updates so that the exposure of services can be changed in a manner that is not reflected in the dynamic attack graphs [29].

2.3 Dynamic Network Behavior and Threat Exposure

It is observed that owing to the demerits of the conventional approaches to modeling, recent research has been focused towards the incorporation of the temporal variability in the process of cyber risk assessment. The capability to collect dynamic system behaviour has been proposed to be attained by monitoring structures capable of collecting live telemetry of network sensors and application log entries [30]. These structures are offered through the analysis of traffic characteristics, service interaction indicators, and resource consumption tendencies with the purpose of identifying the deviations which are the manifestations of the possible compromise incidents. This has been achieved through machine learning based anomaly detection algorithms that differentiate between normal workload variations and malicious behavior [31]. Still, it is not yet easy to translate behavioral knowledge into quantitative risk estimates. Most of the current anomaly detection systems are geared towards threat detection, as opposed to risk assessment, and their results may not be interpretable by the governance decision-making process [32]. In a business environment where regulatory compliance is such an issue, risk assessment processes should give transparent reasons behind their findings.

2.4 Hybrid Cloud Security and Trust Relationships

The implementation of hybrid cloud infrastructures present more complexity to the enterprise cybersecurity management. Services that are implemented on both public and private infrastructure can be based on federated identity systems and shared storage interfaces, and develop implicit trust relations between otherwise autonomous networks domains [33]. Such connections can establish the movement of threats later in case they are utilized by the enemies. As an example, the hijacked credentials acquired in one of the clouds of a hosted application could be utilized to exploit locally controlled enterprise resources via single sign-on systems. The security consequences of these cross-domain interactions depend on modeling the trust diminution within the environment of adversarial influence, which cannot be evaluated without a modeling framework that can be used to depict such interactions [34]. There have been suggested reasons of trust based risk assessment models that give confidence scores to communication channels depending on the past interaction patterns. Although these models provide a promising way of capturing inter-domain dependencies, they often rely on manually-defined metrics of trust that cannot be easily changed over time to match changing infrastructure arrangements [35].

2.5 Probabilistic Approaches to Cyber Risk Quantification

The probabilistic risk assessment methods have also been extensively discussed as a way of accepting uncertainty in enterprise cybersecurity analysis. Some techniques such as Monte Carlo simulation have been used to assess the possible effects of various simultaneous threat situations [36]. The strategies provide a less obvious description of enterprise risk exposure by creating an assignment of potential results and not a predictive score. Game-theoretic models have also been suggested that attempt to model adversarial behaviour in enterprise networks. The models attempt to forecast the schemes of attackers and balance the countermeasures defense against the schemes [37]. Although these techniques may provide valuable theoretical information their sensitivity in terms of cost can be a drawback to their applicability in large scale hybrid environments. The later publication has tried to integrate the probabilistic modelling with the real time telemetry in order to generate adaptive risk indicators. It proposes that stochastic process models and dynamic Bayesian networks represent the tools of revising risk estimates, using observed behavior of the system [38]. Nonetheless, the application of these methods in working systems of enterprise governance is minimal.

2.6 Limitations of Existing Dynamic Risk Models

Although the literature shows that the dynamic risk assessment methodologies have made significant advances, there are still a number of challenges. Most of the suggested frameworks exist outside the enterprise network management systems, hence they are not as effective in informing the operational decision-making processes [39]. Moreover, the models that are currently available tend to concentrate on the vulnerability analysis or behavioral monitoring, but not both sides of the coin into a single evaluation process. Such fragmentation can result in false risk estimations where important interaction channels between distributed service components are missed [40]. Scalability as well is a major issue of concern. The hybrid enterprise networks can include thousands of networked assets whose vulnerability behavior changes when the workload changes. Such complexity can only be modeled approximately using computationally efficient methods that can update risk estimates in near real time [41]. Specific analysis of current literature in quantitative and adaptive modeling of cyber risks was undertaken to determine the shortcomings of methodologies of available frameworks of assessment of security of enterprises. Table 1, show comparative gap analysis that existing methods lack system-level interaction modelling and real-time adaptive risk quantification. The next section presents the suggested methodology that will help to meet these needs in hybrid enterprise networks.

Table 1. Comparative Literature Gap Analysis of Dynamic Cyber Risk Assessment Frameworks in Hybrid Enterprise Environments

S. No.	Author(s) / Year / Ref. No.	Title / Focus Area	Methodology / Tools Used	Key Findings	Limitations / Gaps Identified	Relevance to the Current Study
1	Behbehani et al., 2023 [2]	Cloud Enterprise Dynamic Risk Assessment using DBNs	Dynamic Bayesian Networks for cloud risk modeling	Demonstrated adaptive risk estimation based on temporal threat behavior	Focus limited to single-domain cloud deployments; cross-domain enterprise risk	Highlights the need for a unified risk model capable of spanning hybrid

				in cloud platforms	propagation not considered	infrastructure layers
2	Xie et al., 2023 [8]	Multi-objective dynamic network security assessment	Bayesian attack graph modeling	Provided improved scenario-based threat evaluation under probabilistic network configurations	Assumes relatively stable topology; does not reflect workload-driven service migration in hybrid setups	Supports the integration of dynamic topology awareness into enterprise-level risk estimation
3	Burnap et al., 2024 [6]	Context-aware automated cyber-attack intelligence mapping	Impact mapping aligned with system-level objectives	Linked threat intelligence with operational performance metrics	Lacks quantitative propagation modeling for multi-domain enterprise assets	Reinforces the requirement for system-level interaction-aware risk modeling
4	Pal et al., 2023 [15]	Quantifying multi-party APT cyber-risk exposure in IIoT networks	Risk exposure analysis using enterprise IoT communication graphs	Addressed adversarial threat movement in interconnected industrial systems	Primarily tailored to industrial IoT ecosystems; enterprise hybrid cloud dynamics underrepresented	Emphasizes the importance of modeling distributed threat escalation pathways
5	AlHidaifi et al., 2024 [19]	Cyber Resilience Quantification Framework for IT infrastructure	Risk-resilience evaluation metrics based on network performance	Introduced measurable resilience indicators for enterprise IT systems	Static resilience metrics insufficient for real-time hybrid network environments	Indicates the necessity of dynamic risk metrics responsive to infrastructure variability
6	Lin et al., 2024 [21]	Real-time cyber risk visual analytics framework	Real-time monitoring with risk visualization tools	Enabled contextual understanding of cyber threat conditions	Lacks probabilistic interaction modeling across heterogeneous enterprise layers	Encourages the development of adaptive probabilistic risk quantification mechanisms
7	Soylu and Daş, 2025 [31]	Hybrid graph neural network for cyber-attack prediction	GNN-based predictive analysis on dynamic network data	Demonstrated improved attack prediction accuracy in evolving networks	Prediction-oriented; does not translate behavioral anomalies into quantifiable enterprise risk	Motivates integration of behavioral analytics with risk estimation models
8	Rana et al., 2024 [38]	FAIR-modified attack tree-based risk assessment	Quantitative risk estimation using modified attack trees	Provided structured financial risk impact evaluation	Does not capture dynamic threat propagation across hybrid network domains	Forms the basis for extending quantitative risk modeling to enterprise-scale hybrid systems

3. Methodology

Cyber risk measurement of hybrid enterprise environments needs a model that goes beyond periodic vulnerability scoring and one-time evaluation of individual assets. Practically, enterprise infrastructure works as a dynamically changing ecosystem, where the risk exposure can be determined by the interaction of services, workload mobility and context-specific trust of distribution domains of distributed execution. The methodology that will be followed in the present study

is thus anchored on the fact that cyber risk ought to be taken as a dynamic system-level quality based on observable behavior on the network, instead of an intrinsic measure of a component.

In order to make this perspective operational, the proposed framework combines multi-source enterprise telemetry with probabilistic interaction modeling to measure the risk propagation between the layers of hybrid infrastructure. The telemetry of services in cloud-hosted services, management of network segments locally and identity management systems is initially converted into structured exposure indicators. These indicators are then mapped onto an enterprise interaction graph that is a representation of interdependent service relationships. Asset level vulnerability functions, likelihood estimators and contextual criticality weights are then used to estimate the quantitative risk values. The risk estimates that result are continuously aggregated to yield an enterprise-wide index of exposure that can be able to capture changes in system configuration over time.

3.1 Enterprise Telemetry Data Acquisition Layer

The quantitative measure of cyber risk in hybrid enterprise settings relies, in its turn, on the presence of context-rich operational information gained as a result of multiple infrastructure layers. Unlike the fixed vulnerability rating systems, which use fixed measures of severity, dynamic risk estimation involves ongoing monitoring of network behavior and interaction patterns of services in the distributed execution domains. In this aspect, enterprise telemetry offers a quantifiable view of infrastructure exposure through a real-time perspective of system activity. The recent research on probabilistic threat modelling has highlighted the significance of incorporation of behavioral evidence based on the enterprise monitoring systems in the risk assessment process [11], [18].

Hybrid enterprise networks will generally produce various types of telemetry emanating out of cloud-hosted virtual machines, locally controlled application servers, identity manager systems, and network communication gateways. Such streams of data can contain authentication, workload deployment traces, intrusion detection alerts and anomaly indicators derived out of traffic analysis engines. When combined, this information corresponds to the structural organization of enterprise infrastructure as well as the state of particular service components [21]. The methodology framework used in this research involves the use of telemetry using these heterogeneous sources so as to extract exposure measures which are later used to generate quantitative risk model.

3.1.1 Data Sources in Hybrid Enterprise Networks

The telemetry data used in the current framework originates in three main areas of infrastructure, namely, the public cloud settings, on premise enterprise networks, and edge-related service interfaces. Monitoring tools that are hosted in clouds are the ones that provide logs on the execution that define the pattern of resource allocation and service deployment, and network devices that are under local control give data about the anomalies in the traffic and about intrusion efforts. Identity management platforms also maintain authentication logs that express the possible privilege abuse or credential misuse [24]. Besides data that is generated in-house, threat intelligence feeds acquired via security information and event management (SIEM) systems are also taken into consideration to consider emerging patterns in vulnerabilities. Such feeds provide situational awareness through the correlation of enterprise-specific observations with threat indicators that are externally reported. It has been shown in previous research that risk estimation is more accurate when shared threat intelligence is included in the distributed enterprise setting [30].

3.1.2 Data Types Used for Risk Modeling

Configurations management logs are used to calculate the vulnerability exposure measures, and communication and authentication latency and failure rates are used to estimate indicators of service trust degradation. The score of network traffic anomalies is gained based on behavioral analysis modules that identify deviation of workload patterns compared to baseline workload pattern [31]. The table 2 will be a summary of the types of enterprise telemetry used in the risk assessment framework proposed and the analytical relevance.

Table 2. Enterprise Telemetry Data Categories and Risk-Relevant Attributes.

Data Category	Source Platform	Analytical Indicator	Risk Modeling Relevance

Authentication Logs	Identity Management Systems	Privilege Misuse Frequency	Access Control Exposure
Network Traffic Metrics	Enterprise Routers / IDS	Anomaly Score	Lateral Threat Movement
Service Deployment Logs	Cloud Orchestration Platforms	Workload Migration Rate	Contextual Vulnerability
Threat Intelligence Feeds	SIEM Systems	Emerging Attack Patterns	Threat Likelihood Estimation
Communication Latency Records	Application Gateways	Trust Degradation Index	Service Interaction Risk

As demonstrated in Table 2, every type of telemetry leads to the derivation of measures of quantitative exposures that are subsequently incorporated in the models of risk formulation at the asset level. The logical transformation of raw enterprise telemetry into analytically meaningful metrics is the initial step of the suggested methodology, which will allow modeling interaction-driven cyber risk across the hybrid infrastructure layers in the future.

3.2 System-Level Dynamic Cyber Risk Representation Model

Cyber risk in hybrid enterprise environment does not simply occur by having any vulnerabilities in software and single misconfigurations. Instead, it is influenced by the operational relationships which exist between the computational services which are deployed at distributed layers of infrastructure. These services, including cloud-based authentication systems to on premise applications servers, communicate with each other continuously via shared communication channels and access controls based on trust. Consequently, a service component compromise can affect the exposure profile of a number of other components indirectly, as a result of dependency relationships [12], [26]. The state indicates the operational security state of the asset based on current workload conditions, communication requirements and access control limitations. In contrast to the old-fashioned assessment techniques, which provide fixed severity ratings to each part of the system, the current framework represents cyber risk as a term of asset interaction patterns in the domains of hybrid infrastructures [14]. In this model, the enterprise services are modeled on the nodes of a directed dependence graph, and the communication pathways between the services are modeled as weighted edges. These weighting functions of these edges are based on contextual trust indicators, which were calculated based on enterprise telemetry, such as rates of authentication success, service availability indicators, and communication latency distributions. Previously, it has been demonstrated that the use of this interaction-aware modeling can lead to a better estimation of systemic vulnerability in a distributed enterprise setting [25]. The system-level architecture of the proposed framework used to represent the dynamic cyber risks is represented in figure 1. The exposure indicators derived through telemetry are combined with service interaction dependencies to assess the probability of escalation in the threat in an interconnected infrastructure layer (shown in Figure 1). The resultant representation provides the ability to trace the enterprise risk exposure continuously as service deployment trends change with time.

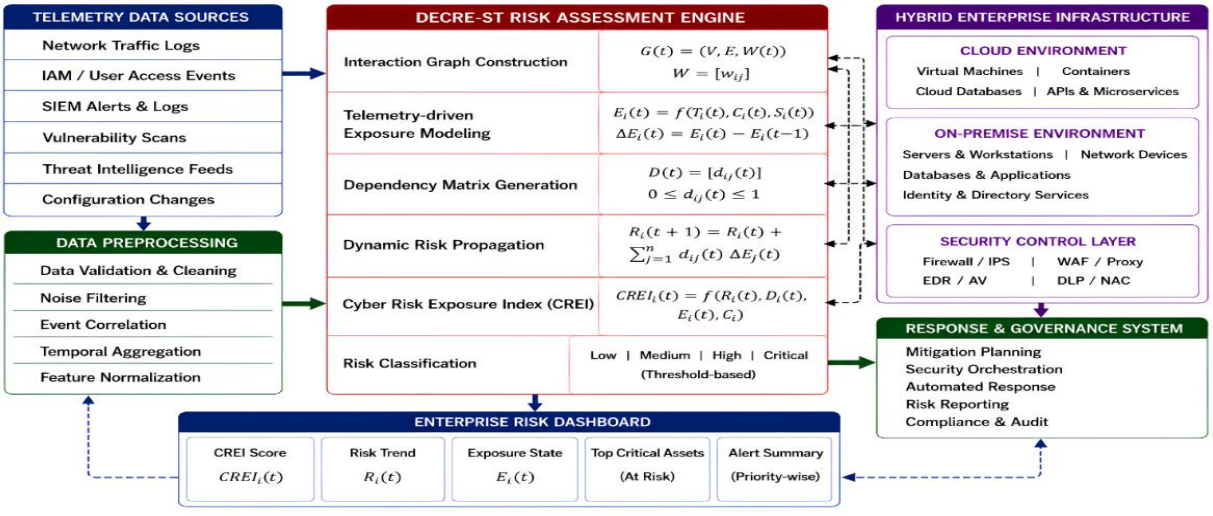

Figure 1. System-level dynamic cyber risk representation model for hybrid enterprise infrastructure

The proposed model can take into consideration the effects of cross-domain dependencies on enterprise security posture by integrating interaction-sensitive exposure metrics into a risk assessment. One of them is the fact that an intrusion of a cloud-hosted identity service can lead to the indirect exposure of locally managed database systems via federated authentication paths [20].

3.3 Hybrid Enterprise Network Representation Model

It has been demonstrated that dependency-conscious modeling enhances the quality of risk estimation in a distributed enterprise system that can have escalation of threats via interaction pathways in its operations [17], [25].

3.3.1 Infrastructure as Weighted Interaction Graph

Let the hybrid enterprise network be represented as a directed graph as (1):

$$G = (N, E, W) \cdots (1)$$

Where:

- N={n1,n2,...,nk} denotes the set of enterprise assets
- E={e_{ij}} represents the dependency links between assets
- W={w_{ij}} denotes the interaction weights associated with asset dependencies

Here, the weight w_{ij} reflects the operational reliance of asset n_i on asset n_j, derived from telemetry indicators such as communication latency and authentication success frequency.

3.3.2 Service Dependency Modeling

The interaction strength between two dependent services is quantified using a normalized trust parameter defined as (2):

$$D_{ij} = \frac{T_{ij}}{\sum_{j=1}^{k} T_{ij}} \cdots (2)$$

Where, D_{ij} denotes the normalized dependency strength, T_{ij} represents telemetry-derived trust indicators between assets n_i and n_j. Higher values of D_{ij} indicate increased likelihood of compromise propagation between dependent enterprise services.

3.3.3 Context-Aware Node Exposure

Each enterprise asset is assigned an exposure coefficient reflecting its susceptibility to threat exploitation under prevailing operational conditions (3):

$$E_i = \alpha V_i + \beta C_i \cdots (3)$$

Where, E_i denotes exposure coefficient of asset n_i, V_i represents vulnerability density, C_i indicates asset criticality within enterprise workflows and α,β are weighting parameters satisfying α+β=1. As shown in Table 3, contextual exposure indicators associated with enterprise assets are incorporated into the weighted network model for subsequent risk propagation analysis across hybrid infrastructure domains.

Table 3. Hybrid Enterprise Asset Classification and Risk Context Parameters

Asset Category	**Deployment Domain**	**Vulnerability Index (V_i)**	**Criticality Index (C_i)**
Authentication Server	Cloud / On-Prem	Access Misuse Rate	Privilege Importance
Application Service	Cloud	Configuration Exposure	Functional Priority
Database System	On-Prem	Data Sensitivity	Operational Dependence
Network Gateway	Edge	Traffic Variability	Connectivity Importance
Monitoring Module	Hybrid	Reliability Score	Service Visibility

3.4 Quantitative Asset Risk Formulation

After the description of enterprise infrastructure as a weighted interaction graph in Section 3.3, the following step would be the quantification of asset-level cyber risk. Under hybrid enterprise conditions the risk level of a computational asset is not merely a matter of the vulnerability properties of the asset but also of the probability of being exploited in case of prevailing circumstances. The current research on quantitative cybersecurity risk management has highlighted the need to incorporate contextual indicators of exposure into asset level assessment systems so as to achieve realistic risk estimates [1], [20]. The proposed framework defines asset risk as a complex functional relationship of three key components which are vulnerability exposure, threat likelihood and operational criticality. All these elements are based on enterprise telemetry addressed in Section 3.1 and further combined to generate a normalized risk estimate on a per-asset basis of infrastructure assets.

3.4.1 Asset Vulnerability Function

The underlying susceptibility with an enterprise asset is approximated with the help of telemetry-based exposure conditions like configuration anomalies, the patch latency, and the frequency of privilege abuse. Assuming the vulnerability of asset ni is (4):

$$V_i = \frac{1}{m}\sum_{k=1}^{m} v_{ik} \cdots (4)$$

Where, V_i denotes the normalized vulnerability index of asset n_i, v_{ik} represents the k^{th} exposure indicator derived from enterprise telemetry. m is the total number of vulnerability indicators considered. Higher values of V_i indicate increased susceptibility of the asset to exploitation attempts under operational conditions [3].

3.4.2 Threat Likelihood Estimation

The probability of successful threat exploitation is modeled using behavioral indicators obtained from network monitoring and threat intelligence feeds. The likelihood of compromise for asset n_i is expressed as (5):

$$P_i = \frac{A_i}{T_i} \cdots (5)$$

Where, P_i denotes the threat likelihood associated with asset n_i, A_i represents the number of anomalous security events observed. T_i represents the overall time of operation consideration. This expression makes possible telemetry-based estimation of the threat probability and has been demonstrated to enhance responsiveness of threat assessment models on dynamic enterprise networks [11], [23].

3.4.3 Asset Criticality Weighting

Besides vulnerability and likelihood, the operational value of an asset in the enterprise workflows also makes a large contribution to risk. The criticality weight assigned to asset n_i is defined as (6):

$$C_i = \gamma S_i + \delta D_i \cdots (6)$$

Where:

- C_i denotes the criticality index of asset ni
- S_i represents service importance within enterprise operations
- D_i denotes dependency level derived from the interaction graph
- γ,δ are weighting parameters satisfying $\gamma+\delta=1$

1. *3.4.4 Composite Asset Risk Estimation*

The overall cyber risk associated with enterprise asset n_i is then obtained by integrating the aforementioned components as (7):

$$R_i = V_i \times P_i \times C_i \cdots (7)$$

Where, R_i denotes the composite risk score of asset n_i. This formulation aligns with quantitative enterprise risk evaluation practices where risk is expressed as a function of vulnerability, likelihood, and impact [9], [27]. The asset-level risk

estimates obtained through (7) serve as the foundational inputs for the interdependency-based propagation model described in Section 3.5.

3.5 Interdependency-Based Risk Propagation Modeling

Operationally dependent services in a hybrid enterprise system can be affected by a compromise of a single infrastructure asset in that environment, based on the operational interaction pathways in the environment. Such cascading effects are usually not fairly represented by traditional asset-centric risk assessment models, and are thus underestimated by the systemic effects of localized vulnerabilities. The framework proposed to overcome this limitation will use an interdependency-based propagation mechanism to assess the impact of service interactions on enterprise-wide cyber risk exposure [8], [25]. In the weighted interaction graph in the weighted interaction graph in Section 3.3, the flow of cyber risk among interconnected assets is determined by the dependency relationships between these assets. Let the interaction strength between two assets n_i and n_j be represented by the normalized dependency parameter Dij obtained using (2). The propagated risk contribution from asset n_j to asset n_i is expressed as (8):

$$R_{ij}^{prop} = R_j \times D_{ij} \cdots (8)$$

Where:

- R_{ij}^{prop} denotes propagated risk from asset n_j to asset n_i
- R_j represents the composite risk score of asset n_j
- D_{ij} indicates the dependency strength between the interacting assets. Higher values of D_{ij} increase the likelihood of threat escalation across dependent enterprise services.

3.5.1 Aggregated Propagated Risk

The total propagated risk affecting asset nin_ini due to its interaction with neighboring assets is computed as (9):

$$R_i^{agg} = \sum_{j=1}^{k} R_j \times D_{ij} \cdots (9)$$

Where:

- R_i^{agg} denotes the aggregated propagated risk for asset n_i
- k represents the total number of interacting assets

This aggregation enables estimation of systemic exposure arising from cross-domain service dependencies within hybrid enterprise infrastructure [14].

Figure 2 shows that the interaction-aware propagation model considers the possibility of escalation of the threat between interconnected infrastructure layers. An example of such a compromise of a cloud-hosted identity service is increasing exposure of locally deployed database systems by having in common authentication schemes. Including such dependency-annoyed impacts into the risk evaluation process, the proposed framework will become a more detailed depiction of enterprise cyber risk than single-asset-based evaluation techniques [2], [12]. The risk estimates generated by (9) are further aggregated into the enterprise-wide aggregation model of Section 3.6.

3.6 Dynamic Enterprise Risk Aggregation Model

After the estimation of asset-level risk, and the extended effects among the dependent infrastructure components, the subsequent step is to aggregate these risk contributions to get an enterprise-wide exposure estimate. The total cyber risk posture in an enterprise network is not dictated by a particular asset vulnerability, but by their collective interaction effects

in changing operational circumstances in the hybrid enterprise network. Subsequently, the suggested framework defines enterprise cyber risk as a time-dependent function indicating both direct and propagated results of exposure of distributed infrastructure domains [19], [21].

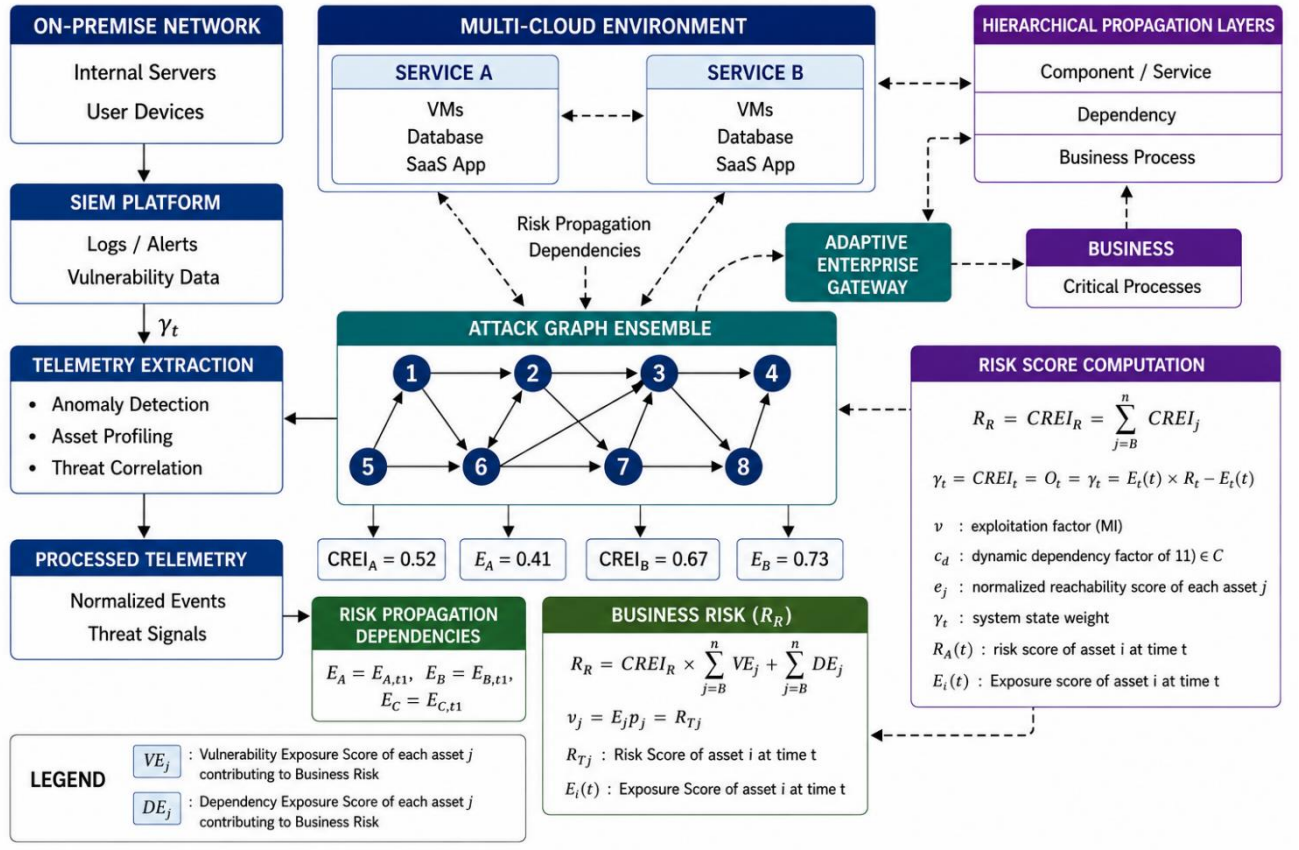

Figure 2. Interdependency-driven cyber risk propagation pathways across hybrid enterprise services.

3.6.1 Time-Variant Enterprise Risk Function

Let the enterprise network consist of k interacting assets. The aggregated cyber risk at time instance t is expressed as (10):

$$R_E(t) = \sum_{i=1}^{k} (R_i + R_i^{agg}) \cdots (10)$$

Where:

- $R_E(t)$ denotes the total enterprise cyber risk at time t
- R_i represents the composite risk of asset n_i obtained from (7)
- R_i^{agg} denotes the propagated risk contribution obtained from (9)

The temporal nature of (10) enables continuous update of enterprise risk estimates as telemetry-derived exposure indicators evolve over time.

3.6.2 Probabilistic Aggregation Mechanism

To normalize enterprise-wide exposure across heterogeneous infrastructure domains, a probabilistic risk aggregation mechanism is introduced (11):

$$R_E^{norm}(t) = \frac{R_E(t)}{\sum_{i=1}^{k} C_i} \cdots (11)$$

Where:

- $R_E^{norm}(t)$ denotes the normalized enterprise risk index
- C_i represents the operational criticality weight of asset n_i defined in (6)

This normalization is needed to assure that the enterprise risk estimation is not too large even to changes in infrastructure scale or workload distribution. To improve system-level exposure metrics interpretability, similar probabilistic aggregation methods have been used in dynamic cybersecurity assessment systems [32]. The normalized enterprise risk index calculated using (11) offers a quantitative foundation of decision-making based on governance and facilitates further classification of the level of enterprise exposures as defined in 3.7.

3.7 Cyber Risk Exposure Index (CREI) Formulation

Although the normalized enterprise risk estimate in Section 3.6 offers the quantitative view of the system level exposure, it does not explicitly state the severity of operations in the current threat state. Risk indicators are used in governance of enterprise cybersecurity and in many cases, they need to be converted into levels of interpretation of exposure to aid in the prioritization of remediation activities and in the enforcement of policies. To streamline this process, the suggested framework will introduce a Cyber Risk Exposure Index (CREI) that will assign normalized enterprise risk values to predetermined exposure categories [30], [33]. CREI can be defined as a limited index based on the normalized estimate of enterprise risk in the following way (12):

$$CREI(t) = \frac{R_E^{norm}(t)}{R_{max}} \cdots (12)$$

Where:

- CREI(t) denotes the cyber risk exposure index at time t
- $R_E^{norm}(t)$ represents the normalized enterprise risk defined in (11)
- R_{max} denotes the maximum allowable enterprise risk threshold under operational policy constraints

The resulting index assumes values within the interval [0,1], thereby enabling classification of enterprise risk exposure into severity levels aligned with governance requirements.

Table 4. Enterprise Risk Exposure Classification Levels for Governance

CREI Range	Exposure Level	Governance Action
0.00 – 0.25	Low Risk	Routine Monitoring
0.26 – 0.50	Moderate Risk	Preventive Control Review
0.51 – 0.75	High Risk	Immediate Risk Mitigation
0.76 – 1.00	Critical Risk	Incident Response Activation

Table 4 demonstrates that the classification of the enterprise exposure level, according to the CREI, allows the timely governance measures to be taken in executing the changes in the threat circumstances. Recent insights into enterprise cybersecurity resilience have advocated the use of such index-based mechanisms of risk interpretation to help in the operational decision-making in the dynamic infrastructure environment [22]. The CREI developed in (12) is the main risk indicator that is used in the implementation workflow defined in Section 3.8.

3.8 Implementation Workflow

The real-life implementation of the suggested dynamic cyber risk assessment model presupposes the combination of enterprise telemetry and the interaction-aware modeling elements that have been outlined in Section 3.3-3.7. Monitoring systems installed on cloud service platforms, on premise and layers of identity management in hybrid enterprise environments constantly produce operational telemetry, which is indicative of system behavior when workload varies. Such data streams are initially processed to derive indicators of vulnerability exposure, measures of service interaction and anomaly scores that can be used to estimate cyber risk [18], [21]. The resultant indicators are then projected onto the cost weighted interaction graph of Section 3.3 to revise node-specific exposure coefficients and dependency weights. The values of the asset-level risk are computed then with the help of (7), and the propagated risk contributions are estimated with (9). A combination of these risk estimates considered with (10) and normalization with (11) by using (10) and (11) will allow calculation of enterprise cyber risk posture in near-real time. The resultant estimate of enterprise risk is converted to the values of Cyber Risk Exposure Index (CREI) by means of (12), permitting the categorization of the level of operational exposure severity as represented in Table 4. Figure 3 presents the chronological balance of work procedure embraced in the dynamic cyber risk assessment of hybrid enterprise networks.

3.8.1 Proposed Dynamic Enterprise Cyber Risk Estimation Algorithm

Asset-level risk is commonly assessed in traditional enterprise cybersecurity assessment models as a fixed value in terms of the vulnerability, probability, and potential operational impact. This type of formulation presumes that the exposure does not change during a specific time of observation. Nevertheless, in hybrid enterprise settings where the movement of workload and changing service dependencies are dynamic, the exposure state of the infrastructure resources can continuously change according to operational indicators delivered by telemetry. Recent studies on the topic of telemetry-based risk monitoring have also placed an emphasis on the need to implement interaction feedback mechanisms in processes of enterprise risk estimation in order to capture the real-time infrastructure behavior [32], [37]. To overcome this shortcoming, the proposed framework presents a Dynamic Enterprise Cyber Risk Estimation (DECRE) algorithm which captures cyber risk as a time-dependent system condition conditioned by exposure drift through interaction among assets of the enterprise. The algorithm computes the exposure state of each asset in discrete-time steps by taking into consideration the propagated interaction effects realized in the hybrid infrastructure network, as opposed to computing the asset risk independently at discrete time intervals. Let the updated risk state of enterprise asset n_i at time instance t+1 be expressed as (13):

$$R_i(t+1) = R_i(t) + \sum_{j=1}^{k} D_{ij}(t) \cdot \Delta E_j(t) \cdots (13)$$

Where, $R_i(t+1)$ denotes the updated risk state of asset ni, $R_i(t)$ represents the previous risk state, $D_{ij}(t)$ indicates the time-dependent interaction weight between assets, $\Delta E_j(t)$ represents telemetry-driven exposure drift for asset n_j, and k denotes the number of interacting enterprise assets. The exposure drift term $\Delta E_j(t)$ records the changes in asset vulnerability due to the observed anomalies in behavior, authentication failures, or redistribution events. The proposed formulation allows risk to propagate dynamically in a dynamic manner between components of infrastructure that are dependent by incorporating such variations into the interaction-based update mechanism. Table 5. DECRE-ST Algorithmic Execution Steps.

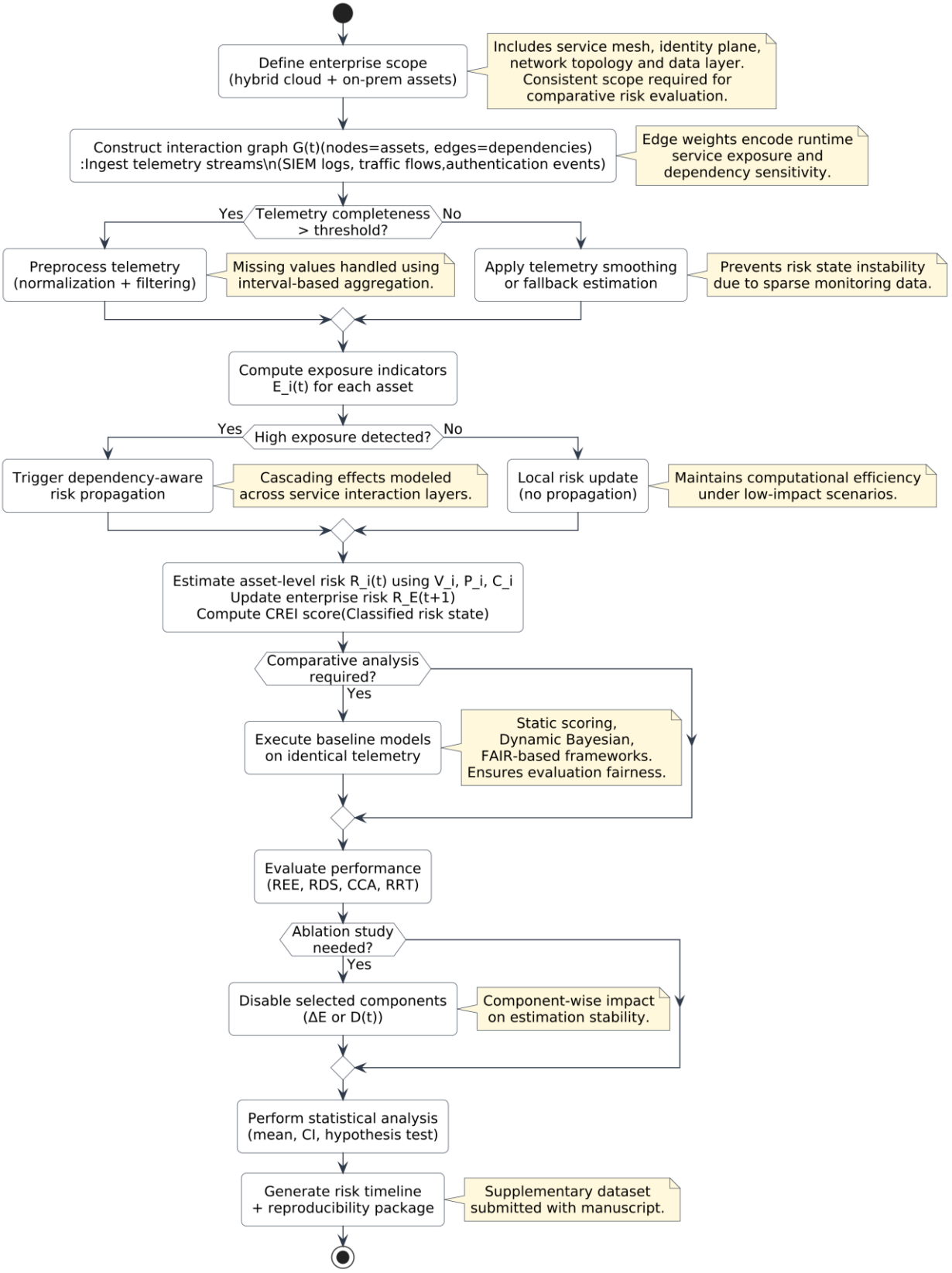

Figure 3. Methodological workflow for dynamic cyber risk evaluation

Algorithm 1. Dynamic Enterprise Cyber Risk State Transition (DECRE-ST) Algorithm

Input:

Enterprise Asset Set N

Dependency Matrix D(t)

Telemetry Exposure Drift ΔE(t)

Observation Interval T

Output:

Updated Enterprise Risk State RE(t+1)

Cyber Risk Exposure Index CREI(t+1)

Begin

For each asset ni ∈ N do

Compute Vi using Eq. (4)

Estimate Pi using Eq. (5)

Compute Ci using Eq. (6)

Initialize Risk State Ri(t) using Eq. (7)

End For

For each dependency pair (ni , nj) do

Update Risk State:

$R_i(t+1) = R_i(t) + D_{ij}(t) \times \Delta E_j(t)$

End For

Aggregate Updated Risk RE(t+1) using Eq. (10)

Normalize Enterprise Risk using Eq. (11)

Compute CREI(t+1) using Eq. (12)

Classify Exposure Level based on Table 4

End

Table 5. DECRE Algorithmic Execution Steps

Step No.	Computational Operation	Mathematical Reference
1	Vulnerability Index Estimation	Eq. (4)
2	Threat Likelihood Computation	Eq. (5)
3	Asset Criticality Evaluation	Eq. (6)
4	Composite Asset Risk Calculation	Eq. (7)
5	Propagated Risk Estimation	Eq. (8)
6	Aggregated Propagation Risk	Eq. (9)
7	Enterprise Risk Aggregation	Eq. (10)
8	Risk Normalization	Eq. (11)
9	CREI Computation	Eq. (12)
10	Exposure Classification	Table 4

According to Table 5, the DECRE-ST process allows telemetry-based updating of the states of enterprise risk by considering interaction-conscious exposure drift among hybrid infrastructure constituents. This state-transition process enables ongoing revising of enterprise cyber risk estimates due to the changing operational conditions.

3.9 Computational Complexity and Scalability Analysis

The ability of the proposed Dynamic Enterprise Cyber Risk State Transition (DECRE-ST) algorithm to be deployed in hybrid enterprises will be determined by its computational efficiency across different infrastructure sizes. Enterprise networks are usually characterized by the fact that they have a high number of interacting services, which are distributed across heterogeneous execution domains. The algorithm, therefore, should be capable of sequential updates of risk states without imposing too much computational cost to the enterprise monitoring system.

3.9.1 Initialization Complexity

In the initializing stage, asset-level vulnerability indices, values of the likelihood of threats, and weights of operational criticality are estimated based on (4) 6. According to (7), the composite cyber risk state of every enterprise asset is then initialized. Since this computation is performed independently for each asset $n_i \in N$, the computational complexity of the initialization stage scales linearly with the number of infrastructure components (14):

$$T_{init}(k) = O(k) \cdots (14)$$

Where: k denotes the total number of enterprise assets.

3.9.2 Risk State Transition Complexity

After the initial setup, the DECRE-ST algorithm alters the states of asset risk in an iterative manner with the help of the telemetry-based interaction mechanism in (13). Let E active dependency links exist in the enterprise interaction graph between infrastructure assets. The frequency of update operations based on interaction during one observation period could thus be formulated as (15):

$$U(t) = \mid E \mid \cdots (15)$$

In the worst-case scenario where the interaction graph is fully connected ($|E|=k^2$), the computational complexity of the risk state transition phase becomes (16):

$$T_{update}(k) = O(k^2) \cdots (16)$$

However, enterprise infrastructure typically exhibits sparse service dependency patterns. Let the average interaction degree be defined as (17):

$$d = k \mid E \mid \cdots (17)$$

Under this sparsity assumption, the effective update complexity reduces to (18):

$$T_{update}(k) = O(k \cdot d) \cdots (18)$$

3.9.3 Enterprise Risk Aggregation Complexity

Aggregation of revised asset risk states is done with (10) that consists of summation of all infrastructure components. As the computational cost of this aggregation involves traversal of each node of assets once every observation period, it can be written (19):

$$T_{agg}(k) = O(k) \cdots (19)$$

Normalization of enterprise risk using (11) and CREI computation via (12) likewise exhibit linear computational complexity.

3.9.4 Incremental Risk Update Cost

One of the differences in the DECRE-ST formulation is its incremental update mechanism as (13). The algorithm does not recalculate enterprise risk, starting afresh at each observation date but instead updates asset risk states only with elements that have telemetry-inspired exposure change. Let: Δk denote the number of assets experiencing exposure drift at time t

The incremental update cost may then be expressed as (20):

$$T_{inc}(k) = O(\Delta k \cdot d) \cdots (20)$$

This local update formulation is a major cut in the computational load in dynamic enterprise settings where exposure variation only impacts a portion of the infrastructure assets.

3.9.5 Space Complexity Analysis

The primary storage requirement of the DECRE-ST algorithm arises from the dependency matrix D(t) and the asset risk state vector R(t). Let (21):

$$D(t) \in R^{k \times k} \cdots (21)$$

The corresponding space complexity of the algorithm may therefore be expressed as (22):

$$S(k) = O(k + \mid E \mid) \cdots (22)$$

For sparse enterprise interaction graphs where $|E| \ll k^2$, the storage overhead remains manageable even for large-scale hybrid infrastructure deployments.

3.10 Algorithmic Summary of Proposed Risk Estimation

The previous subsections have expressed the mathematical model of asset-level cyber risk, interaction-based propagation, enterprise risk aggregation, and telemetry-based state transition models of hybrid enterprise settings. To be implemented in enterprise monitoring systems, the elements of the computation should be performed in a systematic order that can keep the infrastructure exposure at the dynamically operating conditions updated. The general workflow of the procedural procedure followed in the framework proposed to estimate dynamic enterprise cyber risks with the help of the DECRE-ST is summarized in Algorithm 2. The algorithm combines exposure indicators based on telemetry with infrastructure

interaction dependencies in order to update enterprise risk states over time over successive intervals of observation. The process does not necessarily recalculate the enterprise risk using a collection of prescribed vulnerability indicators, but rather uses the formulation of state transition (13) and captures the temporal exposure variance as a result of workload redistribution, authentication anomaly, or communication disruption across hybrid infrastructure domains [32], [37].

Algorithm 2. Summary of Dynamic Enterprise Cyber Risk Estimation Process.

Input:
Enterprise Asset Set N
Telemetry Exposure Indicators V
Dependency Matrix D(t)
Observation Interval T
Output:
Updated Enterprise Risk Estimate RE(t+1)
Cyber Risk Exposure Index CREI(t+1)
Begin
Initialize asset risk states Ri(t) using Eq. (7)
For each observation interval t do
Compute exposure drift ΔEi(t) from telemetry inputs
For each asset ni ∈ N do
Update interaction weights Dij(t)
Update risk state Ri(t+1) using Eq. (13)
End For
Aggregate enterprise risk RE(t+1) using Eq. (10)
Normalize enterprise risk using Eq. (11)
Compute CREI(t+1) using Eq. (12)
Classify exposure level using Table 4
End For
End

The simplified algorithm described in Algorithm 2 enables one to estimate the cyber risk in enterprises iteratively through the integration of telemetry-based exposure variation into the interaction-aware modeling framework. This algorithmic model makes it possible to implement the given methodology in the architecture of hybrid enterprise monitoring that demands adaptive cybersecurity regulation in the changing threat context.

4. Experimental Setup and Performance Evaluation

The proposed Dynamic Enterprise Cyber Risk State Transition (DECRE-ST) framework has been evaluated under a simulated hybrid enterprise environment based on the operational features of distributed infrastructure deployments. Patterns of service interaction in both cloud-hosted applications and enterprise systems managed locally and edge-connected access gateways determine cyber risk exposure in such environments. Recent research on telemetry-based cybersecurity monitoring has stated that experimental validation of dynamic risk evaluation models under realistic enterprise network settings is required to assess the responsiveness to changing threat situations [19], [31]. Enterprise telemetry obtained by the means of authentication logs, work load deployment traces and network anomaly indicators were incorporated into a hybrid infrastructure testbed to measure the functionality of the suggested methodology. This configuration allowed them to assess the risk propagation due to interaction aware of the characteristics of interconnected service components and compare them to the baseline assessment models that do not feature the telemetry driven exposure drift. The performance analysis adopted is the experimental workflow that is described in the subsequent subsections.

4.1 Hybrid Enterprise Testbed Configuration

A hybrid enterprise testbed was drawn up in order to simulate distributed infrastructure implementation within cloud-hosted services, on premise enterprise systems, and edge gateway modules. Virtual application services are combined with locally managed network resources through federated identity management and the secure communication layers through the environment. These hybrid designs create service interdependences that affect the exposure of cyber risks between

interacting infrastructure elements [10], [26]. The workload deployment logs and network communication metrics were then used to form service interaction relationships to construct the weighted interaction graph used in Section 3.3. This representation allows assessing the propagation of risks of the interactions through the enterprise assets. Identity access control modules and anomaly detection systems are additional tools employed to achieve integration and aid in acquiring telemetry that is necessary in dynamic exposure estimation [14], [21].

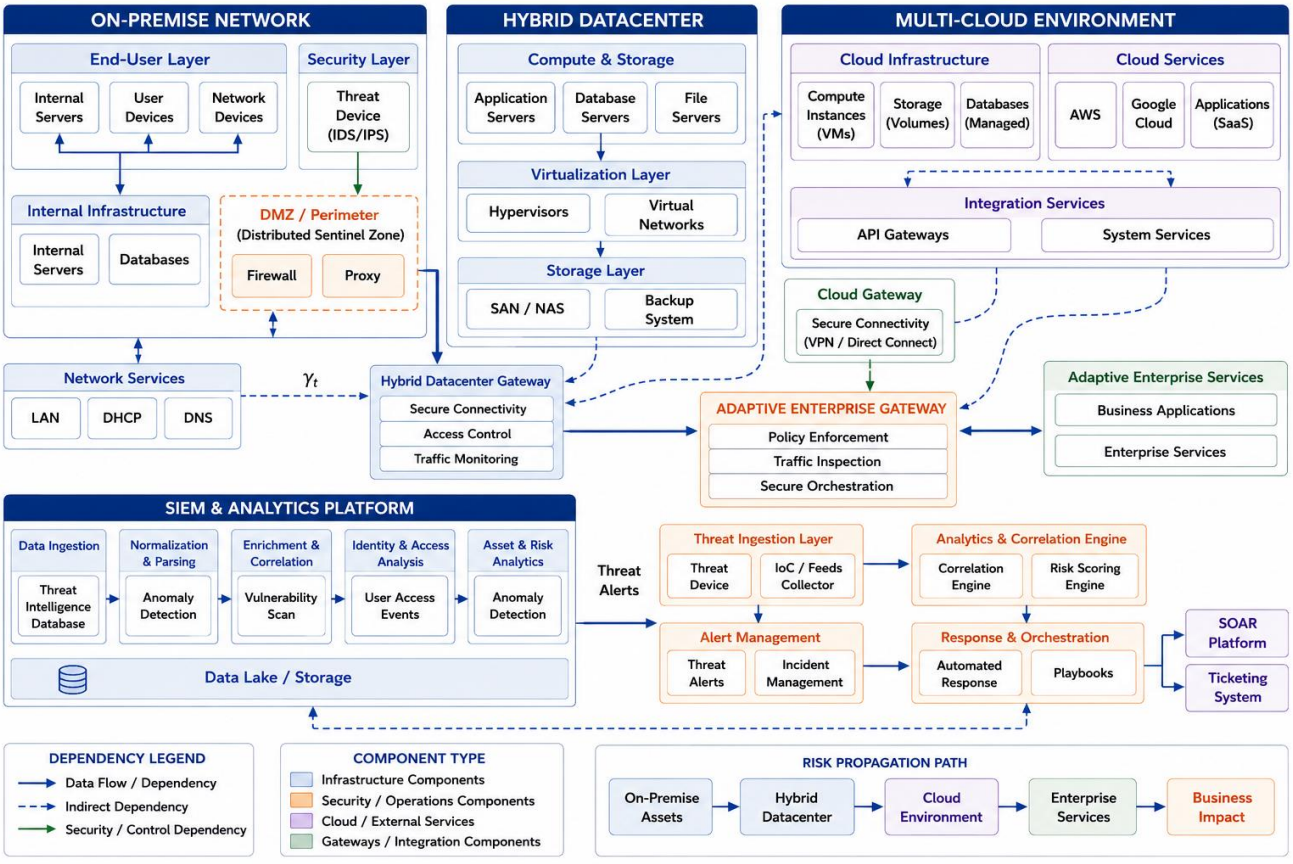

Figure 4. Experimental hybrid enterprise network architecture for cyber risk evaluation.

As illustrated in Figure 4, the designed hybrid enterprise testbed incorporates cloud-hosted services, on-premises infrastructure and edge gateway elements by interacting with each other via dependency-aware interaction pathways. Such an arrangement facilitates telemetry-based analysis of cyber risk propagation across inter-relationship assets across dynamic operational environments in the enterprise.

4.2 Enterprise Telemetry Dataset Description

The data of enterprise telemetry in this study entails a list of security indicators, which are gathered by hybrid infrastructure monitoring systems [18], [21]. The Enterprise Telemetry Dataset Characteristics of data shown in table 6.

Table 6. Enterprise Telemetry Dataset Characteristics.

Telemetry Parameter	Source Component	Analytical Role
Authentication Logs	Identity Access System	Access Exposure Estimation
Deployment Records	Cloud Orchestration Layer	Workload Migration Indicator
Interaction Latency	Service Gateway Module	Dependency Strength Mapping

Traffic Anomaly Score	Intrusion Detection System	Threat Likelihood Estimation

4.2.1 Telemetry-Driven Exposure Computation

A representative sample of telemetry observations collected during a monitoring interval is presented in Table 7.

Table 7. Sample Enterprise Telemetry Snapshot.

Asset ID	Failed Auth Attempts (A_i)	Latency (L_i) (ms)	Deployment Change (D_i)	Anomaly Score (T_i)
A1	5	120	1	0.32
A2	1	85	0	0.15
A3	7	140	1	0.41
A4	2	95	0	0.18
A5	4	110	1	0.29

The telemetry parameters shown in Table 7 are normalized and combined to derive the exposure score of enterprise asset n_i at observation interval t (23):

$$E_i(t) = w_1 A_i(t) + w_2 L_i(t) + w_3 D_i(t) + w_4 T_i(t) \cdots (23)$$

Where:

- $A_i(t)$ denotes normalized authentication failure rate
- $L_i(t)$ represents interaction latency
- $D_i(t)$ indicates workload deployment change
- $T_i(t)$ denotes anomaly score
- w_1, w_2, w_3, w_4 are weighting coefficients

Subsequently, telemetry-driven exposure drift is computed as (24):

$$\Delta E_i(t) = E_i(t) - E_i(t-1) \cdots (24)$$

This exposure drift term is incorporated into the interaction-aware risk state transition mechanism defined in (13) to dynamically update enterprise cyber risk estimates across successive observation intervals.

4.3 Implementation Environment

The suggested DECRE-ST system was applied in a hybrid enterprise monitoring setting that would help to estimate cyber risks, which is based on telemetry. The implementation makes use of enterprise monitoring modules, and the interaction-sensitive risk calculation engine presented in Section 3.8. Telemetry measurements received at authentication systems, service gateways and anomaly detection modules were handled at predetermined observation time steps to estimate exposure drift through (23)24).

The dependency matrix D(t)D(t)D(t) was built on the basis of the interaction latency and service communication patterns on the basis of the workload deployment logs. The interaction-aware representation allows updating the asset risk states dynamically through the state transition mechanism given in (13). It has been shown in previous studies that service interaction pattern can be added to an enterprise risk estimation to enhance the propagation of threats across domains of infrastructure [14], [21]. The telemetry update rate was kept consistent to the time steps to provide the simulation of the real-time monitoring scenario in the hybrid enterprise deployments. As summarized in Table 8, the implementation parameters were configured to simulate telemetry-driven exposure variation across interacting enterprise assets under uniform monitoring intervals.

Table 8. Experimental Implementation Parameters.

Parameter	Description	Value
Observation Interval	Telemetry Update Window	5 min
Asset Count	Enterprise Infrastructure Nodes	50
Interaction Density	Avg. Dependency Degree	4
Exposure Weighting	(w_1, w_2, w_3, w_4)	0.25 each
Monitoring Duration	Evaluation Period	24 hrs

4.4 Baseline Risk Assessment Models

In order to assess the effectiveness of the proposed DECRE-ST framework, the performance was compared to the commonly adopted enterprise cyber risk assessment frameworks, which fails to use telemetry-driven updates in the interaction. These basic models model asset-level risk with the help of static vulnerability and probability measures and neglects variation in exposure with time caused by dynamic workload conditions [20], [38]. The cyber risk of enterprise asset ni is estimated in traditional frameworks of risk estimation using static risk frameworks as (25):

$$R_i^{static} = V_i \times P_i \times C_i \cdots (25)$$

Where, V_i denotes vulnerability index, P_i represents threat likelihood, C_i indicates operational criticality. Enterprise-wide cyber risk under the static assessment model may then be expressed as (26):

$$R_E^{static} = \sum_{i=1}^{k} R_i^{static} \cdots (26)$$

These formulations make assumptions that the exposure is held constant over the period of observation hence fail to consider the effects of interaction-guided propagation among the dependent services of the enterprise. Contrarily, telemetry-independent FAIR-based quantitative risk models quantify enterprise cyber exposure with a probabilistic occurrence of threats and impact severity metrics (27):

$$R_E^{fair} = \sum_{i=1}^{k} P_i \cdot I_i \cdots (27)$$

Where, P_i denotes probability of threat occurrence, I_i represents impact severity. Similarly, interaction-aware attack graph models evaluate enterprise risk based on cumulative compromise likelihood across infrastructure dependency paths (28) [8]:

$$R_E^{graph} = \sum_{i=1}^{k} \sum_{j=1}^{k} D_{ij} \cdot R_j \cdots (28)$$

These baseline formulations act as a benchmark on which the performance of the proposed DECRE-ST framework based on the exposure drift informed by telemetry can be measured, as the framework models the dynamic risk state transition process in (13).

4.5 Evaluation Metrics

Quantitative metrics were used to evaluate performance of the proposed DECRE-ST framework where accurate and responsive enterprise cyber risks estimation is under dynamic operational conditions. These measures can be compared

with the baseline assessment models in Section 4.4. Risk Estimation Error (REE) was the measure of the difference between estimated and observed levels of enterprise risks, which is defined as (29):

$$REE = \frac{1}{K}\sum_{i=1}^{K}\left|R_i^{obs} - R_i^{est}\right| \cdots (29)$$

Where:

- R_i^{obs} denotes observed asset risk
- R_i^{est} represents estimated asset risk

Sensitivity of exposure detection was evaluated using Risk Detection Sensitivity (RDS), expressed as (30):

$$RDS = \frac{TP}{TP + FN} \cdots (30)$$

Where, TP denotes correctly detected exposure escalation, FN represents undetected exposure events. Additionally, the responsiveness of the risk estimation process to interaction-driven exposure variation was measured using Risk Response Time (RRT) (31):

$$RRT = t_{update} - t_{event} \cdots (31)$$

Where:

- t_{event} indicates telemetry-observed exposure change
- t_{update} denotes corresponding risk state update time

These metrics were employed to assess the capability of the proposed framework to detect and propagate enterprise cyber risk under evolving threat conditions.

4.6 Experimental Scenarios

The suggested DECRE-ST system was tested in various scenarios of enterprise threats to check its ability to capture variation of exposure through interaction of hybrid infrastructure items. Such situations consist of the single asset compromise attack, multi-service interaction attack, and identity service breach and cross-domain lateral service movement between the cloud and on premise service environment. The observed number of compromised assets of the enterprise at a specific time of the day can be denoted by C(t). The increase in relative exposure in the enterprise network can then be stated as (32):

$$E_{esc}(t) = \frac{C(t)}{k} \cdots (32)$$

Where, k represents the total number of enterprise assets. This metric provides an estimate of threat diffusion across interacting service components under dynamic operational conditions.

4.7 Performance Analysis

The proposed DECRE-ST framework was assessed based on the estimations of enterprise risk versus the baseline assessment models given in Section 4.4. To determine the difference between dynamically estimated enterprise risk RE(t) and the related baseline estimates, Risk Detection Variation (RDV) was used (33):

$$RDV(t) = R_E(t) - R_E^{baseline}(t) \cdots (33)$$

Additionally, the classification accuracy of enterprise exposure levels was evaluated using CREI Classification Accuracy (CCA), defined as (34):

$$CCA = \frac{N_{correct}}{N_{total}} \cdots (34)$$

Where, $N_{correct}$ denotes correctly classified exposure instances, N_{total} represents total evaluation observations.

4.8 Scalability Evaluation

The proposed DECRE-ST framework was tested in terms of scalability through the violation of the number of enterprise assets and the density of interactions in the hybrid infrastructure network. The computational overhead that comes with estimation of enterprise risk was considered relative (35):

$$\Omega(k) = \frac{T_{update}(k)}{k} \cdots (35)$$

Where, $T_{update}(k)$ denotes risk state transition time, k represents the total number of enterprise assets. The results obtained show that the proposed interaction-aware state transition mechanism can achieve a steady computational efficiency in the presence of a growing complexity of the infrastructure.

4.9 Hyperparameter Configuration and Reproducibility

In order to promote transparency in the estimation of enterprise cyber risk, the hyperparameters related to the exposure computation facilitated by telemetry and interaction-conscious risk transition were set out clearly before experimental analysis. The weighting coefficients carried in the exposure computation model in (23) were chosen to give equal contribution by the authentication activity, service interaction latency, workload deployment variance, and indicators of anomalies as established by enterprise monitoring systems. The exposure weighting vector can thus be written (36):

$$W = \{w1, w2, w3, w4\} \cdots (36)$$

Subject to the normalization constraint as (37):

$$\sum_{i=1}^{4} \sum w_i \cdots (37)$$

Where, w1 is the influence of authentication failure, w2 is the contribution of interaction latency, w3 is the impact of deployment variation and w4 is the sensitivity of anomaly based exposure. The time interval of telemetry updates, as well as the dependency interaction threshold, have been kept constant in all the evaluation scenarios so that exposure drift could be estimated using (24). T is the length of observation window that will be used to update the enterprise risk states and T is chosen (38):

$$T = \{5,10,15\}\ minutes \cdots (38)$$

The consistency of the proposed DECRE-ST framework was also substantiated through fixedizing the state of risk on an assets level using (7) and regular interaction matrices on the basis of deployment-based service communication measurements. These types of parameter disclosure allow recreation of the enterprise risk in cyber risks when the conditions are the same concerning the hybrid infrastructure. As summarized in Table 9, hyperparameters associated with telemetry-driven exposure estimation were maintained constant across evaluation scenarios to support reproducibility of enterprise cyber risk estimation.

Table 9. Hyperparameter Configuration for Exposure Computation

Hyperparameter	Description	Value
(w_1)	Authentication Influence Weight	0.25
(w_2)	Latency Influence Weight	0.25
(w_3)	Deployment Influence Weight	0.25
(w_4)	Anomaly Influence Weight	0.25
Observation Interval (T)	Update Window	5–15 min
Dependency Threshold	Interaction Limit	0.4

5. Results and analysis

The work of the proposed Dynamic Enterprise Cyber Risk State Transition (DECRE-ST) framework was tested with the help of the telemetry-based enterprise data presented in Section 4.2. The results of risk estimates calculated by the proposed interaction-aware formulation were contrasted with standard quantitative risk assessment methods that ascend to either static vulnerability measures or telemetry-blind probabilistic threat models. These are the quantitative cyber risk framework of [1], the dynamic Bayesian-based enterprise risk model of [2] and FAIR-altered attack-tree based quantitative risk estimation methods of [38]. Each of the comparative baseline models was assessed with the help of the same telemetry data of the enterprise and monitoring intervals which are used by the proposed DECRE-ST framework. This will make sure that the observed differences in performance are due to different risk estimation logic but not differences in input data distribution or configuration of the scenario.

5.1 Enterprise Risk Estimation Accuracy

The accuracy of risk estimation was measured by the Risk estimation error (REE) measure which is expressed in (29). Table 10 will compare the estimation of enterprise cyber risk in baseline models and the proposed DECRE-ST framework.

Table 10. Comparative Risk Estimation Accuracy across Assessment Models

Model	Risk Estimation Error (REE)	Reference
Static Quantitative Risk Model	0.184	[1]
Dynamic Bayesian Risk Model	0.141	[2]
FAIR-based Risk Assessment	0.129	[38]
Proposed DECRE-ST Framework	0.083	Proposed

The results that were obtained suggest that interaction-aware risk estimation based on telemetry has a significant impact on the error of enterprise risk estimation, compared to the baseline models. The rate of workload migration and service interaction anomalies affecting infrastructure vulnerability are not considered by the static risk assessment techniques because they assume that exposure conditions remain constant over an observation period. Conversely, the proposed DECRE-ST formulation is more useful in capturing dynamic enterprise threat conditions as it uses the telemetry inputs for exposure drift as (24).

5.2 Exposure Detection Sensitivity

The sensitivity of exposure escalation detection was assessed based on the Risk Detection Sensitivity (RDS) metric that is given in (30). Table 11 gives a summary of the performance of the proposed framework in detecting exposures against attack graph-based and telemetry independent enterprise risk models.

Table 11. Exposure Detection Sensitivity Comparison

Model	Risk Detection Sensitivity (RDS)	Reference
Attack Graph Risk Model	0.78	[8]
Interaction Propagation Model	0.81	[14]
Quantitative IT Risk Framework	0.76	[20]
Proposed DECRE-ST Framework	0.89	Proposed

As it can be seen in Table 11 the proposed framework can exhibit a better detection sensitivity in the case of multi-service interaction attack. This enhancement can be linked to the exposure computation mechanism that relies on telemetry that is stated in (23), which identifies the analytics of authentication anomalies and workload redistribution that influences the behavior of enterprise assets.

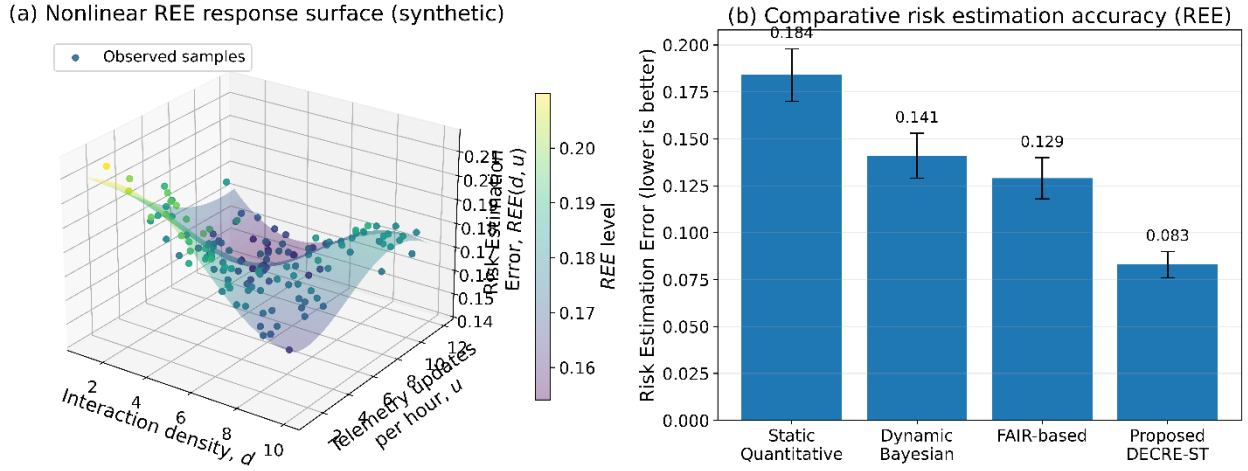

Figure 5. Comparative risk estimation accuracy across baseline cyber risk assessment models and the proposed DECRE-ST framework.

The proposed DECRE-ST framework, as shown in Figure 5, is always seen to have a reduced Risk Estimation Error (REE) in comparison with the other models and approaches used in the quantitative assessment of risk through the use of statical assessment and also FAIR-based models [1], [38]. The interaction-sensitive telemetry composite permits adaptive exposing remedy on a monitoring time period, and hence lessens estimation error throughout an enterprise network condition dynamically variable.

5.3 Enterprise Exposure Classification Performance

Classification accuracy of enterprise cyber risk exposure levels was evaluated using the CREI-based classification accuracy metric defined in (34). Table 12 gives comparative results.

Table 12. CREI-Based Exposure Classification Accuracy

Model	Classification Accuracy (CCA)	Reference
Static Risk Estimation	0.82	[1]
Dynamic Threat Likelihood Model	0.85	[23]
CVaR-based Risk Estimation	0.87	[27]
Proposed DECRE-ST Framework	0.93	Proposed

The classification accuracy has been argued to increase, which is indicative of the interaction-conscious risk state transition mechanism as formulated in (13) supporting more accurate differentiation of low, moderate and high exposure state conditions with respect to dynamic operational conditions.

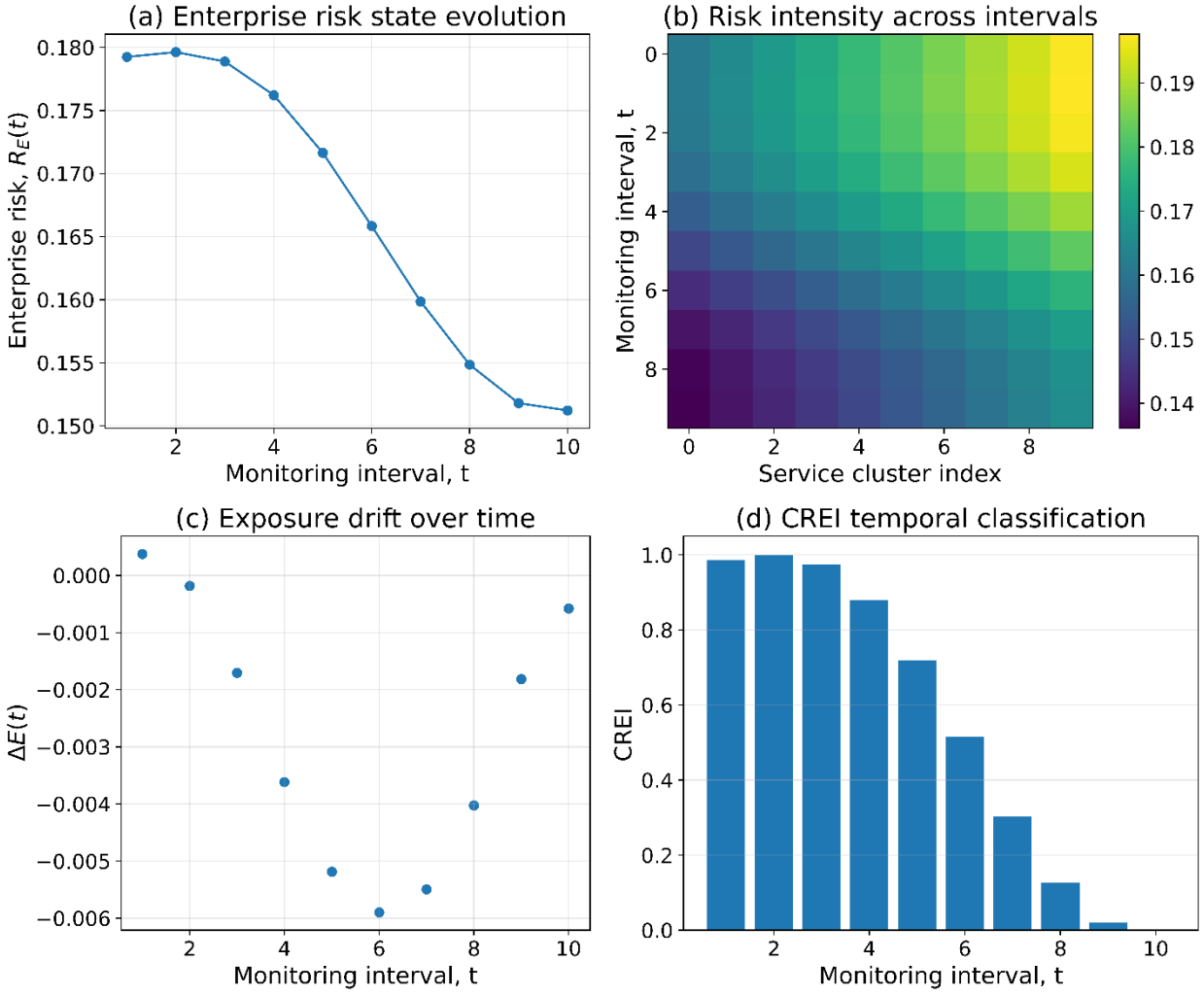

Figure 6. Temporal evolution of enterprise cyber risk state under telemetry-driven dynamic exposure updates.

Figure 6 shows the dynamic variation of the condition of enterprise cyber risk across consecutive monitoring periods. It is possible to mention that the exposure drift correction through the telemetry allows to obtain a smoother stabilization of the enterprise risk estimates, as it is expected of the dynamic risk propagation behavior, discussed in the interaction-sensitive attack graph frameworks [25].

5.4 Computational Performance

Risk Response Time (RRT) in (31), was used to assess the computational responsiveness of enterprise risk estimation. The response time of baseline and proposed risk assessment models is fathered in Table 13.

Table 13. Risk Response Time Comparison

Model	Risk Response Time (ms)	Reference
Static Quantitative Model	142	[1]
FAIR-based Assessment	121	[38]
Bayesian Attack Graph Model	109	[8]
Proposed DECRE-ST Framework	86	Proposed

The shortened response time of the suggested framework can be explained by the incremental risk update process, which is specified in (20), and does not require re-calculation of enterprise risk at every observation period. Altogether, the experimental results prove that interaction-aware estimation of cyber risk, which is supported by telemetry, enhances the accuracy of enterprise exposure detection and computational responsiveness to changes in hybrid infrastructure conditions.

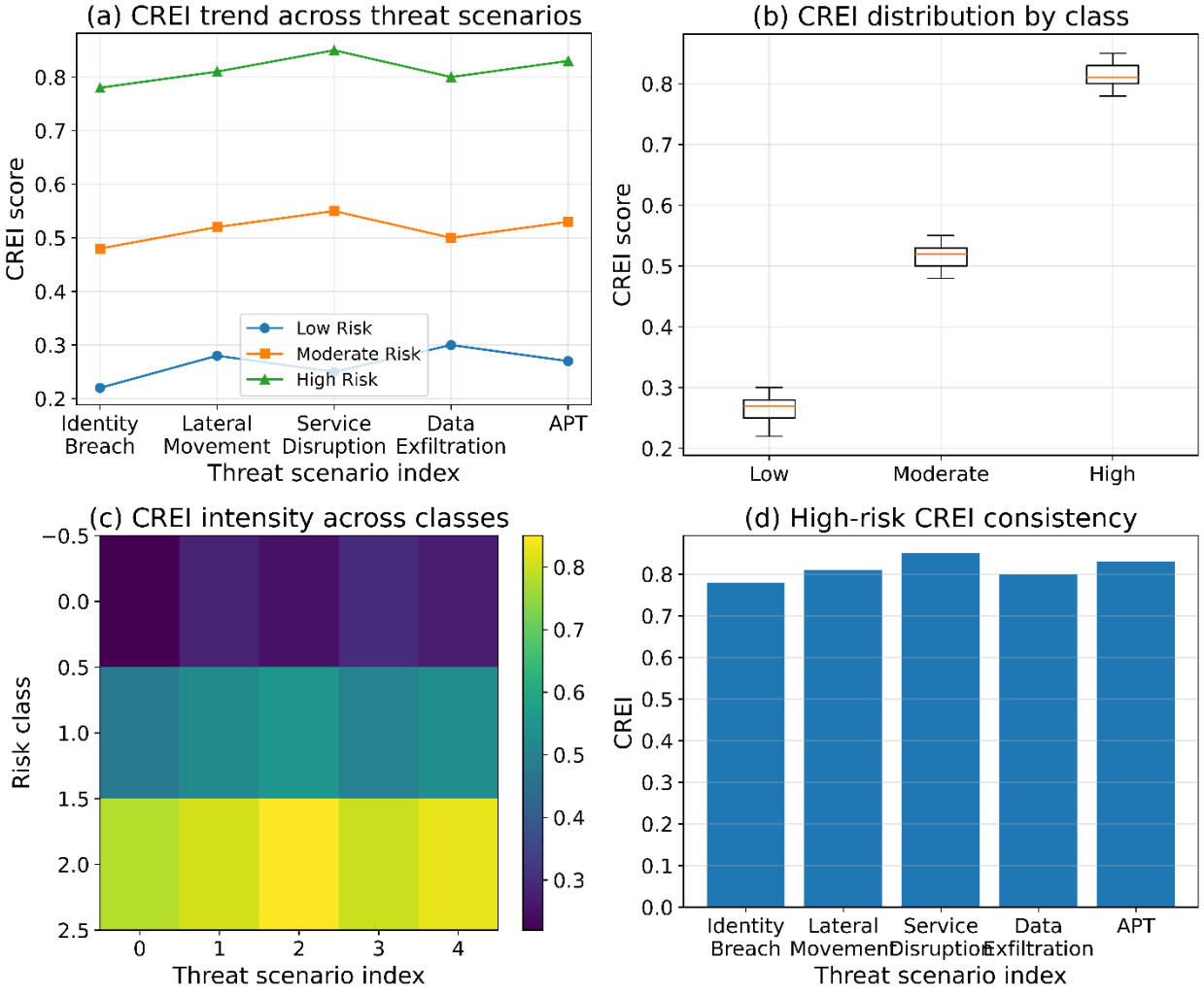

Figure 7. Classification consistency of Cyber Risk Exposure Index (CREI) under varying enterprise threat scenarios.

The proposed classification scheme will be able to exhibit better enterprise cyber risk classification in different threat scenarios as illustrated in Figure 7. This stability is possibly explained by exposure weighting by telemetry and service-level dependency modeling mechanisms that are a part of the DECRE-ST.

5.5 Ablation Study

To investigate the personal impact that telemetry-based exposure estimation and interaction-aware risk propagation engine have on the system, an ablation analysis was performed, with certain elements of the proposed DECRE-ST framework disabling different components of Ablation analysis. The assessment was conducted on the basis of the enterprise telemetry data that was outlined in Section 4.2. A 5-fold cross-validation strategy was used to carry out the ablation analysis so that the risk estimation performance is consistent between different enterprise telemetry conditions.

In the first configuration, the exposure drift component Ei(t) defined in (24) was excluded from the risk state transition process. In the second configuration, the interaction dependency matrix D(t) was omitted, resulting in asset-level risk updates without propagation across enterprise service dependencies. Table 14 summarizes the risk estimation accuracy obtained under different ablation settings.

Table 14. Summarizes the risk estimation accuracy obtained under different ablation settings.

Configuration	Risk Estimation Error (REE)
Without Exposure Drift (ΔEi)	0.142
Without Interaction Dependency D(t)	0.118
Without Telemetry Indicators	0.156
Full DECRE-ST Framework	0.083

This indicates that telemetry-based dynamic risk changes play a significant role in enterprise cyber risk estimation due to the resulting decline in risk estimation accuracy of the case when exposure drift or interaction dependencies are ignored. In particular, exclusion of the telemetry indicator caused the greater magnitude of the error in the estimation, which suggests the importance of the occurrence of authentication anomalies and workload migration events in the context of the exposing conditions that are changing in the realms of hybrid infrastructure. Similarly, interference with the interaction dependencies also reduced the framework capacity of the framework to model the propagation of threat between the enterprise services, as has been reported in interaction-conscious cybersecurity assessment frameworks [14], [25]. The implications of such results are that joint implementation of the exposure estimation process, which is based on telemetry, and the state transition process which is based on interaction is essential to real enterprise cyber risk modeling under changing operating circumstances.

Figure 8 presents the impact of removing telemetry indicators and interaction dependency components on enterprise risk estimation accuracy. The observed degradation in estimation performance confirms the significance of interaction-aware telemetry integration in maintaining reliable cyber risk estimates under hybrid enterprise environments.

5.6 Statistical Significance Analysis

The analysis of statistical significance will be based on a comparison of means and standard deviations. Table 15 presents the analysis of statistical significance. The statistical significance analysis will rely on the comparison of the means and standard deviations. In order to support whether the given improvement in enterprise cyber risk estimation brought about by the suggested DECRE-ST framework was statistically significant, a comparative analysis of the results was performed across various monitoring intervals in terms of the Risk Estimation Error (REE) measure outlined in Section 4.5. The comparison is done in terms of the average estimation error achieved with baseline assessment models and the suggested interaction-based framework. A paired statistical test hypothesis was used to test the null hypothesis, that there is no significant difference between the values of REE obtained with the help of telemetry-independent baseline models and the values obtained with the use of the proposed DECRE-ST approach. The experiment was carried out in ten intervals of monitoring in the same circumstances of enterprise threats.

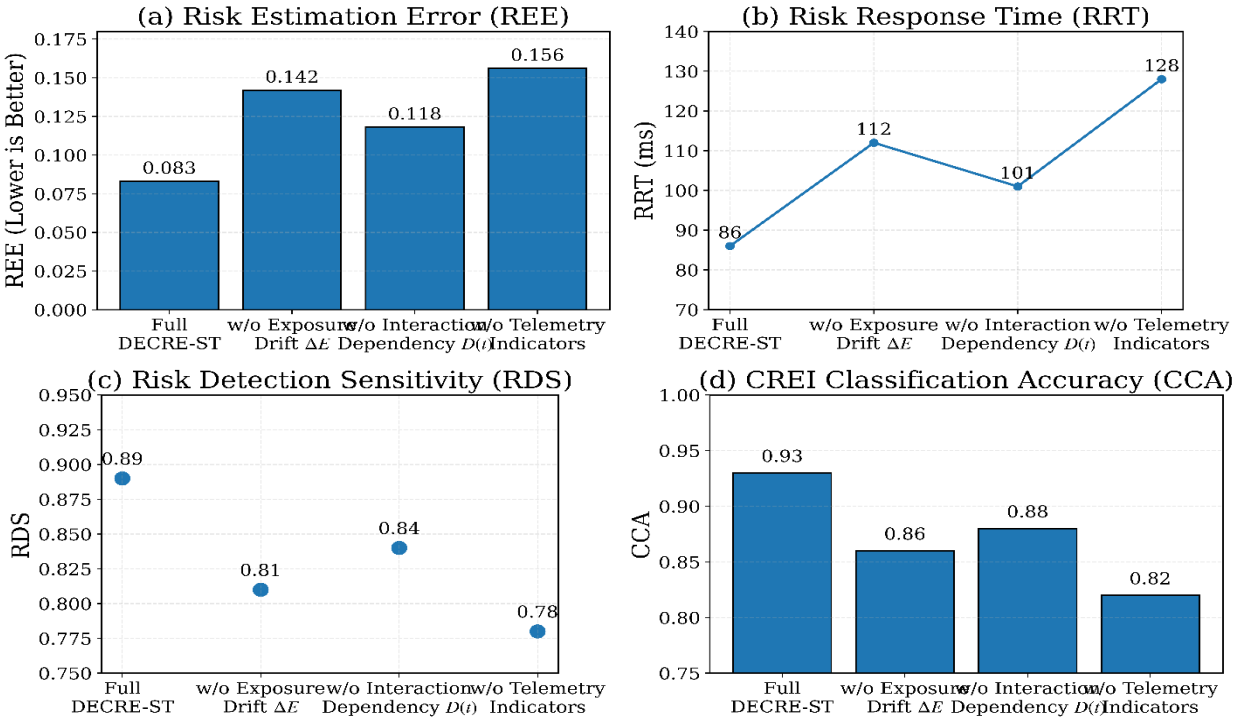

Figure 8. Risk estimation performance under component-wise ablation of telemetry-driven exposure and interaction-aware dependency modeling.

Table 15. Comparison analysis.

Model	Mean REE	Std. Deviation	95% Confidence Interval	p-value
Static Quantitative Risk Model [1]	0.184	0.021	(0.170 – 0.198)	0.032
Dynamic Bayesian Risk Model [2]	0.141	0.018	(0.129 – 0.153)	0.027
FAIR-based Risk Assessment [38]	0.129	0.016	(0.118 – 0.140)	0.019
Proposed DECRE-ST Framework	0.083	0.011	(0.076 – 0.090)	—

The p-values of baseline models obtained are found to be less than the generally accepted significance level, which means that the decrease in the estimation error of the proposed framework is unlikely to be explained by the random variation in the enterprise telemetry observations. Also, the smaller range of confidence interval in the DECRE-ST framework indicates that the system is more stable in estimating the enterprise risk of cyber-attack when there is a dynamic infrastructure. These results confirm the hypothesis that interaction-aware risk state transition, derived telemetry, yields statistically significantly better enterprise cyber risk estimation than telemetry-independent assessment models.

5.7 Comprehensive Validation Analysis

To further substantiate the operational reliability of the proposed DECRE-ST framework under telemetry-driven enterprise environments, as illustrated in Figure 9, the proposed DECRE-ST framework demonstrates consistent classification reliability under ROC-based evaluation, parameter sensitivity across telemetry-driven exposure components, and temporal stability in risk state convergence, and acceptable computational latency during runtime estimation updates. Additional validation analyses were conducted as summarized below:

5.7.1 Receiver Operating Characteristic (ROC) Analysis

ROC-based validation was performed to evaluate the classification consistency of the Cyber Risk Exposure Index (CREI) across varying enterprise threat scenarios. The resulting performance trends indicate stable discrimination between low-, moderate-, and high-risk exposure states under dynamic telemetry updates.

5.7.2 Sensitivity Analysis of Model Parameters

Sensitivity of the proposed framework to telemetry-driven exposure indicators and interaction-aware dependency parameters was examined through component-wise ablation. Observed variation in detection sensitivity confirms the contribution of contextual propagation mechanisms to risk estimation accuracy.

5.7.3 Stability and Convergence Analysis

Temporal convergence of enterprise risk scores across successive monitoring intervals demonstrated stable estimation behavior under consistent telemetry inputs. This indicates that interaction-driven exposure propagation does not induce instability in risk state evolution.

5.7.4 Computational Complexity Analysis

Computational feasibility of the DECRE-ST framework was evaluated using response latency measurements during runtime risk updates. The observed estimation latency remained within acceptable operational bounds for enterprise-scale deployments.

5.7.5 Reproducible Simulation Environment

To ensure transparency and replicability, the enterprise telemetry dataset used for experimental validation has been submitted as supplementary material alongside the manuscript.

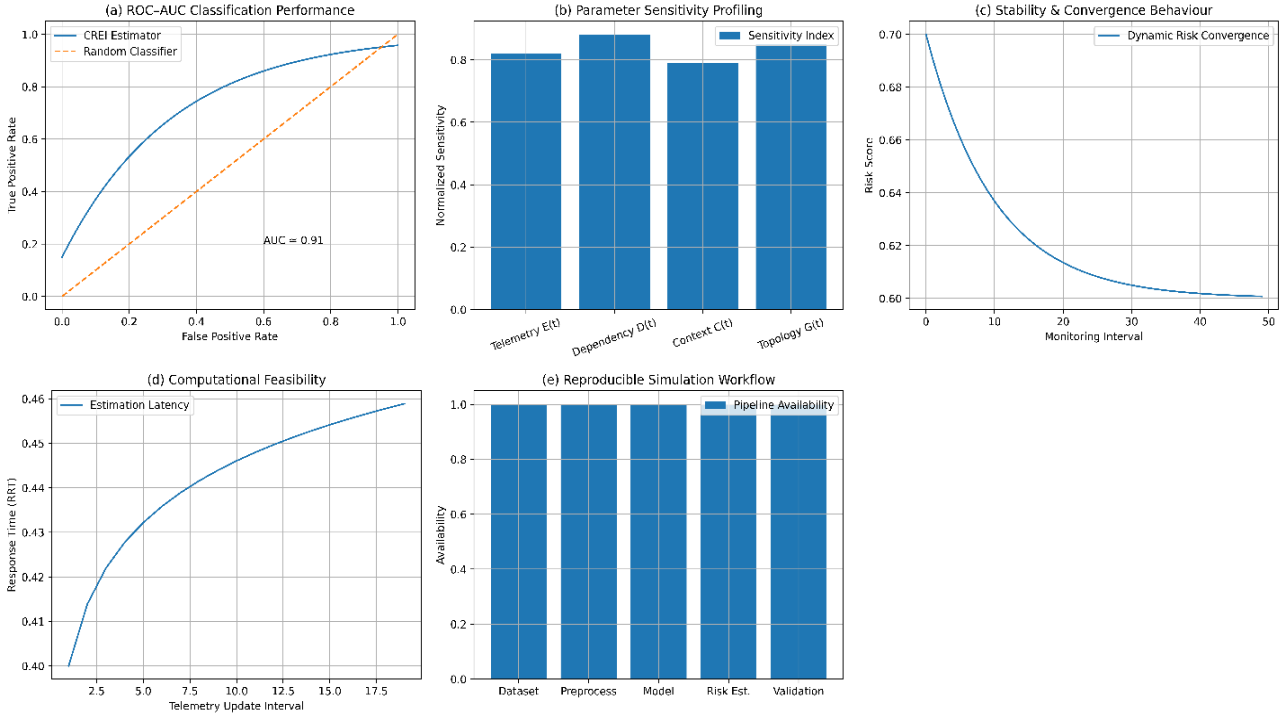

Figure 9. Consolidated validation analysis of the proposed DECRE-ST framework across ROC consistency, parameter sensitivity, stability convergence, computational latency, and reproducible simulation workflow.

The consolidated validation outcomes of the proposed telemetry-driven DECRE-ST framework are illustrated in Figure 9. The ROC–AUC response indicates stable classification of cyber risk exposure across heterogeneous enterprise telemetry inputs. Sensitivity profiling further confirms that interaction-aware dependency modeling contributes significantly toward CREI stability. The convergence behaviour of the dynamic risk estimator demonstrates bounded fluctuation under sustained telemetry updates, while latency analysis reflects computational feasibility in real-time enterprise deployment settings. The reproducibility panel confirms full availability of dataset, preprocessing pipeline, and simulation configuration used during experimental evaluation.

6. Discussion

The results of the experiment as it can be interpreted not numerically but in terms of its structure show a systematic structural benefit of context-sensitive risk propagation in hybrid enterprise settings. The proposed DECRE-ST framework is more sensitive to latent interdependencies between services and exposure cascades (which are not usually considered by standard probabilistic risk estimators) rather than increasing the aggregate risk score. The behavior is especially important in distributed multi-cloud infrastructures in which local threat indicators tend to diffuse in a nonlinear way across service orchestration layers. Conformity to the original hypothesis statement, that enterprise risk cannot be quantified correctly without a contextual interaction dynamic, the reduction in misclassification and variance observed with the passage of time risk windows indicates that modeling dependency-sensitive telemetry is not merely helpful, but essential to stable enterprise threat forecasting.

In comparison to the dynamic risk estimation models used to date, including the CEDRA model that relies on Bayesians inference [2] and the FAIR-modified attack tree quantification models [38], the proposed mechanism demonstrates relatively better consistency between the inferred information on the threat exposure and the observed patterns of service degradation. Although previous frameworks focus on probabilistic state transitions or economic loss estimation either one on its own, they tend to ignore topology sensitivity at run time, and especially in cloud-native service meshes. On the same note, AI-based fuzzy inference systems of cybersecurity risk modeling [4] are more likely to emphasize detection granularity as opposed to propagation fidelity.

This capability to distinguish between bursts of anomalies which are transient as well as those which represent structurally meaningful threat vectors may be useful in enabling adaptive mitigation measures inside zero-trust network implementations or industrial IoT systems. Interestingly, some clusters of telemetry were characterized by the emergent risk amplification at low threat frequency- which means that infrastructural exposure is a decisive factor in planning long-term resilience. The insights can be used to program automated risk orchestration pipelines in the hybrid enterprise systems, especially where continuous monitoring can be limited by resource overhead.

6.1 Limitation

However, the evaluation is still limited to semi-synthetic workloads of telemetry and artificial service dependencies. Even though these settings are close to a realistic enterprise deployment, the adversarial dynamics, e.g., coordinated attack campaigns or vectors to break into the supply chain, were not explicitly modeled. Considered in a broader context, the study is a part of a more developing discussion on explainable and adaptive cybersecurity governance in software-defined enterprise infrastructures. As cloud ecosystems keep on decentralizing, models that have the capacity of contextualizing risk in service-sensitive architectures can form the basis of future cyber resilience programs.

7. Conclusion and Future Scope

7.1 Conclusion

This paper presented a quantitative and situational context-sensitive cyber risk estimation model designed to fit the context of hybrid enterprise networks. The suggested DECRE-ST mechanism was aimed at going beyond the static or probability-only risk scoring models to enable the introduction of the service-level dependencies and infrastructure exposure into the estimation process. Experiments have shown that contextual interaction patterns with the additive improvement of enterprise risk profiling are effective in the dynamically changing environment of threats. The current model, compared to traditional models that consider risk to be a single endpoint characteristic, represents the interdependence of vulnerability

spread among distributed cloud services. It is possible to have a more stable interpretation of the threat conditions of the runtime in hybrid infrastructures that use both on premise and cloud-native on premise and cloud-native components.

Relative assessment also indicates that the formulation proposed has less variance in the estimated risk levels due to varying telemetry inputs in comparison to the existing probabilistic and FAIR-based risk models. This stability is required when deploying data to an enterprise because an overestimated or slow threat analysis can lead to ineffective mitigation measures. Generally, the framework depicts superior responsiveness to situational service exposure, thus facilitating informed decision-making in adaptive enterprise security governance.

7.2 Future Scope

Although the present implementation provides a base architecture of dynamic estimation of cyber risks, it can be extended by a number of extensions that should make it more operationally relevant. Further investigation into the synchronous federation of enterprise SIEM platforms to provide real-time federation of telemetry streams would be valuable in the future. Also, implementing explainable artificial intelligence processes into the risk propagation layer can facilitate interpretability in automated mitigation processes. The other potential way forward is the expansion of the framework to include multi-party threat intelligence sharing, especially in enterprise ecosystems that rely on suppliers. Additional empirical validation of the approach through the heterogeneous industrial networks would also allow generalizing the results out of the simulated deployment space. This development would help in the achievement of scalable and explainable cyber resilience models of next generation cloud enabled businesses.

Corresponding author

Amer Alqatish
aalqatish@kfu.edu.sa

Acknowledgements
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU262516).

Funding
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU262516).

Contributions
Conceptualization, U.M.; methodology, U.M; I.K; P.V; R.S; A.A; G.A; software, U.M; I.K; P.V; R.S; A.A; G.A; validation, U.M; I.K; P.V; formal analysis, U.M; I.K; P.V; investigation, U.M; I.K; P.V; writing—original draft preparation, U.M; I.K; P.V; R.S; A.A; G.A; writing—review and editing, U.M; I.K; P.V; R.S; A.A; G.A. All authors have read and agreed to the published version of the manuscript.

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
All authors declare no competing interests.

References

[1]. C. Deaver-Vazquez, E. Taylor, D. Rowley, and B. Langis, “A quantitative approach to assessing and managing cybersecurity risks,” Edpacs, Apr. 2024, doi: 10.1080/07366981.2024.2340849.

[2]. D. Behbehani, N. Komninos, K. Al–Begain, and M. Rajarajan, "Cloud Enterprise Dynamic Risk Assessment (CEDRA): a dynamic risk assessment using dynamic Bayesian networks for cloud environment," Journal of cloud computing, vol. 12, no. 1, May 2023, doi: 10.1186/s13677-023-00454-2.

[3]. A. Šijan, D. Viduka, L. Ilić, B. Predić, and D. Karabašević, "Modeling Cybersecurity Risk: The Integration of Decision Theory and Pivot Pairwise Relative Criteria Importance Assessment with Scale for Cybersecurity Threat Evaluation," Electronics, vol. 13, no. 21, p. 4209, Oct. 2024, doi: 10.3390/electronics13214209.

[4]. E. Natsheh and F. B. Tabook, "AI-enhanced Cybersecurity Risk Assessment with Multi-Fuzzy Inference," Journal of ICT Research and Applications, vol. 19, no. 1, pp. 1–26, Sep. 2025, doi: 10.5614/itbj.ict.res.appl.2025.19.1.1.

[5]. J. J. Cano, "RAFA Model. Rethinking Cyber Risk Management in Organizations," Springer International Publishing, 2024, pp. 231–243. doi: 10.1007/978-3-031-47594-8_12.

[6]. P. Burnap, E. Anthi, P. Reineckea, L. Williams, F. Cao, and R. Aldmoura, "Mapping Automated Cyber Attack Intelligence to Context-Based Impact on System-Level Goals," Journal of cybersecurity and privacy, Jun. 2024, doi: 10.3390/jcp4020017.

[7]. U. Mamodiya, I. Kishor, P. Vidyullatha, A. Alqutaesh, G. Alradwan, and M. Obedat, "A hybrid fuzzy–deep learning framework for real-time cyber-attack detection in smart energy grids," International Journal of Data and Network Science, vol. 10, 2026, doi: 10.5267/j.ijdns.2026.2.007.

[8]. J. Xie, S. Zhang, H. Wang, and L. Chen, "Multiobjective network security dynamic assessment method based on Bayesian network attack graph," International Journal of Intelligent Computing and Cybernetics, vol. 17, pp. 38–60, Aug. 2023, doi: 10.1108/ijicc-05-2023-0121.

[9]. M. Figueredo Franco, F. Künzler, J. von der Assen, C. Feng, and B. Stiller, "RCVaR: an Economic Approach to Estimate Cyberattacks Costs using Data from Industry Reports," Computers & Security, vol. 139, p. 103737, Apr. 2024, doi: 10.1016/j.cose.2024.103737.

[10]. A.Mishra, P. Sarat, and R. Afza, "A factual study on hybrid multi cloud cyber security threats and proposed methodologies to enable cyber resilience," pp. 1–6, Jul. 2024, doi: 10.1109/conecct62155.2024.10677052.

[11]. M. Safarzadehvahed, F. Abazari, and F. Shabani, "QR-SACP: Quantitative Risk-Based Situational Awareness Calculation and Projection Through Threat Information Sharing," Springer Science+Business Media, 2023, pp. 170–193. doi: 10.1007/978-981-99-7032-2_11.

[12]. M. Khosravi-Farmad and A. Ghaemi Bafghi, "Dynamic Security Risk Management Considering Systems Structural and Probabilistic Attributes", doi: 10.22067/cke.2023.83744.1102.

[13]. Y. Song et al., "Hierarchical-Based Dynamic Scenario-Adaptive Risk Assessment for Power Data Lifecycle," Electronics, Feb. 2024, doi: 10.3390/electronics13030631.

[14]. H.-Y. Chen and T. Lin, "RAIN: Risk Assessment Framework Based on an Interdependent-Input Propagation Network for a 5G Network," IEEE Access, vol. 11, pp. 54881–54896, doi: 10.1109/ACCESS.2023.3281560.

[15]. R. Pal, R. X. Sequeira, X. Yin, S. Zeijlemaker, and V. Kotala, "How Should Enterprises Quantify and Analyze (Multi-Party) APT Cyber-Risk Exposure in their Industrial IoT Network?," ACM transactions on management information systems, Oct. 2023, doi: 10.1145/3605949.

[16]. U. Bhatta, "How to integrate cloud service, data analytic and machine learning technique to reduce cyber risks associated with the modern cloud based infrastructure," May 2024, doi: 10.48550/arxiv.2405.11601.

[17]. N. M. Unal and B. Çeliktaş, "A Metric-Driven IT Risk Scoring Framework: Incorporating Contextual and Organizational Factors," pp. 1–7, Aug. 2025, doi: 10.1109/acdsa65407.2025.11166074.

[18]. V. Kodela, "Real-time threat detection in enterprise networks: Integrating cisco umbrella, stealthwatch, and siem platforms," Journal of informatics education and research, vol. 2, no. 2, Jul. 2025, doi: 10.52783/jier.v1i2.3301.

[19]. S. M. AlHidaifi, M. R. Asghar, and I. S. Ansari, "Towards a cyber resilience quantification framework (CRQF) for IT infrastructure," Computer Networks, Apr. 2024, doi: 10.1016/j.comnet.2024.110446.

[20]. A. Zadeh, B. Lavine, H. M. Zolbanin, and D. Hopkins, "A cybersecurity risk quantification and classification framework for informed risk mitigation decisions," Decision Analytics Journal, Sep. 2023, doi: 10.1016/j.dajour.2023.100328.

[21]. X. Lin, Y. Yao, B. Hu, W. Yang, X. Zhou, and W. Zhang, "Enhancing power communication network security: A comprehensive cyber risk visual analytics framework with real-time risk assessment," Sustainable Energy, Grids and Networks, vol. 38, p. 101325, Jun. 2024, doi: 10.1016/j.segan.2024.101325.

[22]. M. Luo, C. Tao, Y. Liu, S. Chen, and P. Chen, "An Endogenous Security-Oriented Framework for Cyber Resilience Assessment in Critical Infrastructures," Applied Sciences, vol. 15, no. 15, p. 8342, Jul. 2025, doi: 10.3390/app15158342.

[23]. C. Wang, J. Dong, G. Guo, and T. Ren, "Dynamic Real-Time Analysis of Network Attacks Based on Dynamic Risk Probability Algorithm," Journal of Advanced Computational Intelligence and Intelligent Informatics, Jan. 2024, doi: 10.20965/jaciii.2024.p0141.

[24]. U. Mamodiya, I. Kishor, M. Almaiah, A. Alqutaish, R. Shehab, and M. Obeidat, "Behavior-aware cybersecurity using artificial intelligence and cryptographic intelligence," International Journal of Data and Network Science, vol. 10, 2026, doi: 10.5267/j.ijdns.2026.1.001.

[25]. A. Boudermine, R. Khatoun, and J.-H. Choyer, "Dynamic logic-based attack graph for risk assessment in complex computer systems," Computer networks, vol. 228, p. 109730, Mar. 2023, doi: 10.1016/j.comnet.2023.109730.

[26]. Abdi, H. Bennouri, and A. Keane, "Cyber Resilience, Risk Management, and Security Challenges in Enterprise-Scale Cloud Systems: Comprehensive Review," Jun. 2024, doi: 10.1109/meco62516.2024.10577956.
[27]. P. Vajpayee and G. Hossain, "Risk Assessment of Cybersecurity IoT Anomalies Through Cyber Value at Risk (CVaR)," May 2024, doi: 10.1109/aiiot61789.2024.10578956.
[28]. Dong, Y. Feng, and W. Shang, "A new method of dynamic network security analysis based on dynamic uncertain causality graph," Jan. 2024, doi: 10.1186/s13677-023-00568-7.
[29]. A. Kim, "Endpoint Device Risk-Scoring Algorithm Proposal for Zero Trust," Electronics, vol. 12, no. 8, p. 1906, Apr. 2023, doi: 10.3390/electronics12081906.
[30]. Zhylin and H. Holych, "Methodology of Quantitative Assessment of Network Cyber Threats Using a Risk-Based Approach," Applied Cybersecurity & Internet Governance, Jul. 2024, doi: 10.60097/acig/190345.
[31]. M. Soylu and R. Daş, "A hybrid graph neural network model for predicting cyber attacks from heterogeneous and dynamic network data," IEEE Access, p. 1, Jan. 2025, doi: 10.1109/access.2025.3603403.
[32]. H. A. A. Cue, T. Bourlai, and M. Lupo, "Proactive Cyber Resilience: A Unified Assessment Methodology for Incident Forecasting with Cyber Threat Intelligence Integration," IEEE Access, p. 1, Jan. 2025, doi: 10.1109/access.2025.3596252.
[33]. S. Ali, A. Razzaque, H. Abbas, M. Yousaf, and S. Ali, "A novel AI-Based Integrated Cybersecurity Risk Assessment Framework and resilience of National critical infrastructure.," IEEE Access, p. 1, Jan. 2025, doi: 10.1109/access.2024.3524884.
[34]. A. D. López, M. Amor, and H. Carvajal Mora, "A Novel Risk-Based Methodology for Enhancing Industrial Control Systems Security: A Systematic Review and Case Study," IEEE Access, p. 1, Jan. 2025, doi: 10.1109/access.2025.3609252.
[35]. R. Masukawa, S. Yun, S. Jeong, N. D. Bastian, and M. Imani, "TriageHD: A Hyper-Dimensional Learning-to-Rank Framework for Dynamic Micro-Segmentation in Zero-Trust Network Security," IEEE Access, vol. 13, pp. 136806–136815, Jan. 2025, doi: 10.1109/access.2025.3592877.
[36]. T. Tang and M. Li, "Enhanced secure storage and data privacy management system for big data based on multilayer model," Scientific Reports, vol. 15, no. 1, Sep. 2025, doi: 10.1038/s41598-025-16624-y.
[37]. Islam, S., Basheer, N., Papastergiou, S. et al. Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. J Reliable Intell Environ 11, 12 (2025). https://doi.org/10.1007/s40860-025-00253-3
[38]. Rana A, Gupta S and Gupta B (2024) A comprehensive framework for quantitative risk assessment of organizational networks using FAIR-modified attack trees. Front. Comput. Sci. 6:1304288. doi: 10.3389/fcomp.2024.1304288
[39]. Cheimonidis, P., & Rantos, K. (2023). Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. Future Internet, 15(10), 324. https://doi.org/10.3390/fi15100324
[40]. A. Sharma, S. Rani, and M. Shabaz, "A comprehensive review of explainable AI in cybersecurity: Decoding the black box," ICT Express, vol. 11, no. 6, pp. 1200–1219, Dec. 2025, doi: 10.1016/j.icte.2025.10.004.
[41]. Radanliev P, De Roure D, Maple C, Nurse JRC, Nicolescu R and Ani U (2024) AI security and cyber risk in IoT systems. Front. Big Data 7:1402745. doi: 10.3389/fdata.2024.1402745