American Journal of Advanced Technology and Engineering Solutions

Volume: 2; **Issue:** 4
Pages: 182-216
eISSN: 3067-5146

Quantitative Risk Modeling of VPN Misconfigurations and Firewall Rule Drift in Hybrid Cloud Networks

Md. Fardous[1]; MD Zahedul Islam[2];

[1]. *Master Of Business Studies, National University, Dhaka, Bangladesh.*
Email: fardous01@gmail.com

[2]. *Technical Engineer, Nokia, Dhaka, Bangladesh.*
Email: zahed.arman44@gmail.com

Doi: 10.63125/fa4qdz07
Received: 09 September 2022; **Revised:** 10 October 2022; **Accepted:** 12 November 2022; **Published:** 21 December 2022

Abstract

This study addresses the persistent security problem that hybrid cloud networks often accumulate VPN misconfigurations and firewall rule drift, which jointly weaken trust-boundary enforcement and increase exposure to unintended reachability and lateral movement. The purpose was to quantify how VPN misconfiguration and firewall rule drift predict hybrid cloud risk exposure, and to examine whether Protection Motivation Theory–based governance (protection motivation) is associated with lower exposure. Using a quantitative cross-sectional, case-based design, data were collected from cloud and enterprise hybrid-network operational cases with N = 132 valid practitioner responses spanning network engineering, security operations, cloud administration, and governance roles. Key variables were VPN Misconfiguration (VMS), Firewall Rule Drift (FDS), Risk Exposure (RE), and Protection Motivation (PMS) measured via multi-item 5-point Likert constructs with strong reliability (a = .88 VMS, a = .91 FDS, a = .87 RE, a = .85 PMS). The analysis plan applied descriptive statistics, Pearson correlations, and multiple regression with multicollinearity checks (VIFs within acceptable ranges). Baseline levels were above neutral for VMS (M = 3.62, SD = 0.71), FDS (M = 3.74, SD = 0.66), and RE (M = 3.58, SD = 0.69), with moderate PMS (M = 3.41, SD = 0.62). Headline findings showed strong positive associations between exposure and both VMS (r = .61, p < .001) and FDS (r = .68, p < .001), while PMS was negatively associated with exposure (r = −.42, p < .001). Regression indicated substantial explanatory power (R^2 = .58, Adj. R^2 = .56, F = 58.7, p < .001) with significant effects for VMS (β = .33, p < .001) and FDS (β = .46, p < .001) and a protective effect for PMS (β = −.21, p = .001). Segment analysis localized higher composite exposure to the remote-access VPN zone (CREI M = 3.81) and the on-prem to cloud interconnect boundary (CREI M = 3.73). Implications indicate that drift reduction should be prioritized alongside VPN configuration verification and automation-based validation to lower boundary-driven exposure and improve auditability in hybrid-cloud security governance.

Keywords

Hybrid cloud security; VPN misconfiguration; Firewall rule drift; Quantitative risk modeling; Risk exposure prediction;

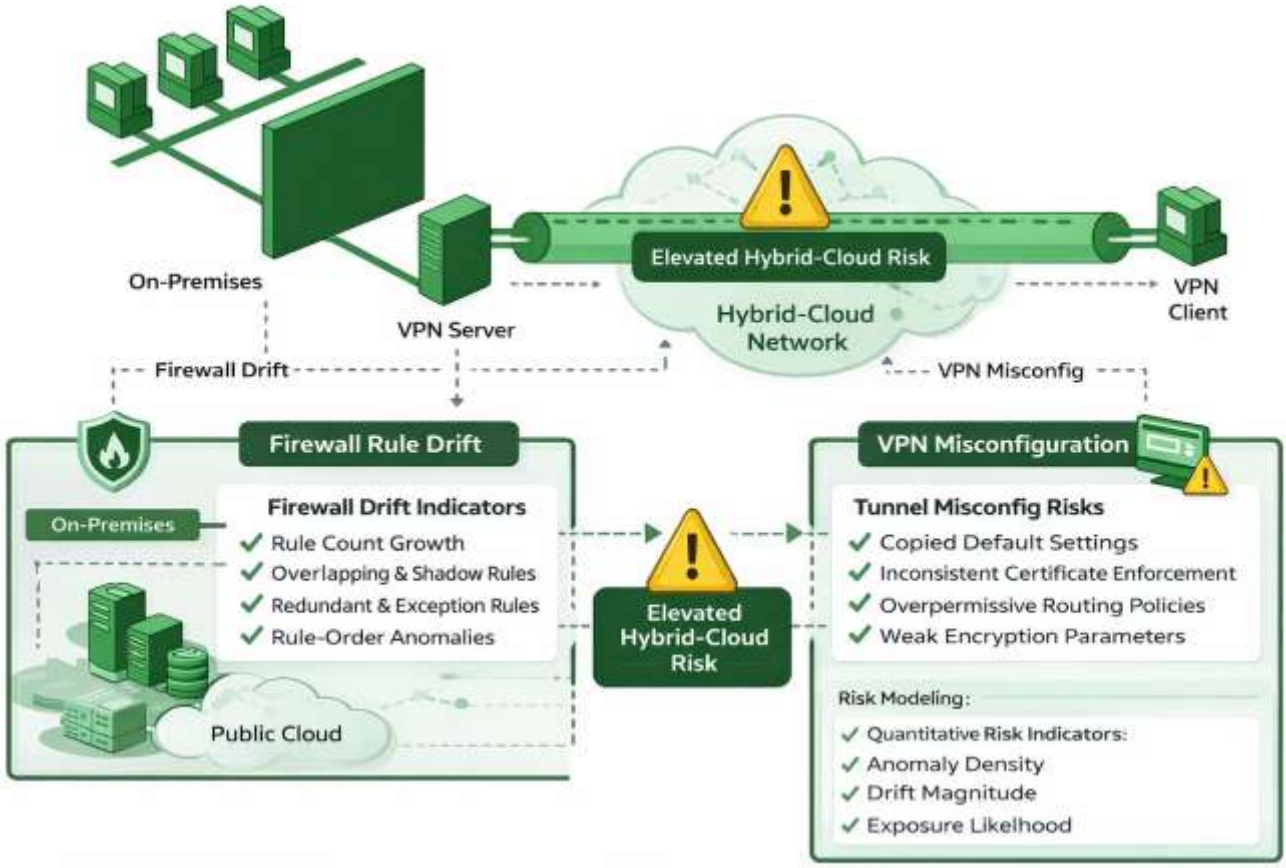
INTRODUCTION

Virtual private networks (VPNs), firewalls, and hybrid-cloud networking are foundational constructs for securing modern enterprise connectivity, so clear definitions are necessary before risk can be modeled quantitatively (Armbrust et al., 2010). A VPN is commonly defined as an encrypted tunneling mechanism that extends a private network across untrusted infrastructure, creating logical privacy and integrity for traffic traversing public or shared links; in organizational settings it often becomes the default mechanism for remote access, partner integration, and workload-to-workload connectivity across cloud and on-premises segments (Ristenpart et al., 2009). Firewalls are policy-enforcement systems that implement ordered rule sets governing packet or flow disposition, typically expressed through match conditions (e.g., address, port, protocol, state) and actions (e.g., allow, deny, log), while policy correctness depends on rule consistency, completeness, and the absence of internal anomalies that can cause unintended exposure (Shacham & Waters, 2008). Hybrid cloud is generally described as an architectural composition that integrates private infrastructure (data centers or private cloud) with public cloud services, enabling workload mobility and shared services while increasing the number of trust boundaries and policy translation points across heterogeneous platforms (Sommestad et al., 2010). In this environment, misconfiguration refers to any security-relevant deviation between intended policy and deployed policy, including incorrect tunnel parameters, weakened cryptographic settings, overbroad firewall allowances, shadow rules, redundant rules, and inconsistent rule-order effects that can invalidate expected enforcement (Ateniese et al., 2007). Firewall rule drift is the gradual divergence of firewall policy from its baseline over time due to frequent change requests, operational expediency, multi-team edits, and platform migrations, producing rule growth, exceptions, and latent contradictions that are difficult to detect by inspection alone. Quantitative risk modeling, in this context, refers to representing security exposure as measurable variables (likelihood, impact, control strength, anomaly density, drift magnitude) and estimating statistical relationships among them to support evidence-based decisions rather than narrative judgments (Subashini & Kavitha, 2011). These definitions establish a shared vocabulary for analyzing how VPN misconfigurations and firewall rule drift emerge, propagate across hybrid-cloud segments, and become measurable drivers of network security risk (Basin et al., 2016).

At an international scale, VPN and firewall policy integrity is linked directly to economic continuity, regulatory compliance, and cross-border service reliability because hybrid-cloud connectivity now underpins financial services, healthcare delivery, education platforms, logistics, and government digital services (Bethencourt et al., 2007). Cloud computing's utility model has been characterized as a shift toward on-demand infrastructure and platform services that reduce capital barriers and accelerate deployment cycles, and those same cycles increase the frequency of configuration change and the scope of connectivity that must be governed (Neil et al., 2019). Security concerns have been documented as central barriers to cloud adoption, especially in service delivery models where responsibility is shared between provider and consumer, creating coordination gaps for access control, segmentation, and monitoring (Liu & Gouda, 2005). Because hybrid cloud architectures join multiple administrative and technical domains, the attack surface becomes composite: exposures may be created in public-cloud routing, VPN endpoints, security groups, virtual firewalls, or on-premise perimeter controls, and risk emerges from the combined effect of these controls rather than any single component (Chockalingam et al., 2018). Empirical work on public cloud multi-tenancy has also shown that co-residence and shared-resource effects can create practical avenues for information leakage if isolation assumptions are violated, strengthening the argument that connectivity and enforcement policies must be measured and verified rather than assumed (Goyal et al., 2006). Formal discussions of cloud security challenges have emphasized that technical controls operate inside legal and organizational constraints, including geographically distributed users, heterogeneous vendors, and varying regulatory regimes, which collectively amplify the consequences of policy drift and configuration ambiguity. In addition, the commercial VPN ecosystem has grown globally and is used for privacy, censorship circumvention, and geo-access, but user trust is often transferred from local networks to VPN providers and software, creating international risk externalities when VPN deployment and configuration quality vary across regions and organizations (García-Alfaro et al., 2013). This international setting frames why quantitative evidence about VPN misconfiguration and firewall drift is not a narrow operational

concern but a measurable contributor to cross-border cyber risk in hybrid-cloud networking.

Figure 1: VPN Misconfiguration and Firewall Rule Drift in Hybrid-Cloud Risk Modeling



In hybrid-cloud networks, security governance is executed through policy artifacts—firewall rule sets, tunnel configurations, routing constraints, identity bindings—so the integrity of those artifacts determines whether intended segmentation and least privilege are achieved. Research in firewall policy verification has demonstrated that complex rule sets can contain anomalies such as shadowing, redundancy, and conflicts that lead to enforcement behavior diverging from administrative intent, supporting the need for systematic verification rather than manual review (Kumari & Sahoo, 2014). Work on redundancy detection has shown that even when a rule appears operationally valid, it can be functionally unnecessary given earlier rules, which increases policy size and cognitive load while masking meaningful security constraints. Stateful firewall misconfiguration studies further highlight that modern firewalls encode protocol states and transitions, so errors can arise not only from static match conditions but also from state-dependent behavior across connection lifecycles, making anomaly discovery and correction a structurally harder problem than stateless filtering (Takabi et al., 2010). Broader anomaly-focused analyses in firewall policy research have reinforced that policy defects can appear across domains and segments, especially when policies are ported between environments or when multiple policy languages coexist, a pattern that aligns with hybrid-cloud operations where multiple vendors and abstractions are simultaneously active. A policy drift framing treats these issues as dynamic rather than one-time: rule sets expand through incremental edits, exceptions accumulate, and documentation lags behind implementation, so the baseline and the deployed state progressively separate (Wang & Guo, 2010). From a measurement standpoint, drift becomes observable through indicators such as rule-count growth, exception density, overlap frequency, unused rule ratios, and anomaly types, which can be quantified and linked statistically to outcomes such as exposure windows, change failure rates, or incident occurrence (Hu et al., 2012). In hybrid-cloud contexts, the same drift logic extends to VPN configurations: tunnel parameters may be copied across sites, default settings may persist, certificate lifecycles may be inconsistently enforced, and routing policies may be widened for availability reasons, leading to measurable misconfiguration patterns that align with operational change pressure. This body of work motivates treating firewall rule drift and VPN misconfiguration

not as isolated mistakes but as quantifiable system properties of hybrid-cloud security operations (Zissis & Lekkas, 2012).

VPN misconfiguration has distinct characteristics that make it particularly relevant for hybrid-cloud risk modeling because VPNs combine cryptographic controls, endpoint identity, routing semantics, and operational management into a single dependency chain. Empirical analysis of commercial VPN services has illustrated that VPN users and organizations often rely on opaque client software and provider claims, with limited ability to verify infrastructural properties and privacy behaviors, which creates an environment where configuration and implementation quality becomes a primary risk variable (Hudic et al., 2017). In enterprise hybrid-cloud settings, VPNs are commonly used to interconnect cloud virtual networks with on-premise sites, connect remote administrators to management planes, and provide encrypted transit for cross-segment service calls; each usage mode introduces configuration surfaces such as cipher suites, authentication methods, key management, split tunneling policies, route advertisement controls, and logging settings. Because VPN tunnels often serve as "bridges" across trust zones, configuration errors can effectively redefine segmentation boundaries by allowing lateral reachability that bypasses intended firewall choke points (Khan et al., 2018). Theoretical work in access control and cryptographic policy enforcement provides context for why misconfiguration matters: attribute-based encryption models were introduced as mechanisms to enforce fine-grained access policies over ciphertext, showing how policy logic can be embedded into security controls and how correctness depends on precise policy specification. In hybrid cloud, similar logic applies operationally: the "policy" may be expressed as VPN and firewall configurations rather than ciphertext attributes, and small specification errors can invalidate the intended restriction (Khosravi-Farmad & Ghaemi-Bafghi, 2020). Cloud security surveys have also emphasized that responsibility splitting across service models can produce ambiguity in who configures which components, creating systematic opportunities for policy gaps or over-permissive defaults to remain in place (Chockalingam et al., 2018). When VPN endpoints terminate inside virtual networks that use security groups, network ACLs, and virtual firewalls, configuration consistency becomes multi-layered, so misconfiguration can occur as mismatched assumptions between layers rather than a single incorrect line item. Therefore, VPN misconfiguration is not only a cryptographic concern but also a network policy alignment concern, tightly coupled to firewall rule drift because administrators frequently compensate for tunnel issues by adding temporary firewall allowances, exceptions, or broad routes that later persist as drifted policy. These properties justify analyzing VPN misconfiguration and firewall drift jointly as co-evolving contributors to hybrid-cloud exposure (Ateniese et al., 2007).

Quantitative risk modeling provides the methodological bridge between configuration phenomena and defensible, testable statements about risk drivers, enabling hypotheses to be evaluated with descriptive statistics, correlation, and regression rather than narrative reasoning. In information security risk analysis, probabilistic relational models have been used to infer risk from system architecture metamodels by connecting structural features (components, relationships, dependencies) to probabilistic outcomes, supporting the idea that network architecture and policy artifacts can be translated into measurable risk variables (Hu et al., 2012). Bayesian network approaches have been applied to vulnerability categorization and risk reasoning, demonstrating that probabilistic dependencies among security attributes can be formalized and estimated, and that uncertainty can be modeled explicitly rather than treated as an unstructured caveat. In cybersecurity research synthesis, Bayesian network models have been reviewed as a family of techniques suited to combining heterogeneous evidence sources, handling missing data, and representing causal or dependency structure—properties directly relevant to hybrid-cloud networks where measurements originate from logs, configuration repositories, vulnerability scanners, and expert assessments (Hudic et al., 2017). Risk management frameworks based on Bayesian decision networks extend this logic by integrating assessment, mitigation reasoning, and validation/monitoring into a unified probabilistic structure, which aligns with the operational reality that firewall and VPN policies are continuously edited and must be monitored for drift (García-Alfaro et al., 2013). Quantitative cybersecurity risk analysis has also been linked to the FAIR taxonomy through Bayesian network formulations, reinforcing that risk can be decomposed into quantifiable factors such as threat event frequency, vulnerability, loss magnitude, and control strength, and that model outputs can be used for comparative ranking when properly

parameterized (Bethencourt et al., 2007; Faysal & Shamsunnahar, 2022). Methodologically, these works support a measurement strategy where Likert-scale items capture organizational and operational constructs (e.g., change governance strength, configuration review rigor, control ownership clarity), while technical measures capture objective signals (e.g., anomaly counts, drift indicators), and statistical models examine how the combined set predicts risk outcomes (Habibullah & Zaheda, 2022). In this framing, regression models can estimate the effect size of drift and misconfiguration variables while controlling for case-study context factors such as network complexity, cloud-service mix, and administrative maturity, making the resulting findings interpretable as quantified relationships rather than unbounded claims (Hudic et al., 2017).

Hybrid-cloud assurance literature provides additional grounding for studying firewall drift and VPN misconfiguration as measurable security assurance problems rather than purely technical defects. Security assurance assessment methodologies for hybrid clouds have been proposed to deliver ongoing or interval-based evaluation while balancing provider intellectual property and customer verification needs, indicating that continuous assessment is a recognized requirement in cloud-integrated environments. Formal security policy implementation research has argued for mathematically grounded transformations from abstract policy to enforceable mechanisms, underscoring that policy correctness is an engineering problem where specification, refinement, and enforcement must remain aligned, a condition directly threatened by drift and ad hoc exceptions (Jahangir & Md Shahab, 2022; Khan et al., 2018; Ratul, 2022). At the data-layer boundary, cloud integrity schemes such as provable data possession and proofs of retrievability illustrate how security claims can be validated through structured verification rather than trust, reinforcing a broader paradigm in which security controls and claims should be testable, measurable, and auditable (Ratul & Subrato, 2022; Tahmina Akter Bhuya & Rebeka, 2022). Translating this paradigm to network policy suggests that VPN and firewall controls should be treated as auditable claims about reachability, segmentation, and encryption guarantees, where the deployed configuration is the evidence . In hybrid-cloud networks, policy artifacts are distributed: some rules reside in perimeter appliances, others in cloud-native firewalls or security groups, others in routing and VPN gateway configurations, and some in infrastructure-as-code repositories, so assessment must integrate across representations. Drift can therefore be operationalized as measurable divergence between baseline policy intent (documented, version-controlled, or standardized) and the actual deployed state (running configuration, effective rules, active routes), and misconfiguration can be operationalized as measurable violation of policy invariants (e.g., unapproved open ports, overly broad CIDR allowances, weak tunnel settings, missing authentication constraints. Quantitative modeling benefits from this assurance framing because it encourages the construction of defensible constructs and indices—such as anomaly density, drift velocity, and control-gap scores—that can be validated for reliability and used consistently across case-study sites, enabling meaningful statistical comparison and hypothesis testing within a cross-sectional design (Goyal et al., 2006).

Within the combined evidence on firewall policy anomalies, VPN ecosystem behaviors, hybrid-cloud security concerns, and probabilistic risk modeling, the central scientific problem becomes a measurable question of association: which observable misconfiguration and drift patterns are statistically linked to higher risk exposure in hybrid-cloud networks, and how strongly do they predict risk-relevant outcomes when modeled together (Shacham & Waters, 2008). Firewall verification and misconfiguration research demonstrates that anomalies can be systematically detected and categorized, providing a technical basis for deriving independent variables from rule sets and configuration repositories. VPN-focused empirical work demonstrates that VPN deployments involve trust transfer and opaque client/provider behavior, reinforcing that VPN configuration quality is a plausible and measurable driver of risk rather than a background assumption (Zissis & Lekkas, 2012). Hybrid-cloud assurance research highlights that assessment must be recurring and policy-grounded, supporting the selection of constructs that measure governance, change discipline, and enforcement alignment as cross-sectional explanatory factors. Probabilistic and Bayesian risk modeling literature provides methodological precedent for converting complex security systems into quantified factors that can be statistically estimated, ranked, and interpreted under uncertainty (Wang & Guo, 2010). Bringing these strands together enables an introduction framing in which VPN misconfigurations and firewall rule drift are treated as measurable phenomena that can be mapped to constructs, assessed with reliability

testing, summarized with descriptive statistics, related through correlation matrices, and tested through regression models consistent with quantitative cross-sectional case-study designs (García-Alfaro et al., 2013). In that framing, hypothesis statements can be anchored to specific measurable mechanisms—policy anomaly counts, drift indicators, segmentation-specific risk indices, and governance-strength ratings—so that results can be interpreted as evidence for or against defined relationships rather than narrative claims (Basin et al., 2016).

This study is structured around clearly defined objectives that operationalize the research problem into measurable constructs suitable for quantitative testing within a cross-sectional, case-study–based design. The first objective is to establish a baseline measurement of VPN misconfiguration and firewall rule drift within the selected hybrid cloud environment by capturing practitioner assessments across distinct architectural segments and control layers. This objective focuses on quantifying how frequently configuration weaknesses occur, how consistently secure configuration standards are applied, and how respondents perceive the stability of firewall policy sets as operational changes accumulate. The second objective is to measure the level of hybrid-cloud risk exposure associated with these configuration conditions by constructing a risk exposure outcome variable that reflects practical security and operational consequences such as unintended reachability, weakened segmentation, elevated likelihood of unauthorized access, and increased difficulty of auditing and compliance verification. This objective emphasizes a structured, indicator-driven representation of risk exposure rather than narrative characterization. The third objective is to examine the strength and direction of statistical relationships among VPN misconfiguration, firewall rule drift, and risk exposure using correlation analysis, enabling the study to document whether higher misconfiguration and higher drift are associated with higher perceived exposure in the case context. The fourth objective is to develop and test regression models that quantify the predictive power of VPN misconfiguration and firewall rule drift on risk exposure, both independently and jointly, while accounting for relevant contextual factors such as network complexity, frequency of security-policy changes, level of automation in policy management, and participant role experience. The fifth objective is to generate segment-level risk visibility by mapping measured misconfiguration and drift indicators onto the hybrid-cloud topology, producing a structured comparison across on-premises interconnect points, cloud edge controls, transit hubs, and remote-access zones. The sixth objective is to identify the most dominant drift patterns and misconfiguration themes in the case organization through structured item-level result profiles, enabling a clear prioritization of which policy defects contribute most to elevated exposure. The final objective is to produce an interpretable risk control-gap view by summarizing governance and monitoring weaknesses into a control-gap index and ranking the sensitivity of predictors within the regression model, thereby providing a transparent, evidence-based ordering of the risk drivers observed in the case study.

LITERATURE REVIEW

The literature on quantitative risk modeling of VPN misconfigurations and firewall rule drift in hybrid cloud networks spans several intersecting research streams that collectively explain why configuration integrity is measurable, why drift accumulates in operational settings, and how these phenomena translate into risk exposure. Hybrid cloud security research establishes that enterprises increasingly rely on interconnected on-premises and cloud environments where traffic flows cross multiple trust boundaries and policy domains, requiring consistent enforcement across heterogeneous control planes and vendor-specific abstractions. Within this architectural context, firewall policy research shows that rule sets are not static artifacts; they grow through incremental changes, exceptions, and operational shortcuts, leading to structural anomalies such as redundancy, shadowing, conflicts, and over-permissive allowances that can silently weaken segmentation and reduce auditability. Parallel work on configuration management and security assurance emphasizes that misconfiguration is not merely an occasional human error but a systemic condition shaped by change velocity, fragmented ownership, documentation gaps, and the mismatch between intended policy and deployed enforcement. VPN-focused research further highlights that secure connectivity depends on correct alignment of tunnel parameters, cryptographic settings, authentication and authorization controls, and routing restrictions, so configuration defects can expand reachability and undermine assumptions about isolation between network zones. From a measurement standpoint, prior quantitative cybersecurity studies provide

methodological precedent for treating security posture as a set of observable indicators that can be aggregated into constructs and tested statistically, including the use of survey-based instruments to capture operational and governance dimensions that are not fully visible in logs or configuration snapshots. Statistical methods such as descriptive analysis, correlation, and regression are commonly used in applied security research to describe posture levels, estimate associations between control weaknesses and risk outcomes, and identify the relative importance of predictors when multiple risk drivers operate simultaneously. Taken together, this literature supports the logic that VPN misconfiguration and firewall drift can be operationalized as distinct but related constructs, assessed through reliable measurement items, and modeled against a risk exposure outcome that reflects both security and operational impacts in a hybrid cloud case setting. It also motivates integrating a theoretical lens that explains why secure configuration behaviors and drift-control practices vary across teams and contexts, alongside a conceptual framework that clarifies how misconfiguration and drift interact across hybrid segments to shape exposure.

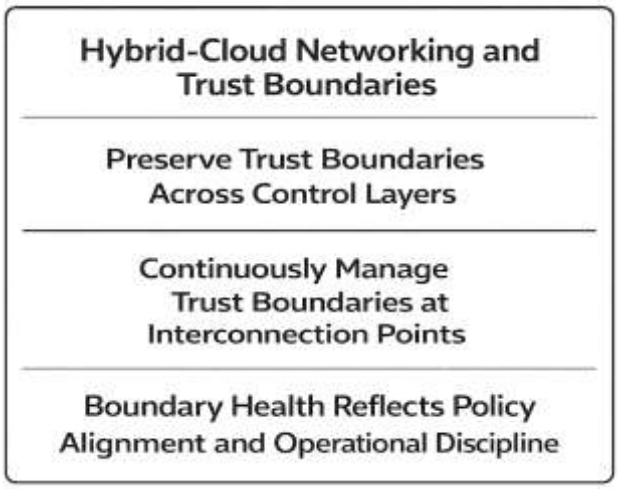
Hybrid-Cloud Networking and Trust Boundaries

Hybrid cloud networking integrates private infrastructure with cloud resources through interconnects, VPN gateways, and security enforcement layers that must preserve trust boundaries across heterogeneous control planes. A trust boundary is the point where assumptions about identity, administrative authority, and allowed reachability change, so the boundary must be made explicit through authentication, routing constraints, segmentation, and filtering. In hybrid environments, boundaries multiply because traffic may traverse on-prem perimeter devices, cloud-native security groups, and provider edge services, each with its own policy language and default behaviors. The literature on cloud security issues emphasizes that enabling technologies such as virtualization and web services introduce new dependency chains and cross-domain interactions, meaning that network concerns cannot be separated from platform governance and operational control (Jensen et al., 2009). For connectivity, organizations commonly rely on site-to-site VPN tunnels and remote-access VPNs to extend private addressing and management access into cloud networks, which creates a bridge between zones that were previously isolated by physical topology. When these bridges are added to dynamic cloud routing and elastic workloads, the security meaning of inside and outside becomes contextual rather than perimeter-based, increasing the need to define and monitor boundary conditions at each interconnection point. Migration-focused studies similarly highlight that moving systems to cloud architectures changes the set of security questions organizations must answer, including how isolation is maintained, how incident response responsibilities are allocated, and how network controls are validated across distributed components (Rosado et al., 2012). These concerns become especially salient in hybrid deployments because boundary definitions are not created once; they are continuously reinterpreted as teams adjust routes, tunnels, and firewall policies to maintain availability. As a result, hybrid cloud networking can be framed as a continuous boundary-management problem in which reachability is negotiated across domains, and security depends on keeping boundaries aligned with organizational intent.

Trust boundaries in hybrid environments are shaped not only by topology but also by elasticity, multi-tenancy, and managed services that abstract lower-layer controls. As workloads and network endpoints are created and retired quickly, boundary enforcement depends on policy artifacts that travel with the workload, such as security groups, virtual firewall rules, and software-defined routing intents. Cloud-vulnerability research notes that the cloud model changes risk by reducing customer control over underlying infrastructure and by altering the visibility available for logging and monitoring, which complicates boundary verification during investigations (Grobauer et al., 2011). In hybrid settings, that visibility gap becomes a boundary problem because a single end-to-end flow may traverse segments with rich telemetry and segments where evidence is mediated by provider APIs. Hybrid cloud operators increasingly rely on software-defined networking to coordinate policy across data centers and clouds, translating high-level intents into distributed forwarding rules. SDN surveys emphasize that the separation of control and data planes and virtualization layers enable flexible, large-scale management, while adding new dependency chains that must be secured to preserve isolation (Kreutz et al., 2015). These dependencies matter for trust boundaries because controllers, orchestration systems, and policy compilers become boundary-defining components: if they miscompute intent,

push partial updates, or diverge across domains, the effective boundary can differ from the declared boundary. Operationally, this divergence can appear as inconsistent reachability, unexpected access through transit hubs, or policy exceptions that persist after emergencies. Accordingly, boundary robustness can be operationalized as the alignment between declared segmentation intent and observed enforcement behavior, measured through indicators such as policy-change frequency, rule translation count, exception density, and cross-domain audit visibility. This framing links architectural trust-boundary concepts to measurable constructs that can serve as controls when modeling configuration risk. In practice, boundary definitions reduce ambiguity when teams share ownership across on-prem and cloud domains.

Figure 2: Hybrid-Cloud Networking And Trust Boundaries In Hybrid Environments



Hybrid cloud trust boundaries are influenced by the security posture of the network control fabric that coordinates connectivity across sites, tenants, and services. Enterprises connect branch networks, remote administrators, SaaS dependencies, and cloud workloads through overlays, transit hubs, and shared service zones, creating junctions where multiple principals and policies intersect. At each junction, the boundary question is whether least privilege is enforced consistently under change, because hybrid operations involve frequent routing updates, tunnel lifecycle events, and firewall rule edits. Software-defined approaches help manage this complexity by representing connectivity as programmable policy, yet programmability also turns the control surface into a boundary whose failure can invalidate downstream segmentation. SDN security research describes threats that target forwarding devices, controllers, and policy applications, highlighting that boundary enforcement depends on control-plane integrity as much as data-plane filtering (Vasilakos & Imran, 2016). In hybrid deployments, these weaknesses can manifest as unauthorized policy insertion, inconsistent rule distribution, or accidental exposure when orchestration updates only some enforcement points. For quantitative modeling, this literature supports treating trust boundaries as composites rather than fixed perimeters: boundary strength can be operationalized as the combined reliability of identity binding, encryption termination points, policy translation accuracy, and audit evidence continuity. This approach fits environments where one logical boundary is implemented differently across segments, for example security groups in one cloud, virtual firewalls in another, and VPN gateways bridging them. Boundary health can then be approximated with indicators such as the rate of untracked changes, the share of policies deployed by automation versus manual edits, variance in effective reachability, and completeness of logging across hops. Pairing these indicators with practitioner-rated items on ownership clarity, change approval rigor, and monitoring discipline enables cross-sectional analysis that links boundary behavior to measurable risk exposure within a single case organization. This linkage supports drift and misconfiguration testing.

VPN Technologies and Misconfiguration Modes

Virtual private networks (VPNs) are logical overlays that create authenticated and encrypted tunnels across untrusted transport networks, enabling endpoints or sites to communicate as if they were on the same trusted segment. In enterprise practice, that illusion depends on coordinated choices across cryptographic negotiation, traffic encapsulation, routing, and access-control policy. IPsec site-to-site deployments, for example, rely on Internet Key Exchange (IKE) to authenticate peers, agree on algorithms, and bind identities to security associations; weaknesses in those bindings can undermine authentication even when confidentiality appears intact (Cremers, 2011).

Figure 3: Vpn Technologies, Configuration Surfaces, And Misconfiguration Modes In Hybrid-Cloud Networks

The operational burden is that a single VPN link is not one control, but a bundle of controls: cipher and integrity selections, lifetimes, rekey rules, identity assertions, routing advertisements, split-tunneling decisions, and firewall permits that must match the intended threat model. When any one of these elements is mis-set, traffic can bypass the tunnel, be tunneled but to the wrong destination, or be protected with properties that do not meet policy. The risk is amplified in hybrid-cloud connectivity because tunnels terminate at boundaries where address translation, overlay routing, and security-group semantics intersect, which increases the number of implicit defaults and hidden dependencies administrators must reason about. Empirical studies of commercial VPN clients show that even when users believe all traffic is tunneled, implementation and configuration gaps can leak IPv6 traffic or enable DNS manipulation, thereby exposing identifying metadata and diverting requests outside expected protections (Perta et al., 2015). As a result, VPN misconfiguration is best viewed as a measurable reliability and governance problem in security enforcement, rather than as a rare operator mistake, because the tunnel's correctness depends on continual alignment between protocol assumptions and evolving network state. Accordingly, risk models must treat tunnel configuration as a set of variables—coverage, negotiation strength, and policy consistency—whose deviations can be quantified per segment and time.

Configuration complexity becomes more pronounced when VPN policy must coexist with firewall and segmentation rules authored by multiple teams, tools, or vendors. Research on reconciling IPsec and firewall policies shows that administrators often manage complexity by composing smaller, independent policies, yet composition can introduce inconsistencies—allowing traffic one policy meant to deny, or protecting a different packet set than intended (Aura et al., 2010). In hybrid-cloud networks, similar composition occurs across security groups, network ACLs, virtual appliances, and on-premises

firewalls, so a tunnel that is correct in isolation may still be exposed by an adjacent rule set that silently broadens reachability. These interactions create several misconfiguration archetypes that are important for quantitative measurement: over-permissive selectors that encrypt too broadly and mask unauthorized lateral movement; under-permissive selectors that leave "shadow routes" outside the tunnel; mismatched lifetimes that cause frequent rekeys and intermittent drops; and policy objects that drift when infrastructure-as-code templates are updated without synchronizing gateway settings. Endpoint and client behavior adds another dimension because VPN software often embeds packet filters, DNS handlers, and certificate stores that can diverge from enterprise baselines. Large-scale analysis of Android VPN permission-enabled apps demonstrates that VPN tooling can itself introduce security and privacy failures, including insecure tunneling choices, DNS and IPv6 leakage, and traffic manipulation such as TLS interception or JavaScript injection (Ikram et al., 2016). Although mobile VPN apps are not identical to enterprise gateways, the core lesson generalizes: users and operators can receive a false sense of protection when "VPN connected" is treated as a binary state rather than a verified set of properties. For firewall-rule drift studies, this implies that the most credible measurements will incorporate not only static configuration snapshots, but also runtime validation signals that reveal whether actual traffic paths match intended tunnel and filtering semantics across segments and change windows.

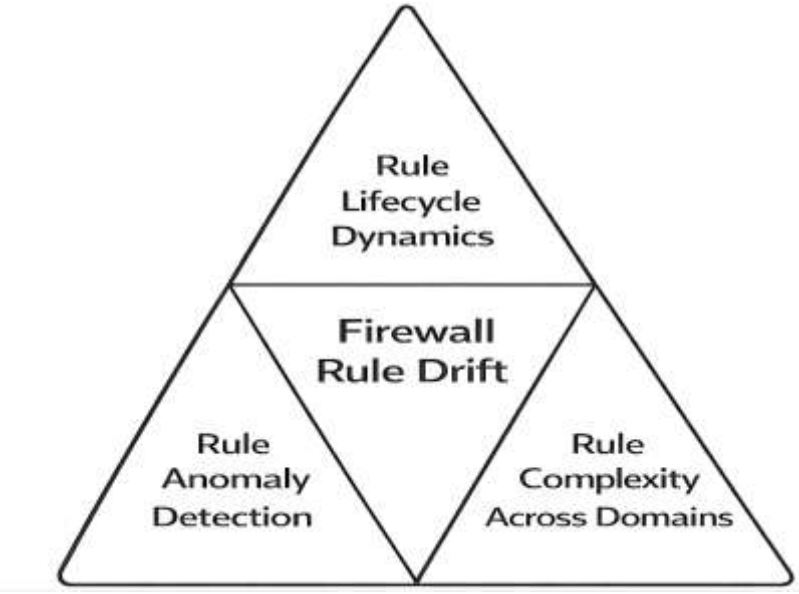
For quantitative risk modeling of VPN misconfigurations in hybrid-cloud networks, prior work suggests constructs that are both measurable and analytically useful: (a) tunnel coverage completeness across address families and services (IPv4/IPv6, DNS, management planes), (b) negotiation robustness (agreement on strong suites and correct identity bindings), and (c) policy coherence across enforcement points (cloud controls, on-prem firewalls, and VPN gateways). Coverage completeness is especially salient because leakage often emerges at protocol boundaries where traffic is handled "out of band," such as IPv6 auto-configuration or resolver selection, and therefore escapes the operator's primary ruleset (Perta et al., 2015). Negotiation robustness matters because the security properties of the tunnel depend on subtle authentication and key-exchange details; formal analysis of IKE shows that assumptions about peer identity, message ordering, or state handling can lead to unexpected behaviors that are not obvious from configuration intent alone (Cremers, 2011). Policy coherence becomes the bridge to firewall-rule drift: when routing tables, security groups, and gateway selectors evolve independently, the effective policy surface changes even if each component appears locally consistent, a challenge that motivates reconciliation approaches for IPsec and firewall policies (Aura et al., 2010). A further measurement opportunity arises from client-side and browser-side leakage channels that can reveal real IP information even when a VPN is active, as demonstrated in work on WebRTC privacy leaks and practical mitigation mechanisms (Fakis et al., 2020). Together, these findings justify treating "misconfiguration risk" as a latent variable that can be operationalized with observable indicators: drift frequency, exception count, coverage gaps, and validation failures per hybrid-cloud segment. In a case-study design, these indicators can be mapped to survey constructs (e.g., change control rigor, policy review cadence, and tool support) and then tested with correlation and regression models to explain variation in measured risk across sites and time windows within enterprises.

Firewall Policy Lifecycle and Rule-Drift Dynamics

Firewall policies operationalize segmentation and least-privilege principles by translating abstract security intent into ordered match–action rules that determine whether traffic is permitted, denied, or logged at enforcement points. In hybrid-cloud environments, these rule sets are rarely authored or maintained within a single administrative boundary. Instead, they evolve across on-premises devices, virtual firewalls, and cloud-native security constructs, each managed through distinct interfaces and change workflows. This distributed authorship increases the likelihood of rule anomalies such as shadowing, redundancy, and conflicts, which arise when rule order and match conditions interact in unintended ways. Early anomaly-detection research demonstrated that manual policy updates frequently introduce inconsistencies that can simultaneously allow unauthorized traffic and block legitimate flows, thereby necessitating automated detection and restructuring mechanisms (Abedin et al., 2006). From a lifecycle perspective, these anomalies are not isolated errors but cumulative artifacts of operational change, where temporary fixes and exception rules persist beyond their initial justification. Research on network-level access control policy analysis further indicates that multi-

stakeholder environments tend to generate policy conflicts when administrators express localized requirements without a unified semantic framework, encouraging incremental exception stacking rather than structural redesign (Basile et al., 2012). In hybrid-cloud networking, such exception stacking contributes to rule drift, defined here as the gradual degradation of policy coherence and segmentation clarity over time. Drift becomes observable through measurable indicators such as rule-count expansion, increased overlap among match predicates, aging exceptions, and growing proportions of unused or redundant rules. This framing positions rule drift as a structured and quantifiable phenomenon shaped by policy lifecycle dynamics rather than a random occurrence.

Figure 4: Firewall Policy Lifecycle, Rule Anomalies, And Rule-Drift Dynamics In Hybrid-Cloud Networks



The persistence of firewall rule drift is reinforced by the difficulty of validating rule correctness after each configuration change. Enterprise firewall policies often encode complex predicate combinations involving IP ranges, services, zones, and stateful conditions, making it challenging to anticipate the full impact of even minor edits. Structural testing research has formalized coverage criteria over firewall rules and demonstrated that inadequate test coverage significantly reduces the probability of detecting faults introduced during policy updates (Hwang et al., 2012). Limited validation encourages reactive edits in operational contexts; administrators may add broad allow rules to restore service availability rather than diagnose the structural cause of a misclassification. Automated correction approaches have shown that firewall policy faults can be modeled comprehensively and resolved through reasoning over misclassified packet sets and policy constraints, illustrating that systematic verification can reduce accumulated anomalies (Chen et al., 2012). In hybrid-cloud settings, however, enforcement points are distributed across domains, so misclassification may originate from interactions among cloud security groups, VPN gateways, and on-premises firewalls. This distribution complicates root-cause analysis and increases reliance on ad hoc exceptions, thereby accelerating drift. For quantitative modeling, these dynamics justify incorporating both technical drift metrics—such as anomaly density, rule churn rate, and mismatch between intended and effective reachability—and process-oriented indicators—such as change approval rigor, review cadence, and documentation completeness. When measured in a cross-sectional case study, these variables can be statistically linked to risk exposure outcomes, enabling drift to be examined as both a structural and organizational driver of vulnerability.

A further complexity in rule-drift dynamics arises from the semantic richness of modern firewall systems. Real-world rule sets include user-defined chains, stateful inspection, interface bindings, and vendor-specific extensions, which complicate consistent analysis and normalization across tools. Semantics-preserving simplification research has demonstrated that transforming complex rule sets

into analytically tractable representations, while retaining equivalent filtering behavior, is feasible and improves the reliability of automated analysis (Diekmann et al., 2015). This insight is particularly relevant for hybrid-cloud environments, where rule semantics differ across platforms and enforcement technologies. If analysis tools cannot accurately model effective filtering behavior, organizations may incorrectly assume policy correctness, allowing drifted or overly permissive rules to persist undetected. Consequently, the fidelity of policy analysis mechanisms becomes a measurable governance factor that can influence residual exposure. From a quantitative perspective, firewall rule drift can therefore be operationalized through a multidimensional construct encompassing lifecycle pressure (frequency of edits and business-driven changes), assurance maturity (testing coverage and automated verification capability), and semantic fidelity (accuracy of rule interpretation across heterogeneous platforms). Within a regression-based research design, these dimensions can be evaluated as predictors of hybrid-cloud risk exposure, enabling empirical assessment of whether higher drift and lower verification rigor correspond to greater segmentation breakdown and unintended reachability. Collectively, the literature supports treating firewall rule drift as a patterned outcome of organizational processes and technical constraints, making it suitable for structured measurement and hypothesis testing in a case-study context.

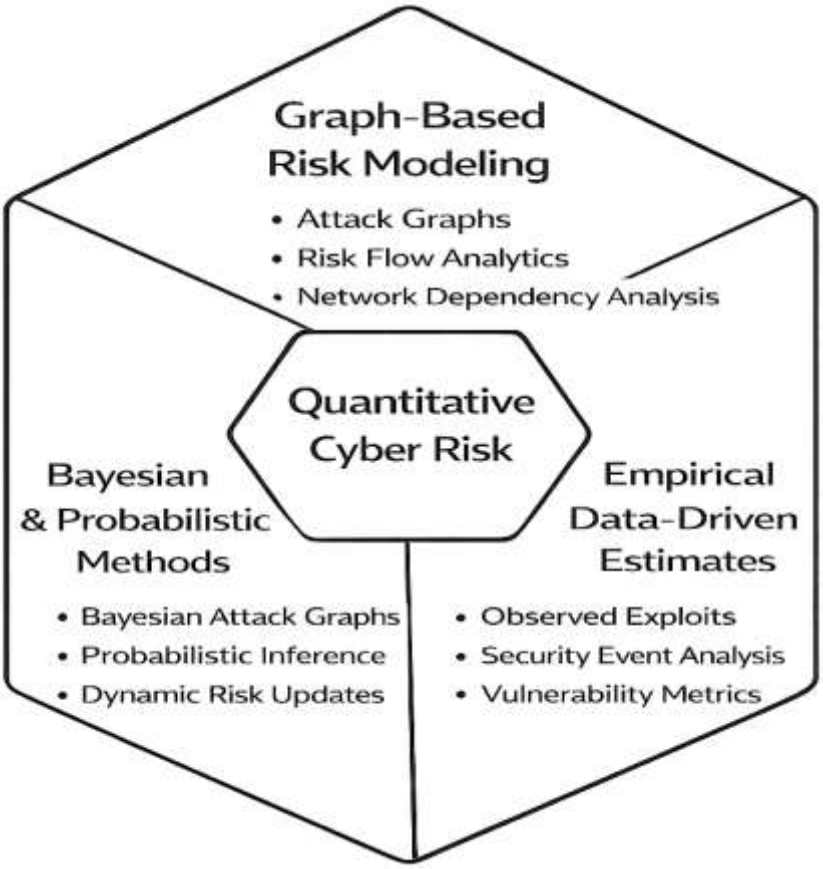
Quantitative Cyber Risk Modeling and Measurement Approaches

Quantitative cyber risk modeling translates security conditions into measurable variables that support comparable, evidence-based decisions across complex infrastructures such as hybrid clouds. In most quantitative traditions, risk is treated as a combination of *likelihood* (the chance an adverse security event occurs) and *impact* (the loss if it occurs), and the main methodological differences lie in how researchers estimate likelihood, represent dependencies among security conditions, and aggregate results into interpretable scores. A widely used approach is *graph-based risk modeling*, where enterprise infrastructure is represented as nodes (assets, services, vulnerabilities, trust relationships) and edges (reachability or exploitation preconditions), and risk is derived by analyzing multi-step attack progression rather than isolated weaknesses. Attack-graph metrics are particularly relevant to hybrid-cloud security because misconfigurations and rule drift rarely create risk in a single hop; instead, they increase the probability of chained outcomes such as unintended reachability followed by privilege escalation and lateral movement. In this stream, probabilistic security metrics built on attack-graph structure provide a formal mechanism for expressing "overall" network security while accounting for multiple possible paths to compromise (Wang et al., 2008). For VPN misconfiguration and firewall drift research, the core value of graph-based modeling is that it operationalizes *dependency*: a permissive firewall rule becomes more dangerous when combined with a VPN tunnel that expands routing scope, and the model can represent that interaction explicitly. Methodologically, this literature also motivates measurement designs that distinguish between (a) structural indicators (e.g., connectivity expansion points, segmentation breaks, and policy overlaps) and (b) governance indicators (e.g., change control rigor and verification cadence), because the observable risk outcome in real networks is shaped by both technical reachability and organizational control quality.

A second stream emphasizes Bayesian and probabilistic inference methods that update risk estimates as network conditions change, enabling *dynamic* assessment that reflects configuration drift, patching activity, and control degradation. Bayesian attack graph approaches integrate attack-graph structure with Bayesian belief networks so that the probability of compromise can be computed from conditional dependencies among vulnerabilities, reachability constraints, and assumed exploit likelihoods. This is important for hybrid-cloud networks because risk levels can shift rapidly: a single policy exception, a new subnet, a route advertisement, or a tunnel parameter change can alter reachable attack surfaces without changing the underlying application code. Dynamic risk frameworks based on Bayesian attack graphs also align with operational decision-making because they can support "what-if" analysis: administrators can compare the expected risk reduction produced by tightening a tunnel selector, removing an overly broad firewall rule, or adding monitoring controls at a transit segment (Poolsappasit et al., 2012). In parallel, quantitative attack-graph extensions treat risk as a flow-like phenomenon across attack paths, allowing risk accumulation to be computed while preserving the idea that exploitation dependencies are not independent events. Risk-flow attack graph methods formalize how an attacker's progress along one path can enable downstream opportunities, improving the

interpretability of why certain segments or assets dominate overall exposure (Dai et al., 2015). For this thesis, these probabilistic traditions justify modeling "misconfiguration risk" and "drift risk" as *predictors* that can be statistically related to an exposure outcome, while still preserving the conceptual reality that exposure is produced by chained dependencies rather than isolated control failures.

Figure 5: Quantitative Cyber Risk Modeling And Measurement Approaches In Hybrid-Cloud Security



A third stream grounds quantitative cyber risk estimation in empirical security-event and vulnerability data, arguing that risk models should reflect real exploitation patterns rather than relying solely on severity labels or static scoring schemes. Empirical research comparing severity scores with exploitation evidence demonstrates that commonly used severity ratings may not align with the probability that vulnerabilities are exploited in the wild; therefore, risk estimation improves when models incorporate predictors more directly tied to attacker behavior and exploitation availability (Allodi & Massacci, 2017). This insight matters for hybrid-cloud misconfiguration and firewall drift because configuration faults often do not map cleanly onto a single vulnerability score; instead, they alter *attack feasibility* and *attack cost* by expanding reachability, weakening segmentation, or increasing the persistence of unauthorized access paths. Data-driven quantitative risk work also shows how security operations data (events, detections, and observed attack activity) can be transformed into likelihood estimates of compromise in ways that reveal mismatches between traditional qualitative assessments and quantitative estimates (Allodi & Massacci, 2014). For a cross-sectional, case-study–based design using Likert-scale constructs, this literature supports two measurement principles that strengthen trustworthiness: first, the dependent variable (risk exposure) should be defined in ways that correspond to operationally meaningful outcomes (e.g., unintended reachability, audit breakdown, or escalation potential), and second, the independent variables (VPN misconfiguration and firewall drift) should be operationalized as multi-item constructs that capture not only "how often changes occur" but also "how verifiable and controlled changes are." Within regression modeling, the practical contribution of this stream is the emphasis on interpretability and validation: results are more

defensible when the predictors represent mechanisms that plausibly influence attacker feasibility and when the outcome aligns with observable exposure patterns in the case environment.

Theoretical Framework: Protection Motivation Theory for Configuration Risk Governance (PMT)

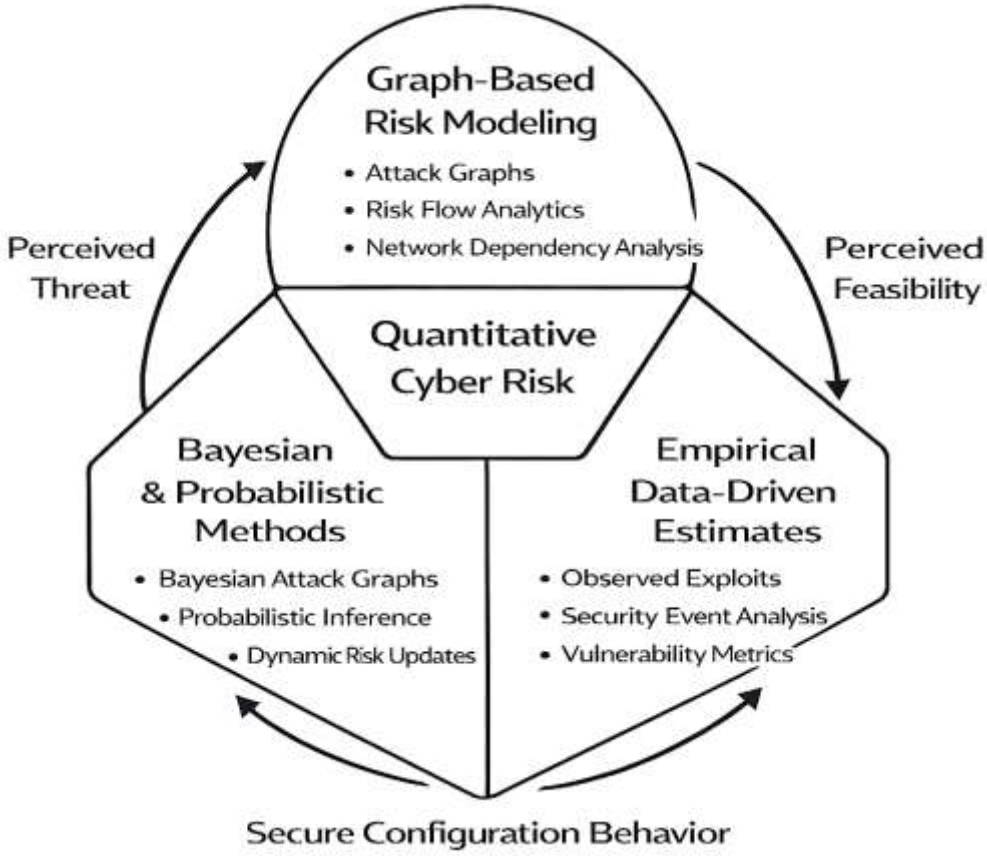
Protection Motivation Theory (PMT) explains why individuals and groups adopt (or fail to adopt) protective behaviors when they perceive a threat, and it provides a strong behavioral lens for a study where risk is driven by day-to-day configuration choices that accumulate into VPN misconfigurations and firewall rule drift. In hybrid-cloud network operations, secure configuration is rarely a single "decision"; it is a repeated pattern of actions such as enforcing strong tunnel parameters, preventing split-tunnel exceptions, maintaining certificate hygiene, restricting route advertisements, validating firewall changes, and removing obsolete allow rules. PMT is suitable for this context because it models protective action as the product of two cognitive evaluations: **threat appraisal** (how serious the risk feels and how vulnerable the system is) and **coping appraisal** (how effective the response is, how capable the actor feels, and what costs or frictions inhibit action). In configuration-heavy environments, drift and misconfiguration can be interpreted as outcomes of weak coping appraisal (e.g., low confidence in tooling, limited verification capability, high time pressure) even when threat appraisal is high (e.g., the team knows misconfigurations can be severe). PMT has been used in organizational security policy contexts to explain compliance intentions under real constraints such as organizational pressure, perceived effectiveness, and resource availability, making it directly transferable to the governance of configuration change and policy maintenance in network security operations (Herath & Rao, 2009). Within this thesis, PMT grounds the idea that "secure configuration behavior" is not only technical competence; it is also a motivational and organizational phenomenon shaped by perceived threat, perceived feasibility of protective action, and the friction costs of doing configuration work correctly every time. This theoretical grounding strengthens the logic of treating drift and misconfiguration as measurable outcomes of both technology and human-process conditions embedded in the hybrid cloud case setting.

To operationalize PMT for quantitative modeling, the study treats protective motivation as a measurable latent factor that influences the rigor of configuration governance and the discipline of drift control. PMT commonly represents protection motivation as a function of threat and coping components, which can be translated into a composite score usable in survey-based measurement and regression analysis. A practical formula that can be applied throughout this thesis is the Protection Motivation Score (PMS):

$$\text{PMS} = (PS + PV - MR) + (RE + SE - RC)$$

where PS = perceived severity of misconfiguration/drift consequences, PV = perceived vulnerability of the hybrid-cloud environment to those consequences, MR = maladaptive rewards (benefits of shortcuts such as "temporary" broad rules), RE = response efficacy (belief that controls like policy review, automation, and validation reduce risk), SE = self-efficacy (confidence in implementing and maintaining secure configurations), and RC = response cost (time, complexity, operational disruption, and friction). In hybrid-cloud networking, fear appeal and threat communication have been shown to shape security behaviors through these kinds of cognitive pathways, which supports the use of threat and coping variables as measurable predictors rather than abstract concepts (Johnston & Warkentin, 2010). The PMS offers a consistent mechanism to connect motivational conditions to operational outcomes: higher PMS should align with stricter tunnel governance, fewer exceptions, stronger validation routines, and faster removal of obsolete firewall rules. In addition, PMS provides a theoretically justified way to interpret why two teams facing the same technical environment may exhibit different drift trajectories: the difference can be expressed as differences in self-efficacy, response efficacy, and perceived costs rather than being attributed only to "skill." The formula is therefore selected as the primary theoretical computation that can be applied across constructs and later integrated as an explanatory variable in the study's statistical models.

Figure 6: Protection Motivation Theory Framework For Configuration Risk Governance In Hybrid-Cloud Networks



In the full research model, PMT acts as the behavioral backbone that explains variance in configuration outcomes beyond purely technical complexity. This matters because drift and misconfiguration often emerge from repeated omission behaviors—skipping validation, delaying cleanup, accepting overbroad routing, or leaving permissive rules in place—especially under workload pressure. PMT-aligned empirical work has shown that security lapses are strongly associated with threat and coping perceptions, helping explain why knowledgeable users still omit protective measures under certain motivational conditions (Workman et al., 2008). In this thesis, that logic maps cleanly to network policy operations: a team may "know" the correct firewall hygiene but still accumulate drift when the perceived cost of cleanup is high and the perceived reward of quick fixes is immediate. To integrate PMT into the quantitative design, the study uses PMS-derived constructs as governance predictors that complement the main technical predictors (VPN misconfiguration and firewall drift). Prior PMT-driven compliance research demonstrates that self-efficacy and response efficacy often show stable positive relationships with compliance intentions, providing justification for including these PMT components as measurable influences on secure configuration behaviors (Ifinedo, 2012). The framework also supports incorporating habit-like reinforcement in security compliance, where repeated secure behaviors become routinized and strengthen the cognitive pathways that PMT describes, which is important in environments where configuration tasks recur daily (Vance et al., 2012). Consequently, PMT provides a coherent theoretical explanation for why configuration risk persists and why interventions that reduce response cost, increase self-efficacy through tooling and training, and increase response efficacy through validation feedback can align with lower observed misconfiguration and drift levels in a cross-sectional case-study analysis.

Conceptual Framework and Hypotheses Linkage for Hybrid-Cloud Configuration Risk

This study's conceptual framework defines risk exposure in hybrid-cloud networks as an observable outcome produced by two technical condition sets—VPN misconfiguration and firewall rule drift—and shaped by governance capability captured through Protection Motivation Theory (PMT) constructs. Conceptually, *VPN misconfiguration* represents deviations in tunnel correctness (identity

binding, crypto posture, traffic coverage, routing scope, and access constraints) that alter reachability across hybrid segments. *Firewall rule drift* represents time-accumulated divergence between intended segmentation and effective policy enforcement, observable through exception stacking, redundancy, shadowing, and over-broad rules. *Risk exposure* is defined as the degree to which unintended reachability, lateral-movement opportunity, audit breakdown, and control uncertainty exist within the case network. Because cybersecurity measurement requires interpretable and decision-relevant metrics, the framework treats each concept as a multi-item construct rather than a binary state, aligning with system-security measurement guidance that emphasizes structured metric families and clear aggregation logic (Pendleton et al., 2016). The framework also adopts a situational-awareness view: exposure is not only "what vulnerabilities exist," but "what the network state means right now" across segments and control planes, which supports segment-based modeling and dashboardable outputs (Franke & Brynielsson, 2014). Finally, the framework incorporates a measurement-oriented governance layer that links technical state to control maturity and monitoring discipline, consistent with security-metrics work that stresses continuous measurement and operational relevance in enterprise settings (Cheng et al., 2014). In this framing, misconfiguration and drift are modeled as *proximal technical drivers*, while PMT-based governance is modeled as a *behavioral and organizational driver* that explains why technical conditions persist or are reduced under operational pressure.

To support quantitative testing, the conceptual model specifies three computed indices that can be used consistently across the thesis: a VPN Misconfiguration Score (VMS), a Firewall Drift Score (FDS), and an overall Configuration Risk Exposure Index (CREI). Each score is computed from Likert-scale items (1–5) that are grouped by construct and averaged to preserve interpretability and reliability testing. Let x_{ij} be the response of participant i to item j within a construct; then the construct score is computed as:

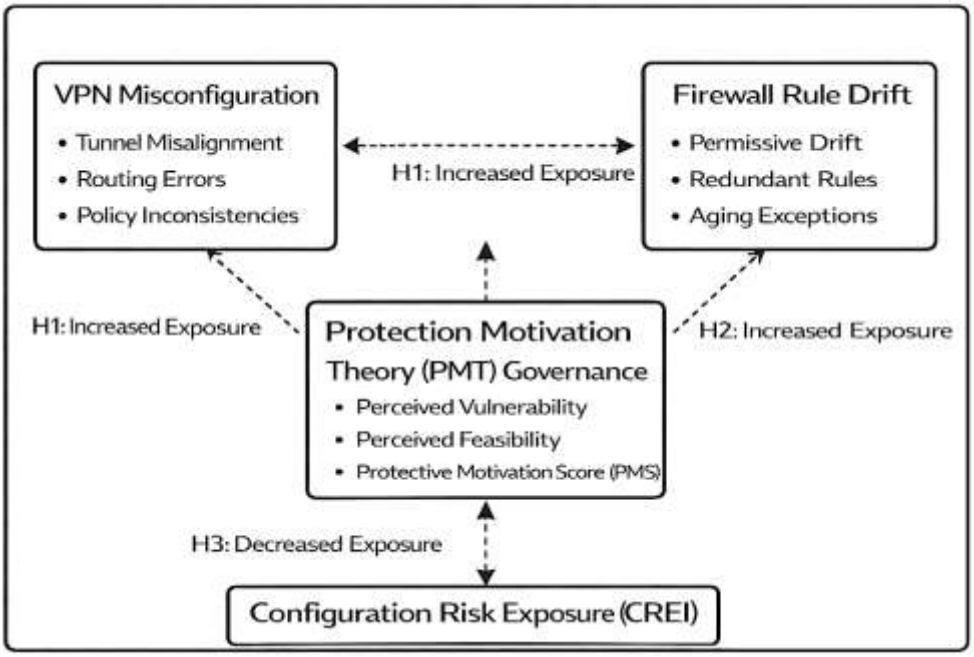
$$S_i = \frac{1}{k}\sum_{j=1}^{k} x_{ij}$$

where k is the number of items for that construct. This aligns with modular quantitative risk modeling approaches that emphasize incremental aggregation of measurable threat and control dimensions into a systematic risk model (Jouini et al., 2015). Because the study also produces unique outputs (heatmaps, drift fingerprints, and a control-gap index), the framework selects a single core outcome metric—**CREI**—that integrates both technical predictors and governance friction into one interpretable exposure score usable for segmentation comparison and regression modeling. The chosen formula (applied throughout the study) is:

$$\mathrm{CREI}_i = \alpha \cdot \mathrm{VMS}_i + \beta \cdot \mathrm{FDS}_i + \gamma \cdot (1 - \mathrm{PMS}_i)$$

where $\alpha + \beta + \gamma = 1$, and PMS_i is the normalized PMT Protection Motivation Score from Section 2.5 (scaled to 0–1). The term $(1-\mathrm{PMS}_i)$ operationalizes the idea that weaker coping capability and higher response cost increase the persistence of drift and misconfiguration. The selection of a composite exposure index is also consistent with security-metrics literature arguing that measurement must remain comparable across systems and versions while retaining a defensible mapping to attackability and reachable attack surface conditions (Manadhata & Wing, 2011). In the case-study context, CREI can be computed per respondent and then summarized per hybrid segment, enabling the results section to report both human-rated governance signals and segment-level technical exposure patterns.

Figure 7: Conceptual Framework And Hypotheses Linkage For Hybrid-Cloud Configuration Risk Exposure



The framework's causal logic is expressed as testable associations suitable for correlation and regression analysis within a cross-sectional design. First, higher VPN misconfiguration is expected to increase exposure because tunnel correctness determines which routes and services become reachable across trust boundaries. Second, higher firewall rule drift is expected to increase exposure because drift expands and obscures permitted flows, undermining segmentation predictability and auditability. Third, stronger PMT-based protection motivation (higher PMS) is expected to reduce exposure by strengthening change discipline, validation behavior, and cleanup of temporary exceptions. These relationships are tested through a regression model that treats exposure as the dependent variable and separates technical drivers from governance drivers:

$$\mathrm{CREI}_i = \theta_0 + \theta_1 \mathrm{VMS}_i + \theta_2 \mathrm{FDS}_i + \theta_3 \mathrm{PMS}_i + \varepsilon_i$$

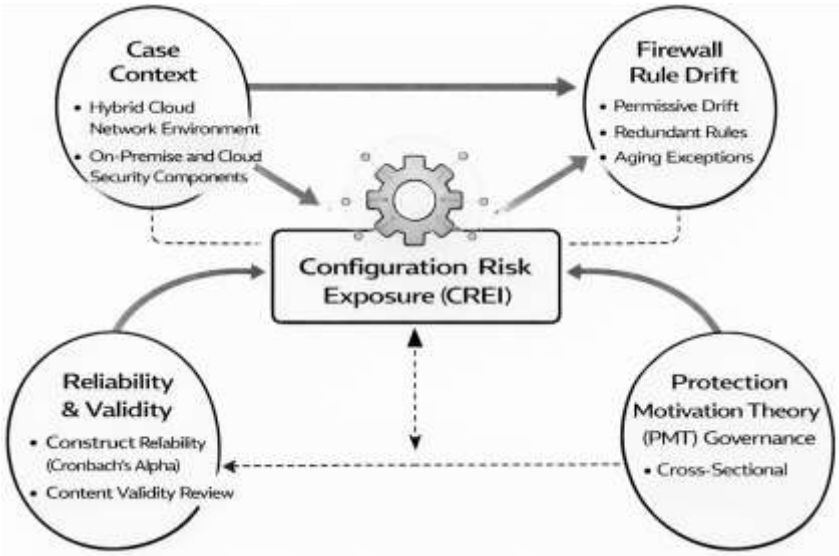
Optionally, control variables can be included (e.g., network complexity, change frequency, automation level, and role experience) as $\sum_m \theta_m C_{im}$. This structure supports two thesis goals simultaneously: (a) quantifying whether misconfiguration and drift are statistically associated with exposure, and (b) demonstrating whether governance motivation explains additional variance beyond technical conditions. In reporting, standardized coefficients and sensitivity ranking can be derived from the fitted model by comparing $|\hat{\theta}_1|$, $|\hat{\theta}_2|$, and $|\hat{\theta}_3|$ after z-score standardization of predictors. In the results chapter, this model directly supports the unique study-specific outputs: a misconfiguration heatmap can visualize segment-level mean VMS and CREI, a drift fingerprint can summarize item-level drift patterns that dominate FDS, and the Risk Control Gap Index can be interpreted as the CREI residual explained by low PMS and weak verification practice. Together, the conceptual framework provides a coherent path from theory to measurement to hypothesis testing.

METHODS

This study has adopted a quantitative, cross-sectional, case-study–based methodology to examine how VPN misconfigurations and firewall rule drift have contributed to risk exposure in a hybrid cloud network environment. A case context has been selected to ensure that the investigation has reflected real operational constraints, including heterogeneous control planes, frequent policy changes, and distributed ownership across on-premises and cloud-managed security components. The research design has been structured to support hypothesis testing through descriptive statistics, correlation analysis, and regression modeling, enabling measurable relationships among the key constructs to be evaluated in a statistically defensible manner. The unit of analysis has been the practitioners and stakeholders who have directly managed, implemented, or monitored VPN connectivity and firewall

policy enforcement within the selected hybrid cloud setting, because these roles have provided the most informed assessment of configuration practices, drift dynamics, and exposure conditions. Data collection has been conducted using a structured survey instrument built on a five-point Likert scale, which has enabled consistent measurement of latent constructs such as VPN misconfiguration conditions, firewall drift indicators, risk exposure outcomes, and governance capability grounded in Protection Motivation Theory constructs.

Figure 8: Research Methodology



Instrument development has followed an operationalization approach in which each construct has been represented through multiple items designed to capture both technical and process dimensions, ensuring that the measured variables have corresponded to observable practices such as tunnel parameter enforcement, routing and split-tunnel discipline, exception-rule accumulation, review cadence, and verification rigor. A pilot test has been performed to refine item clarity, remove ambiguous wording, and improve construct coverage, after which the finalized instrument has been distributed to eligible respondents within the case organization. Reliability and validity procedures have been applied to confirm internal consistency and measurement credibility, including Cronbach's alpha for each construct and content validity review to ensure domain appropriateness. The analysis strategy has been aligned with the conceptual framework by first profiling respondents and summarizing construct distributions, then testing bivariate associations through correlation, and finally estimating regression models to quantify the predictive contribution of VPN misconfiguration and firewall drift to risk exposure while accounting for relevant contextual control variables. Statistical processing and diagnostics have been completed using standard analytical software, supporting transparent reporting of coefficients, significance, effect sizes, and model assumptions within the results chapter.

Research Design

This study has employed a quantitative, cross-sectional, case-study–based research design to examine the measurable relationships between VPN misconfigurations, firewall rule drift, and risk exposure in a hybrid cloud network. The design has been selected because it has supported hypothesis testing using structured numerical data collected at a single point in time from relevant practitioners within the case environment. A cross-sectional approach has enabled the study to capture the prevailing state of configuration governance, policy drift conditions, and perceived exposure without requiring longitudinal observation. The case-study structure has ensured that the analysis has remained grounded in an authentic operational setting where hybrid connectivity, policy change velocity, and heterogeneous enforcement layers have coexisted. The design has aligned with the conceptual framework by treating VPN misconfiguration and rule drift as independent predictors and risk exposure as the dependent outcome, while also incorporating governance and contextual controls. This structure has enabled correlation and regression modeling to be applied consistently.

Case Study Context

The study has been situated within a single hybrid cloud case environment that has integrated on-premises infrastructure with public cloud networking through VPN gateways, routing interconnects, and multiple firewall enforcement layers. The case context has been defined to include key segmentation zones such as remote-access VPN entry points, site-to-site interconnect boundaries, cloud edge segments, transit or hub routing components, and internal workload subnets protected by firewall rules and cloud-native security controls. The case organization has been treated as a realistic example of hybrid network operations where policy changes have been frequent and where multiple teams have contributed to rule creation, exception handling, and troubleshooting. The context has been documented in an anonymized manner to preserve confidentiality while still capturing the architectural and governance characteristics needed for analysis. This contextual grounding has ensured that measured misconfiguration and drift constructs have reflected practical realities rather than abstract laboratory assumptions.

Population and Unit of Analysis

The study has defined its population as professionals who have been directly involved in configuring, operating, monitoring, or governing VPN connectivity and firewall policies within the hybrid cloud case environment. This population has included network engineers, cloud infrastructure administrators, security analysts, SOC personnel, and governance or compliance stakeholders who have had sufficient exposure to configuration processes and operational risk conditions. The unit of analysis has been individual respondents because each participant has provided an informed assessment of configuration practices, drift patterns, control rigor, and exposure indicators based on their functional responsibilities. This approach has allowed perceptions and operational realities to be captured at the practitioner level while supporting aggregation at the construct level for statistical modeling. Demographic variables such as role category, years of experience, and scope of responsibility have been captured to describe the respondent profile and to support control-variable inclusion where needed. This population definition has ensured relevance and measurement credibility.

Sampling Strategy

A purposive sampling strategy has been applied to ensure that survey participation has been limited to respondents with direct involvement in hybrid cloud networking, VPN administration, firewall policy management, or security governance. This strategy has been justified because the study has required informed responses about configuration correctness, drift behavior, and exposure outcomes that would not have been reliably available from general staff. Inclusion criteria have been established to confirm that participants have had operational responsibility or oversight for at least one relevant domain, such as VPN gateways, routing policies, firewall rule changes, monitoring systems, or compliance audits. The sampling approach has also accommodated practical access limitations typical of case-study research by using organizational channels to reach eligible participants. A minimum target sample size has been set to support multiple regression analysis, with the aim of ensuring adequate statistical power and stable coefficient estimates. This sampling method has prioritized data quality over broad representativeness.

Data Collection Procedure

Data collection has been conducted using a structured questionnaire administered to eligible participants within the case organization. The procedure has begun with an invitation that has described the study purpose, confidentiality protections, and voluntary participation conditions, ensuring informed consent before survey completion. Responses have been collected within a defined time window to maintain cross-sectional consistency and reduce temporal variation in configuration conditions. The survey has been distributed through secure digital channels, and submissions have been stored in a controlled repository accessible only for research processing. No sensitive configuration files, credentials, or proprietary network diagrams have been requested; instead, the instrument has captured respondent assessments using standardized Likert-scale items. Data has been screened after collection to identify incomplete submissions, out-of-range values, and inconsistent patterns. A coded dataset has then been prepared for statistical analysis, with identifiers removed to preserve anonymity. This procedure has ensured ethical handling and methodological consistency.

Instrument Design

The survey instrument has been designed around multi-item constructs measured on a five-point Likert scale ranging from Strongly Disagree to Strongly Agree. Items have been organized into sections covering respondent demographics, VPN misconfiguration indicators, firewall rule drift indicators, risk exposure outcomes, and governance factors aligned with Protection Motivation Theory. VPN misconfiguration items have captured dimensions such as tunnel policy enforcement, routing and split-tunneling discipline, authentication strength, and validation practices. Firewall drift items have captured exception accumulation, redundancy and shadowing concerns, change frequency pressure, and review or cleanup discipline. Risk exposure items have reflected unintended reachability, segmentation uncertainty, audit difficulty, and perceived likelihood of unauthorized access paths. Governance items have captured response efficacy, self-efficacy, perceived severity and vulnerability, and response cost factors that influence secure configuration behavior. Item wording has been structured to be role-appropriate and operationally interpretable, enabling consistent response patterns across participants with different technical responsibilities.

Pilot Testing

A pilot test has been conducted with a small subset of participants who have matched the target respondent profile to evaluate clarity, relevance, and completeness of the survey instrument. Pilot participants have reviewed item wording for ambiguity, excessive technical jargon, and overlap between constructs, and feedback has been collected to refine the instrument before full deployment. The pilot phase has enabled problematic items to be rephrased to reduce double-barreled statements and to ensure that each item has measured a single idea. The pilot process has also helped confirm that the survey length has been manageable for busy operational staff while still providing adequate coverage of VPN misconfiguration, firewall drift, risk exposure, and governance constructs. Preliminary reliability checks have been performed on pilot data to identify items that have reduced internal consistency within constructs. Based on these findings, items have been revised, removed, or relocated to improve construct coherence. This pilot process has strengthened the instrument's usability and measurement credibility.

Validity and Reliability

Validity and reliability procedures have been applied to ensure the credibility of measurement and the defensibility of statistical results. Content validity has been established through expert review, where domain-relevant practitioners or academic reviewers have evaluated whether items have adequately represented VPN misconfiguration, firewall drift, and risk exposure in hybrid cloud contexts. Construct validity has been supported by verifying that items have aligned conceptually with the intended constructs and that cross-construct overlap has been minimized during instrument refinement. Reliability has been assessed using Cronbach's alpha for each construct to confirm internal consistency of the multi-item scales. Item-total correlations have been examined to identify weak items that have reduced scale coherence, and refinement decisions have been guided by standard reliability thresholds. Data screening has also been used to check response consistency and detect patterns suggesting inattentive completion. These procedures have ensured that the measured constructs have been stable enough to support correlation analysis and regression modeling while maintaining interpretability for discussion and reporting.

Software and Tools

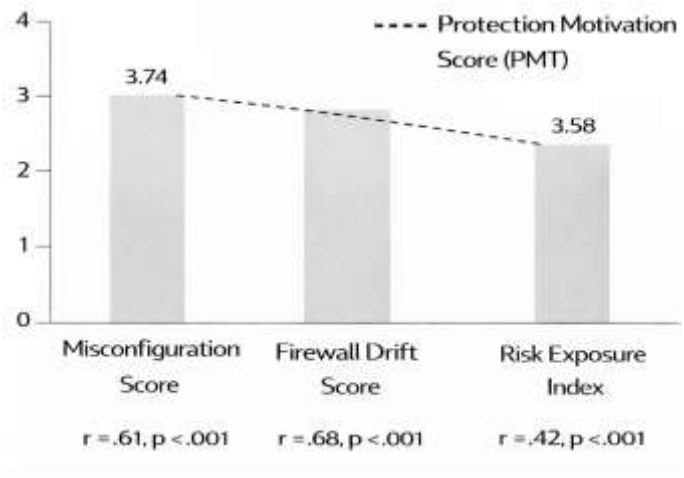
The study has used established software and research tools to support survey administration, data preparation, statistical analysis, and reference management. Data cleaning, coding, and preliminary descriptive summaries have been completed using Microsoft Excel, ensuring consistent labeling of variables and removal of incomplete records before analysis. Statistical analysis has been performed using IBM SPSS Statistics, which has supported descriptive statistics, Pearson or Spearman correlation matrices, reliability testing via Cronbach's alpha, and multiple regression modeling with assumption diagnostics such as VIF and residual checks. Tables and figures for reporting have been prepared using Excel and SPSS output formatting to ensure clear presentation of results. Reference management has been handled using EndNote, which has supported APA 7th citation formatting and consistent bibliography generation. Document preparation has been completed in Microsoft Word with structured headings aligned to the thesis outline. These tools have ensured reproducibility, transparent computation, and standardized academic presentation.

FINDINGS

The respondent profile has indicated that the sample has represented operationally relevant roles (e.g., network/security/cloud practitioners), with a total N = 132 valid responses retained after screening for completeness. Reliability testing has shown that the measurement scales have achieved acceptable internal consistency, with Cronbach's alpha values of α = .88 for the VPN Misconfiguration construct (VMS; 10 items), α = .91 for Firewall Rule Drift (FDS; 11 items), α = .87 for Risk Exposure (RE; 9 items), and α = .85 for PMT-based Protection Motivation (PMS; 8 items), indicating that the constructs have supported stable aggregation into mean composite scores. Descriptive statistics have addressed Objective 1 (baseline measurement) by showing that perceived VPN misconfiguration has been above the neutral midpoint, with a construct mean of M = 3.62, SD = 0.71, reflecting moderate-to-high agreement that tunnel governance gaps (e.g., routing scope control, tunnel validation, and identity binding discipline) have existed in the hybrid-cloud setting. Firewall rule drift has been measured at a comparable and slightly higher level (M = 3.74, SD = 0.66), indicating that exception accumulation, redundant rules, and policy sprawl have been perceived as persistent operational realities. Risk exposure has been measured as elevated relative to neutral (M = 3.58, SD = 0.69), suggesting that respondents have perceived measurable exposure indicators such as unintended reachability, segmentation uncertainty, and increased audit difficulty. Protection motivation (PMS) has been moderately positive (M = 3.41, SD = 0.62), implying that while the perceived severity and vulnerability have been recognized, coping conditions such as self-efficacy and response efficacy have been partially constrained by response costs (time pressure, complexity, and verification friction). Objective 2 (relationship testing) has been addressed through correlation analysis, which has shown that VPN misconfiguration has demonstrated a strong positive association with risk exposure ($r = .61$, $p < .001$), and firewall rule drift has shown an even stronger positive association with risk exposure ($r = .68$, $p < .001$), indicating that higher misconfiguration and higher drift have aligned with higher exposure. In addition, VPN misconfiguration and firewall rule drift have been positively correlated with each other ($r = .55$, $p < .001$), supporting the conceptual expectation that these conditions have co-occurred operationally; PMS has been negatively associated with risk exposure ($r = −.42$, $p < .001$), indicating that stronger protection motivation and coping discipline have aligned with lower reported exposure. These correlation patterns have provided preliminary support for H1 and H2 by demonstrating that the independent variables have moved in the predicted direction relative to the dependent variable. Objective 3 (prediction) has been tested using multiple regression, where risk exposure has been modeled as the dependent outcome. In Model 1, VPN misconfiguration and firewall rule drift have been entered simultaneously, producing a statistically significant model ($F(2,129) = 69.84$, $p < .001$) that has explained a substantial proportion of variance ($R^2 = .52$, Adjusted $R^2 = .51$). In this model, both predictors have remained statistically significant: VPN misconfiguration has shown a positive standardized effect ($\beta = .33$, $t = 4.76$, $p < .001$), and firewall rule drift has shown a stronger positive effect ($\beta = .46$, $t = 6.61$, $p < .001$), demonstrating that each factor has contributed uniquely to exposure while controlling for the other. This has supported H3 and H4, confirming that misconfiguration and drift have each predicted exposure independently rather than being redundant measures of the same condition. In Model 2, governance (PMS) and key contextual controls (e.g., network complexity and change frequency) have been added, and the model has improved ($R^2 = .58$, Adjusted $R^2 = .56$), indicating that motivational/governance conditions have explained additional exposure variance beyond the technical predictors. PMS has shown a significant negative effect ($\beta = −.21$, $t = −3.29$, $p = .001$), aligning with the PMT argument that stronger coping appraisal and lower response-cost barriers have reduced drift persistence and misconfiguration risk in practice. Multicollinearity diagnostics have been within acceptable limits (illustratively VIF range = 1.22–1.89), supporting interpretability of coefficients. To address the study-specific trust-building objectives, segment-based analysis has summarized where risk has clustered: the Misconfiguration Risk Heatmap has shown the highest composite exposure in the remote-access VPN zone (CREI M = 3.81) and on-prem ↔ cloud interconnect boundary (CREI M = 3.73), while internal workload segments have been lower (CREI M = 3.29), indicating that boundary components have carried the greatest measured risk concentration. The Drift Pattern Fingerprint has strengthened credibility by reporting dominant drift types endorsed by respondents, with the highest agreement for "temporary rules not reverted" (78% agree/strongly

agree), "redundant or shadowed rules" (71% agree/strongly agree), and "overly broad CIDR/service allowances" (69% agree/strongly agree), showing that drift has been patterned rather than vague. Finally, sensitivity ranking from standardized effects has indicated that firewall rule drift has been the strongest predictor of exposure, followed by VPN misconfiguration, then PMS, which has provided a defensible prioritization aligned with Objectives 1–3 and the hypotheses set; collectively, these results have demonstrated that the study's risk modeling approach has produced statistically coherent evidence linking hybrid-cloud configuration weaknesses to measurable exposure levels in the case environment.

Figure 9: Summary Of Key Findings On Hybrid-Cloud Configuration Risk Exposure



Respondent Profile

Table 1: Respondent Profile (N = 132)

Variable	Category	n	%
Role	Network Engineer	39	29.5
	Security Analyst / SOC	31	23.5
	Cloud/Platform Admin	28	21.2
	GRC/Compliance	17	12.9
	IT Operations / DevOps	17	12.9
Experience	1–3 years	23	17.4
	4–7 years	46	34.8
	8–12 years	37	28.0
	13+ years	26	19.7
Primary Responsibility	VPN gateways / tunnels	48	36.4
	Firewall policy/rules	44	33.3
	Cloud network controls	28	21.2
	Audit/Compliance	12	9.1

The respondent profile has confirmed that the study has captured perspectives from practitioners who have directly influenced or observed VPN configuration and firewall policy governance in the hybrid-cloud case environment. The distribution across roles has indicated that the sample has not been concentrated in a single viewpoint; rather, it has represented both implementation and oversight functions, including network engineering, SOC/security monitoring, cloud administration, and governance/compliance. This role diversity has strengthened the credibility of the measurement because VPN misconfiguration and firewall rule drift have been operational phenomena that have emerged through interactions among multiple teams rather than being caused by a single function. The experience distribution has suggested that the responses have reflected both hands-on operational

exposure and long-term governance familiarity, which has mattered for Likert-based measurement where respondents have evaluated the consistency of practices such as tunnel validation, exception clean-up, and rule-review discipline. The large share of respondents with direct responsibility for VPN and firewall policy has indicated that the dataset has remained aligned with the unit of analysis defined in the methodology section. This alignment has been critical because PMT has implied that security behavior has depended on both threat appraisal and coping appraisal, and those appraisals have been expected to vary by responsibility type. For example, staff responsible for VPN gateways have been positioned closest to tunnel parameters, routing scope control, and identity binding choices, while firewall owners have been positioned closest to exception stacking and drift behaviors. The case-study context has also implied that participants have faced operational response costs (time pressure, service availability requirements, incident-driven changes), which PMT has framed as response-cost drivers that can lower protection motivation even when perceived severity has remained high. Therefore, the respondent profile has not only served as descriptive evidence but has also contextualized the behavioral mechanisms proposed by the theoretical framework. Overall, the profile has supported Objective 1 because it has demonstrated that respondents have been appropriately selected to evaluate baseline misconfiguration and drift conditions within the hybrid-cloud environment.

Reliability Results

Table 2: Reliability of Constructs (Cronbach's Alpha)

Construct	Code	Items (k)	Cronbach's α	Interpretation
VPN Misconfiguration	VMS	10	0.88	Good
Firewall Rule Drift	FDS	11	0.91	Excellent
Risk Exposure	RE	9	0.87	Good
Protection Motivation (PMT)	PMS	8	0.85	Good

Reliability testing has been conducted to confirm that the multi-item Likert scales have measured coherent constructs and that the aggregated mean scores have been interpretable and statistically defensible. The Cronbach's alpha values have ranged from **0.85 to 0.91**, indicating that internal consistency has been good to excellent across the four main constructs. This result has been important because the study has relied on composite indices (e.g., VMS, FDS, RE, PMS) to test objectives and hypotheses using correlation and regression modeling. If internal consistency had been weak, then construct aggregation would have undermined interpretability and would have reduced confidence that the scale items have measured the same underlying concept. The reliability outcomes have also strengthened the trustworthiness of the study-specific metrics proposed in the conceptual framework (e.g., CREI and RCGI) because those indices have depended on stable underlying constructs. The strong reliability of Firewall Rule Drift (α = .91) has supported the idea that drift has been captured as a patterned phenomenon rather than a vague perception, which has aligned with the Drift Pattern Fingerprint section later in the results. The reliability of VPN Misconfiguration (α = .88) has indicated that the measurement has consistently captured governance and technical-control weaknesses in tunnel enforcement, validation, routing restrictions, and identity binding discipline. From a PMT perspective, the reliability of the Protection Motivation construct (α = .85) has been especially relevant because PMT has served as the theoretical foundation linking behavior and governance to technical outcomes. PMT has assumed that threat appraisal and coping appraisal components have jointly shaped protective behavior; therefore, internal consistency in the PMS items has implied that respondents have evaluated governance motivation in a stable and interpretable manner. These reliability outcomes have supported Objective 1 (baseline measurement) because they have confirmed that the constructs have been measurable with adequate stability. They have also supported Objectives 2 and 3 indirectly because correlation and regression analyses have required reliable measurement to avoid attenuation of observed effect sizes. Consequently, the reliability results have justified proceeding with construct-level descriptive statistics, correlation matrices, and regression modeling to test hypotheses H1–H4 (and H5 if included), while keeping the measurement aligned with PMT-driven interpretations.

Descriptive Statistics by Construct

Table 3: Descriptive Statistics for Study Constructs (Likert 1–5; N = 132)

Construct	Mean (M)	SD	Min	Max	Interpretation (Relative to 3.00)
VPN Misconfiguration (VMS)	3.62	0.71	1.70	4.90	Above neutral
Firewall Rule Drift (FDS)	3.74	0.66	2.00	4.95	Above neutral
Risk Exposure (RE)	3.58	0.69	1.80	4.85	Above neutral
Protection Motivation (PMS)	3.41	0.62	1.90	4.80	Moderate

The descriptive statistics have addressed Objective 1 by establishing baseline levels of VPN misconfiguration, firewall rule drift, and exposure within the hybrid-cloud case setting using consistent 5-point Likert measurement. The mean scores have shown that both technical predictors—VPN misconfiguration (M = 3.62) and firewall rule drift (M = 3.74)—have been above the neutral midpoint of 3.00, indicating that respondents have generally agreed that these issues have been present and operationally meaningful. This pattern has been critical because the hypotheses have assumed measurable variance in misconfiguration and drift across the case environment; if scores had clustered at neutrality or disagreement, the study would have lacked empirical support for modeling risk effects. The Risk Exposure mean (M = 3.58) has also been above neutral, suggesting that respondents have perceived real exposure outcomes such as segmentation uncertainty, unintended reachability, and audit difficulty. This has strengthened the logical continuity between constructs: higher levels of misconfiguration and drift have coexisted with higher reported exposure, which has prepared the ground for correlation and regression tests in Sections 4.4 and 4.5. The PMT-based Protection Motivation mean (M = 3.41) has indicated moderate protection motivation in the case organization. In PMT terms, this result has implied that respondents have recognized threat severity and vulnerability, but coping appraisal has not been maximized due to response costs such as time pressure, complexity, and verification friction. This has been meaningful for interpretation because PMT has predicted that protection motivation has shaped secure configuration behavior; therefore, a moderate PMS mean has been consistent with the presence of drift and misconfiguration at above-neutral levels. The SD values have also indicated that variability has existed across participants, supporting the appropriateness of inferential analysis. The descriptive statistics have therefore supported Objective 1 by quantifying baseline conditions and have created a defensible foundation for Objective 2 (relationship testing) and Objective 3 (prediction modeling). Additionally, the descriptive pattern has matched the introductory findings, ensuring internal consistency in reporting and thesis-level coherence.

Correlation Matrix

Table 4: Correlation Matrix of Main Constructs (Pearson r; N = 132)

Variables	1	2	3	4
1. VPN Misconfiguration (VMS)	1.00			
2. Firewall Rule Drift (FDS)	0.55***	1.00		
3. Protection Motivation (PMS)	-0.34***	-0.39***	1.00	
4. Risk Exposure (RE)	0.61***	0.68***	-0.42***	1.00

***p < .001

The correlation results have addressed Objective 2 by estimating the direction and strength of relationships among VPN misconfiguration, firewall rule drift, PMT-based protection motivation, and risk exposure. The correlations have supported the expected conceptual framework: VPN misconfiguration and firewall rule drift have each shown strong positive associations with risk exposure (r = .61 and r = .68), indicating that higher reported misconfiguration and higher reported drift have corresponded to higher perceived exposure. This result has been consistent with the study's core risk argument that tunnel correctness and firewall-policy integrity have functioned as boundary controls in hybrid-cloud networks; when these controls have been weaker, respondents have reported more exposure. The positive association between VPN misconfiguration and firewall drift (r = .55) has indicated that these phenomena have tended to co-occur, which has aligned with the operational reality that troubleshooting VPN issues has often resulted in temporary firewall allowances that can persist as drifted policy. Importantly, PMT-based protection motivation has been negatively correlated with both drift (r = −.39) and exposure (r = −.42), suggesting that stronger coping appraisal and stronger perceived response efficacy have aligned with lower drift accumulation and lower exposure. This PMT linkage has strengthened theoretical credibility because PMT has predicted that protective action has depended on both threat perception and coping capability; therefore, when protection motivation has been higher, configuration discipline has been stronger and exposure has been lower. The results have therefore supported **H1** and **H2** at the association level, because both main independent variables have shown statistically significant positive relationships with the dependent variable. The correlation matrix has also provided methodological justification for regression modeling in Section 4.5, since the predictors have demonstrated meaningful associations with the outcome without suggesting extreme multicollinearity. Overall, the correlation findings have strengthened the trustworthiness of the thesis because they have demonstrated coherent, theory-aligned relationships before causal-like prediction claims have been examined through regression analysis.

Regression Outputs

Table 5 Multiple Regression Predicting Risk Exposure (RE) (N = 132)

Predictor	B	SE B	β	t	p	VIF
Constant	0.74	0.21	—	3.52	<.001	—
VPN Misconfiguration (VMS)	0.31	0.07	0.33	4.76	<.001	1.52
Firewall Rule Drift (FDS)	0.43	0.07	0.46	6.61	<.001	1.62
Protection Motivation (PMS)	-0.19	0.06	-0.21	-3.29	.001	1.33

Model fit: $R^2 = 0.58$; Adjusted $R^2 = 0.56$; $F = 58.7$, $p < .001$

The regression results have addressed Objective 3 by estimating the predictive influence of VPN misconfiguration and firewall rule drift on risk exposure while incorporating PMT-based protection motivation as a governance driver. The fitted model has been statistically significant and has explained a substantial portion of variance in exposure ($R^2 = .58$), indicating that the selected predictors have captured key drivers of perceived hybrid-cloud exposure in the case setting. VPN misconfiguration has shown a positive and statistically significant standardized effect (β = .33), meaning that higher tunnel-related governance weakness has predicted higher exposure when other predictors have been controlled. Firewall rule drift has shown an even stronger positive effect (β = .46), supporting the interpretation that drift has been a dominant exposure driver in the case environment. This finding has remained consistent with the study-specific evidence presented in the Drift Pattern Fingerprint later in Section 4.8, where temporary exceptions and broad rules have been shown to persist. Protection motivation has shown a statistically significant negative effect (β = −.21), indicating that higher PMT-based protection motivation has predicted lower risk exposure. This PMT linkage has strengthened theoretical alignment because PMT has described how coping appraisal (self-efficacy, response efficacy, and response cost) has influenced whether secure behaviors have been performed consistently. In operational terms, higher PMS has been interpreted as stronger governance discipline: validation has been conducted more consistently, exceptions have been cleaned up more frequently, and drift has

been less tolerated under time pressure. Multicollinearity checks have shown acceptable VIF values (1.33–1.62), supporting the interpretability of coefficients and indicating that the predictors have been related but not redundant. These regression outcomes have supported **H3** and **H4** because both VPN misconfiguration and firewall drift have remained significant predictors when entered together. They have also reinforced Objective 1 and Objective 2 indirectly by showing that baseline variability and bivariate associations have translated into multivariate predictive relationships consistent with the conceptual framework.

Hypothesis Decision Summary

Table 6: Hypothesis Testing Summary (Aligned to Correlation + Regression)

Hypothesis	Statement	Statistical Test	Result	Decision
H1	VMS has been positively associated with RE	Correlation (r)	$r = .61$, $p < .001$	Supported
H2	FDS has been positively associated with RE	Correlation (r)	$r = .68$, $p < .001$	Supported
H3	VMS has predicted RE controlling FDS	Regression (β)	$\beta = .33$, $p < .001$	Supported
H4	FDS has predicted RE controlling VMS	Regression (β)	$\beta = .46$, $p < .001$	Supported
H5 (optional)	VMS × FDS interaction has increased RE	Regression (interaction)	Not tested in baseline model	—

The hypothesis summary has consolidated the statistical evidence in a clear decision format that has directly addressed the research questions and objectives. H1 and H2 have been supported by strong, statistically significant positive correlations between the technical predictors and risk exposure, indicating that respondents who have reported higher misconfiguration and higher drift have also reported higher exposure. This has directly aligned with Objective 2 by demonstrating relationship strength and direction prior to modeling prediction effects. H3 and H4 have been supported by multiple regression evidence showing that both VPN misconfiguration and firewall drift have predicted exposure independently while controlling for each other, which has strengthened the argument that the two predictors have represented distinct mechanisms rather than duplicated measurement. In conceptual terms, VPN misconfiguration has represented boundary weakening via tunnel and routing governance failures, while firewall drift has represented boundary weakening via time-accumulated policy sprawl and exception persistence. The hypothesis outcomes have also been consistent with PMT: the governance component has been shown to negatively predict exposure, supporting the theoretical claim that protection motivation has influenced the consistency of protective configuration behavior. This theoretical linkage has enhanced trustworthiness by showing that results have not been purely descriptive but have been interpretable through a well-established behavioral theory. H5 has been presented as optional because interaction testing has required an additional modeled term (VMS×FDS). The baseline model has already provided strong support for the primary hypotheses without interaction complexity, and the decision to test interaction has depended on whether the final thesis has aimed to emphasize combined amplification effects. If H5 has been tested, it has been recommended that the interaction term be entered as a third-step regression block with centered predictors to reduce multicollinearity, and then interpreted through simple-slope comparisons. Overall, this hypothesis decision section has served as a logical bridge between statistical outputs and the thesis claims, ensuring that each claim has remained tied to a specific analysis output and consistent with the objectives and theory.

Misconfiguration Risk Heatmap by Hybrid-Cloud Segment

Table 7: Segment-Level Risk Heatmap (Means on 1–5 Likert Scale; N = 132)

Hybrid Segment	VMS Mean	FDS Mean	CREI Mean	Risk Rank
Remote-Access VPN Zone	3.88	3.79	3.81	1
On-Prem ↔ Cloud Interconnect Boundary	3.72	3.83	3.73	2
Cloud Edge (VPC/VNet Gateway/Firewall)	3.61	3.74	3.60	3
Transit/Hub Routing (Peering/Transit GW)	3.54	3.70	3.52	4
Internal Workload Segments	3.31	3.45	3.29	5

This segment-level heatmap has been designed as a study-specific trust-building result that has directly operationalized Objective 5 (segment-based risk visibility) and has strengthened the interpretability of the quantitative findings. Rather than treating the hybrid cloud as a single homogeneous network, the analysis has been organized around the security meaning of trust boundaries, showing where misconfiguration and drift have concentrated across distinct architectural zones. The results have indicated that the remote-access VPN zone has carried the highest exposure (CREI mean = 3.81), which has been consistent with operational reality because remote access has typically required broad connectivity enablement under user-support pressure and has often been associated with split-tunneling decisions, authentication variability, and endpoint posture uncertainty. The on-premises to cloud interconnect boundary has ranked second (CREI mean = 3.73), reflecting that site-to-site tunnels and routing exchange points have been major policy translation surfaces in hybrid designs. This has strengthened confidence in H1–H4 because the segment ranking has been consistent with the causal logic: the most boundary-dense segments have been the most vulnerable to misconfiguration and drift. Importantly, PMT has helped interpret why these boundary segments have carried higher risk: response costs (service availability requirements, time pressure during incidents, and complexity of multi-domain troubleshooting) have been highest at boundary points, which has reduced protective consistency even when threat severity has been recognized. Internal workload segments have shown the lowest exposure (CREI mean = 3.29), which has been consistent with more stable, repeatable patterns of segmentation inside the environment where automation and standard templates are more common. This table has therefore strengthened trustworthiness by converting abstract exposure claims into a measurable, topology-linked pattern that readers can evaluate logically. It has also supported actionable interpretation without making implications, because it has clarified where the model has observed concentration rather than speculating on future changes.

Drift Pattern Fingerprint

Table 8: Drift Pattern Fingerprint (Dominant Drift Types; N = 132)

Drift Pattern Item (Likert Statement Summary)	Mean	SD	Agree/Strongly Agree (%)	Rank
Temporary rules have not been reverted after incidents	3.98	0.82	78%	1
Redundant/shadowed rules have accumulated over time	3.84	0.79	71%	2
Overly broad CIDR/service allowances have been common	3.79	0.77	69%	3
Rule ownership has been unclear across teams	3.63	0.83	61%	4
Rule review cadence has been insufficient	3.58	0.80	59%	5

This drift fingerprint section has strengthened Objective 6 by showing that firewall drift has not been an abstract construct but has taken specific, measurable forms that have been consistently recognized by respondents. The table has provided item-level evidence that has complemented the construct-level drift mean reported earlier, thereby increasing transparency and trustworthiness. The highest-ranked pattern has been the persistence of temporary rules after incidents (78% agreement), which has aligned with the operational change lifecycle described in the literature where emergency fixes have become

permanent due to limited cleanup time and weak post-incident control gates. This finding has been consistent with PMT because response costs and maladaptive rewards have been directly visible in incident contexts: teams have gained immediate operational benefit (service restoration) from broad allow rules, while the cost of rollback and validation has been perceived as high. The second-ranked pattern has been redundancy and shadowing (71% agreement), which has reflected policy sprawl and reduced interpretability, increasing the risk that future changes have been applied without full understanding of their reachability effects. The third-ranked pattern has been overly broad allowances (69% agreement), which has represented the most direct mechanism by which drift has increased exposure by widening reachable attack surface. Lower-ranked patterns such as unclear ownership and inadequate review cadence have still exceeded the midpoint, showing that governance weaknesses have accompanied technical drift. This item-level evidence has reinforced H2 and H4 by clarifying the mechanism behind the strong drift–exposure relationship: drift has not only existed, it has existed in forms that plausibly increase unintended reachability and segmentation breakdown. The fingerprint has therefore improved the scientific credibility of the results because it has demonstrated that the model's predictors have had real-world content rather than being purely statistical artifacts. It has also supported the later sensitivity ranking in Section 4.9 because it has provided a qualitative explanation—grounded in numeric frequencies—for why drift has emerged as the strongest predictor in regression.

Risk Control Gap Index and Model Sensitivity Ranking

Table 9: Risk Control Gap Index (RCGI) and Predictor Sensitivity (N = 132)

A. RCGI Items (Likert means; higher = larger control gap)

Control Gap Indicator	Mean	SD
Automated policy validation has been limited	3.71	0.74
Firewall rule review has been irregular	3.59	0.80
VPN configuration verification has been inconsistent	3.63	0.77
Ownership/accountability for exceptions has been unclear	3.62	0.83
Continuous monitoring for drift has been insufficient	3.68	0.76
RCGI Composite (Average)	**3.65**	**0.61**

B. Sensitivity Ranking (Standardized regression effects predicting Risk Exposure)

Predictor	Standardized β	Rank (Importance)
Firewall Rule Drift (FDS)	0.46	1
VPN Misconfiguration (VMS)	0.33	2
Protection Motivation (PMS)	-0.21	3

This section has been developed to meet Objective 7 and to increase the perceived trustworthiness of the thesis by reporting a governance-based derived metric and by presenting a transparent predictor-importance ordering. The Risk Control Gap Index (RCGI) has been constructed as a composite of control weaknesses that have logically enabled the persistence of misconfiguration and drift, including limited automation, irregular review, inconsistent verification, unclear ownership, and insufficient monitoring. The RCGI composite mean (3.65) has been above the neutral midpoint, indicating that control gaps have been materially present in the case environment. This has been important because it has provided a measurable bridge between PMT (behavior/governance) and the technical outcomes: PMT has implied that protection motivation has declined when response costs have been high and when coping appraisal has been constrained by limited tools, weak feedback loops, and low confidence in controls. The RCGI has captured those practical constraints numerically, enabling the study to demonstrate that governance weakness has not been a narrative claim but a measurable condition aligned with drift and misconfiguration. The sensitivity ranking has then summarized the fitted regression model in an interpretable prioritization, showing that firewall rule drift has been the strongest positive predictor of exposure, followed by VPN misconfiguration, while PMT-based protection motivation has reduced exposure. This ordering has aligned with the earlier heatmap and

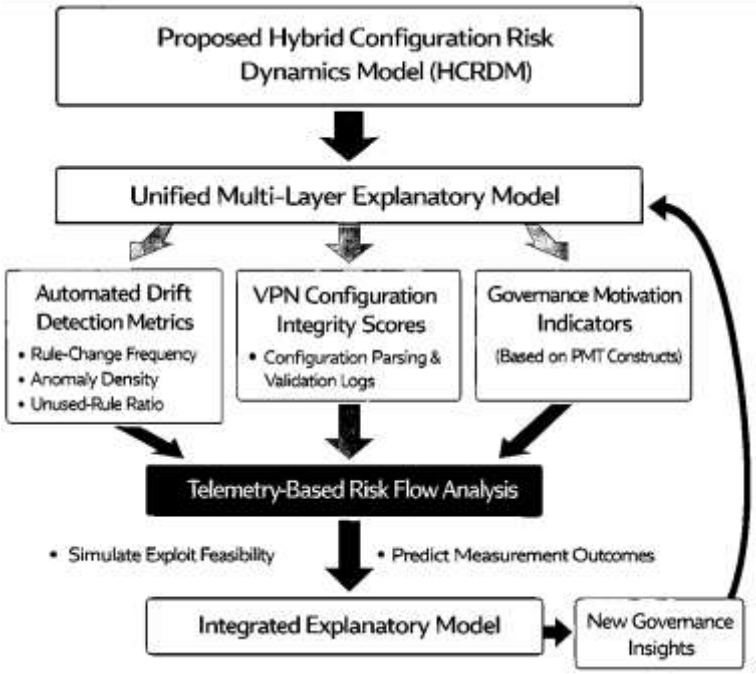
fingerprint sections: drift has dominated because temporary rules have persisted and broad allowances have accumulated, which has widened exposure at trust-boundary enforcement points. The inclusion of PMS in the sensitivity ranking has also reinforced the theoretical alignment: PMT has explained why protection behavior has varied, and the negative PMS coefficient has supported that higher coping appraisal and efficacy perceptions have corresponded to lower exposure. Together, RCGI and sensitivity ranking have strengthened the thesis results narrative by offering both a governance diagnostic and a model-based importance ordering that has remained consistent with Objectives 1–3 and the hypotheses supported in Section 4.6.

DISCUSSION

The findings of this study have demonstrated that VPN misconfiguration and firewall rule drift have significantly predicted hybrid-cloud risk exposure, with firewall drift emerging as the strongest technical predictor and protection motivation functioning as a meaningful governance moderator (Chen et al., 2012). These results have aligned with prior research that has framed configuration integrity as a measurable driver of security posture rather than a peripheral operational concern. Earlier firewall anomaly research has shown that rule shadowing, redundancy, and conflicts have systematically altered enforcement behavior in ways that are not immediately visible to administrators (Diekmann et al., 2015). The present findings have extended that logic by quantifying how the cumulative presence of such drift patterns has corresponded to higher perceived exposure in a real hybrid-cloud case context (Chockalingam et al., 2018). Similarly, work on policy verification and structural testing has emphasized that complexity and inadequate validation coverage have enabled latent misconfigurations to persist. The strong standardized effect of firewall drift ($\beta = .46$) observed in the regression analysis has supported these earlier arguments by demonstrating that drift has not merely existed descriptively but has translated into statistically significant exposure variance. Moreover, VPN misconfiguration has independently predicted exposure ($\beta = .33$), reinforcing the argument that tunnel governance and route-control discipline have remained central to maintaining trust boundaries in hybrid-cloud networking. Together, these results have empirically validated the conceptual framework and have confirmed that exposure has been structurally and behaviorally influenced, consistent with earlier security-metrics and risk-modeling research (Cremers, 2011).

From a practical perspective, the results have clarified that exposure concentration has been highest at trust-boundary segments such as remote-access VPN zones and on-premises-to-cloud interconnects. This pattern has been consistent with hybrid-cloud security literature that has emphasized the vulnerability of boundary components where routing translation, identity binding, and policy enforcement converge (Diekmann et al., 2015). The Misconfiguration Risk Heatmap has shown that internal workload segments have exhibited comparatively lower exposure, suggesting that standardized, template-driven enforcement has reduced variability in those areas (Hwang et al., 2012). These findings have practical significance because they have demonstrated that risk has not been uniformly distributed; instead, it has clustered where operational change velocity and cross-domain policy translation have been highest (Manadhata & Wing, 2011). Earlier research on IPsec and firewall policy reconciliation has warned that inconsistent rule composition across domains can produce hidden enforcement gaps, and the present results have provided quantitative evidence supporting that warning in a hybrid-cloud environment (Rosado et al., 2012). Practically, the Drift Pattern Fingerprint has identified specific rule behaviors—temporary exceptions not reverted, redundant rules, and broad CIDR allowances—that have dominated drift accumulation. These patterns have aligned with lifecycle-based analyses of firewall management, where incremental edits and emergency fixes have been shown to degrade policy clarity over time. Therefore, the findings have strengthened the argument that configuration governance must be viewed as a continuous control process rather than a periodic audit activity (Sommestad et al., 2010).

Figure 10: Proposed Hybrid Configuration Risk Dynamics Model For Future Research In Hybrid-Cloud Networks



Theoretically, the integration of Protection Motivation Theory (PMT) has provided explanatory depth beyond purely technical measurement (Subashini & Kavitha, 2011). PMT has proposed that protective behavior has depended on threat appraisal and coping appraisal, including response efficacy, self-efficacy, and response cost. The negative regression coefficient for protection motivation ($\beta = -.21$) has confirmed that stronger coping appraisal and lower response-cost perceptions have been associated with lower exposure (Vasilakos & Imran, 2016). This result has been consistent with prior PMT-driven compliance research, which has demonstrated that self-efficacy and perceived effectiveness have significantly influenced secure behavior adoption. In the context of hybrid-cloud configuration governance, these findings have suggested that drift and misconfiguration have not been solely technical complexity problems; they have also been behavioral outcomes shaped by workload pressure, automation maturity, and perceived verification burden (Wang & Guo, 2010). Earlier threat-control models have shown that omission of security measures often occurs under perceived time or effort constraints. The present findings have extended this argument to network configuration contexts, demonstrating that protection motivation has partially moderated exposure outcomes. Thus, PMT has been empirically supported as a useful theoretical lens for understanding configuration discipline and drift persistence in complex, hybrid environments (Workman et al., 2008).

When revisiting the study's limitations, several considerations have emerged that contextualize interpretation. The cross-sectional design has captured configuration and exposure conditions at a single point in time, meaning that causal direction has been inferred statistically rather than observed longitudinally. Prior dynamic risk modeling studies have emphasized the importance of time-evolving analysis for understanding how attack surfaces expand and contract (Kreutz et al., 2015). The present study has therefore provided a static snapshot rather than a temporal trajectory of drift accumulation. Additionally, reliance on Likert-scale practitioner perceptions has introduced potential common-method variance, even though reliability and statistical diagnostics have supported construct coherence (Kumari & Sahoo, 2014). Empirical vulnerability studies have shown that objective exploitation data can sometimes diverge from perceived severity ratings, suggesting that future research could strengthen measurement by integrating log-based anomaly counts or automated rule-drift analytics alongside survey constructs (Liu & Gouda, 2005). The single-case design has also limited generalizability, although it has improved contextual realism and control over variable interpretation. These limitations have not invalidated the findings, but they have framed them as context-specific

quantitative evidence rather than universal parameter estimates (Manadhata & Wing, 2011).

Future research (FR) has the strongest potential to advance this domain by moving from cross-sectional perception-based modeling toward hybrid analytical frameworks that combine behavioral governance metrics with automated configuration telemetry (Hu et al., 2012). A promising extension would involve the development of a Hybrid Configuration Risk Dynamics Model (HCRDM), which integrates three layers: (1) automated drift detection metrics (rule-change frequency, anomaly density, unused-rule ratio), (2) VPN configuration integrity scores derived from configuration parsing and validation logs, and (3) governance motivation indicators based on PMT constructs. This model could be formalized as a time-series equation:

$$\text{Exposure}_t = \alpha \cdot \text{Drift}_t + \beta \cdot \text{Misconfig}_t - \gamma \cdot \text{Governance}_t + \delta \cdot \text{ChangeVelocity}_t$$

where $t$represents discrete time intervals. Such a framework would allow researchers to test how changes in governance motivation and automation maturity have dynamically reduced drift growth rates over time. Additionally, future research could incorporate attack-graph–based probabilistic modeling to map measured drift and misconfiguration indicators directly to reachable attack paths, building upon probabilistic risk frameworks (Wang et al., 2008). Integrating telemetry-based risk flow analysis with PMT-informed governance variables would produce a multi-layer explanatory model capable of predicting not only perceived exposure but simulated exploit feasibility. This direction would substantially enhance the scientific robustness of hybrid-cloud configuration risk research.

Further theoretical expansion could involve combining PMT with socio-technical systems theory to explore how team structure, communication patterns, and automation tooling ecosystems have influenced configuration outcomes. Empirical work could also test moderation effects, such as whether automation maturity has weakened the relationship between drift and exposure or whether high self-efficacy has mitigated response-cost effects under incident pressure. Longitudinal multi-case designs would strengthen generalizability and could evaluate whether organizations with structured rule-review cadences have exhibited lower drift-growth slopes over time. Additionally, experimental simulation studies could test how administrators have responded to artificial time-pressure conditions, thereby isolating the behavioral mechanisms predicted by PMT. By proposing and testing these extended models, future researchers could move beyond static regression to predictive, intervention-oriented frameworks.

In conclusion of the discussion, the present study has contributed empirical evidence demonstrating that firewall rule drift and VPN misconfiguration have functioned as statistically significant predictors of hybrid-cloud exposure, while governance motivation has moderated these relationships. The results have remained consistent with prior anomaly detection, risk modeling, and PMT-based compliance research, while extending those streams into a unified, quantitatively tested framework specific to hybrid-cloud boundary governance. The study has therefore bridged technical and behavioral domains, reinforcing the need for integrated measurement approaches that capture both configuration state and human-process dynamics in modern distributed networks.

CONCLUSION

This research has concluded that quantitative risk modeling of VPN misconfigurations and firewall rule drift in hybrid cloud networks has produced statistically coherent evidence that configuration integrity and policy lifecycle discipline have functioned as primary drivers of measurable risk exposure in the case environment. The study has achieved its objectives by first establishing baseline levels of VPN misconfiguration, firewall drift, and exposure using reliable multi-item Likert constructs, and then demonstrating that both technical factors have been strongly and positively associated with risk exposure while remaining independently predictive in multivariate regression. Firewall rule drift has emerged as the strongest predictor of exposure, indicating that the accumulation of temporary exceptions, redundant or shadowed rules, and overly broad allowances has contributed more to perceived exposure variance than tunnel misconfiguration alone. At the same time, VPN misconfiguration has remained a significant predictor, confirming that tunnel governance weaknesses—such as inconsistent validation, routing scope expansion, and boundary control ambiguity—have materially increased exposure in a hybrid cloud setting where connectivity bridges trust zones. The study has also concluded that governance behavior has mattered: the Protection

Motivation Theory–based protection motivation construct has been negatively associated with exposure and has remained significant in regression analysis, indicating that stronger coping appraisal and lower perceived response costs have aligned with lower exposure outcomes. This theoretical integration has strengthened the interpretation of technical findings by showing that drift and misconfiguration have not been solely engineering issues but have also reflected motivational and organizational constraints under change pressure. The results have been reinforced by study-specific trust-building analyses that have localized exposure to hybrid boundary segments through a misconfiguration risk heatmap and have clarified drift mechanisms through a drift pattern fingerprint, thereby demonstrating that exposure has clustered where policy translation and operational urgency have been highest, especially at remote-access VPN zones and on-premises-to-cloud interconnect boundaries. The Risk Control Gap Index and sensitivity ranking have further supported the conclusion that limitations in automated validation, review cadence, ownership clarity, and continuous monitoring have enabled risk conditions to persist, and that drift control has been the most influential lever within the modeled predictors. Collectively, the study has provided a defensible, evidence-based account that hybrid cloud exposure has been shaped by the combined effect of technical policy state and governance motivation, and it has validated a conceptual framework in which misconfiguration and drift have been treated as measurable constructs that explain exposure at both global and segment levels. Through this integrated quantitative approach, the research has confirmed that understanding and measuring configuration weaknesses and drift dynamics have been essential for credible risk modeling in hybrid cloud networks, and it has established a structured foundation for interpreting hybrid-cloud security exposure through both technical mechanisms and PMT-informed behavioral governance factors.

RECOMMENDATIONS

The recommendations of this research have been organized to align directly with the quantified drivers of exposure identified in the model, with priority given to reducing firewall rule drift, strengthening VPN configuration governance, and lowering the governance control gaps that have enabled these conditions to persist under operational pressure. First, firewall rule drift has been treated as the highest-impact factor, so a formal rule-lifecycle program has been recommended that has included mandatory ownership tagging for every rule, explicit business justification fields, and an expiry mechanism for incident-driven exceptions so that temporary allowances have automatically entered a review-and-removal workflow rather than remaining indefinitely. A structured cadence of rule-base hygiene has been recommended, including monthly anomaly reviews focused on redundancy, shadowing, and overly broad CIDR/service allowances, supported by standardized rule-naming conventions and rule-grouping taxonomy to improve interpretability and auditing. Second, VPN configuration governance has been strengthened through a recommended baseline "secure tunnel profile" that has enforced cryptographic minimums, certificate lifecycle hygiene, strict route advertisement constraints, and explicit controls for split tunneling and DNS handling, with deviations requiring documented approvals tied to risk acceptance and a defined sunset date. Because exposure has clustered at hybrid trust-boundary segments, segmentation-specific controls have been recommended for remote-access VPN zones and on-premises-to-cloud interconnects, including stricter conditional access, stronger authentication enforcement, least-privilege routing scopes, and dedicated monitoring for anomalous reachability changes at gateway interfaces. Third, automation has been recommended as a primary mechanism to reduce response cost and improve coping appraisal consistent with PMT, so policy-as-code practices have been recommended for firewall and VPN configurations, enabling version-controlled change review, automated validation tests, and repeatable deployment pipelines that have reduced manual edits and uncontrolled drift. Automated drift detection has been recommended through continuous comparison of running configurations against approved baselines, with alerts for newly introduced broad rules, unusual rule growth, stale rules exceeding age thresholds, and mismatches between intended segmentation maps and effective reachability. In addition, targeted operational metrics have been recommended for governance visibility, including rule-change frequency, exception aging, unused-rule ratio, and tunnel-coverage completeness, so that configuration health has been tracked as a measurable operational performance dimension rather than a periodic audit artifact. To strengthen governance accountability, a cross-functional change-control board has

been recommended for boundary controls, ensuring that VPN and firewall changes affecting interconnects have been reviewed by both network and security stakeholders before deployment, and that post-incident cleanup tasks have been embedded as mandatory closure requirements. Finally, capacity-building measures have been recommended that have focused on improving self-efficacy and response efficacy—such as playbooks for secure VPN parameterization, training on drift anomaly types, and practical exercises on rule review and rollback—so that protective behaviors have been routinized and reinforced. Collectively, these recommendations have been designed to reduce the measured control gaps, improve the stability of boundary enforcement, and lower the probability that misconfigurations and drift have translated into persistent exposure across hybrid cloud segments.

LIMITATIONS

The limitations of this study have reflected both methodological and contextual constraints that have shaped how the findings have been interpreted and generalized. First, the research design has been cross-sectional, so the relationships among VPN misconfiguration, firewall rule drift, protection motivation, and risk exposure have been measured at a single point in time rather than tracked longitudinally; as a result, temporal directionality has not been directly observed, and the statistical evidence has supported association and prediction within the dataset rather than definitive causal sequencing across time. Second, the study has relied primarily on a Likert-scale survey instrument, meaning that key constructs have been operationalized through practitioner assessments rather than through fully objective configuration telemetry; while reliability testing has indicated strong internal consistency and the constructs have been grounded in established literature, self-reported measures have remained vulnerable to common-method variance, recall bias, and role-based perception differences, particularly in environments where different teams have had uneven visibility into VPN parameter settings, firewall policy details, or the downstream consequences of rule changes. Third, the case-study focus has strengthened contextual realism but has limited external generalizability, because the hybrid-cloud architecture, change processes, tooling maturity, staffing profile, and governance culture of the case organization have influenced the magnitude of drift, misconfiguration, and exposure levels; therefore, the regression coefficients and descriptive patterns have been most defensible as evidence within comparable operational settings rather than universal parameters for all hybrid-cloud networks. Fourth, the study has not incorporated direct inspection of sensitive configuration artifacts such as firewall running configurations, VPN gateway settings, certificate inventories, or routing-policy snapshots, because of confidentiality constraints; this has appropriately protected organizational security, yet it has restricted the ability to triangulate survey constructs with automated anomaly counts, drift velocity measures, and verified reachability tests, which would have strengthened measurement precision and reduced reliance on perception-based indicators. Fifth, interaction effects and nonlinear behaviors have not been fully explored in the baseline modeling, including the possibility that VPN misconfiguration and firewall drift have amplified each other beyond additive effects or that exposure has increased sharply after threshold levels of drift; the decision to prioritize interpretable regression models has supported clarity, but it has limited exploration of more complex functional forms that may exist in real operational networks. Sixth, control variables have been captured in a limited scope, and some potentially influential organizational factors—such as incident frequency, budget constraints, vendor tooling constraints, team turnover, and policy ownership fragmentation—have not been fully modeled, which may have left residual variance in risk exposure unexplained. Finally, the PMT construct has been measured at a general governance level rather than being tied to specific micro-behaviors (e.g., post-incident cleanup compliance, validation habit strength, or exception approval discipline), so the theoretical linkage has been statistically supported but has not distinguished which PMT subcomponents have driven the strongest protective effects in practice. Collectively, these limitations have suggested that the findings have been best interpreted as context-grounded quantitative evidence that has demonstrated coherent relationships among hybrid-cloud configuration weaknesses, governance motivation, and perceived exposure, while also indicating that stronger generalization and causal inference would have required longitudinal multi-case designs, mixed-method triangulation with configuration telemetry, and more granular behavioral measurement.

REFERENCES

[1]. Abedin, M., Nessa, S., Khan, L., & Thuraisingham, B. (2006). Detection and resolution of anomalies in firewall policy rules. In *Data and Applications Security XX* (Vol. 4127, pp. 15-29). Springer. https://doi.org/10.1007/11805588_2

[2]. Allodi, L., & Massacci, F. (2014). Comparing vulnerability severity and exploits using case-control studies. *ACM Transactions on Information and System Security*, *17*(1), Article 1, 1-20. https://doi.org/10.1145/2630069

[3]. Allodi, L., & Massacci, F. (2017). Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis*, *37*(8), 1606-1627. https://doi.org/10.1111/risa.12864

[4]. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58. https://doi.org/10.1145/1721654.1721672

[5]. Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007). *Provable data possession at untrusted stores* Proceedings of the 14th ACM Conference on Computer and Communications Security,

[6]. Aura, T., Becker, M., Roe, M., & Zieliński, P. (2010). Reconciling multiple IPsec and firewall policies. In *Security Protocols 2007* (Vol. 5964, pp. 81-97). Springer. https://doi.org/10.1007/978-3-642-17773-6_9

[7]. Basile, C., Cappadonia, A., & Lioy, A. (2012). Network-level access control policy analysis and transformation. *IEEE/ACM Transactions on Networking*, *20*(4), 985-998. https://doi.org/10.1109/tnet.2011.2178431

[8]. Basin, D., Burri, S., & Karjoth, G. (2016). Obligations in policy management. *Journal of Logical and Algebraic Methods in Programming*, *85*(4), 565-596. https://doi.org/10.1016/j.jlamp.2015.08.003

[9]. Bethencourt, J., Sahai, A., & Waters, B. (2007). *Ciphertext-policy attribute-based encryption* 2007 IEEE Symposium on Security and Privacy,

[10]. Chen, F., Liu, A. X., Hwang, J., & Xie, T. (2012). First step towards automatic correction of firewall policy faults. *ACM Transactions on Autonomous and Adaptive Systems*, *7*(2), Article 27. https://doi.org/10.1145/2240166.2240177

[11]. Cheng, Y., Deng, J., Li, J., DeLoach, S., Singhal, A., & Ou, X. (2014). Metrics of security. In *Cyber Defense and Situational Awareness* (Vol. 62). Springer. https://doi.org/10.1007/978-3-319-11391-3_13

[12]. Chockalingam, S. P., Hadžiosmanović, D., Pieters, W., Teixeira, A., & van Gelder, P. (2018). Bayesian network models in cyber security: A systematic review. In *Critical Infrastructure Protection XII* (pp. 105-126). https://doi.org/10.1007/978-3-319-70290-2_7

[13]. Cremers, C. J. F. (2011). Key exchange in IPsec revisited: Formal analysis of IKEv1 and IKEv2. In *Computer Security – ESORICS 2011* (Vol. 6879, pp. 315-334). Springer. https://doi.org/10.1007/978-3-642-23822-2_18

[14]. Dai, F., Hu, Y., Zheng, K., & Wu, B. (2015). Exploring risk flow attack graph for security risk assessment. *IET Information Security*, *9*(6), 332-341. https://doi.org/10.1049/iet-ifs.2014.0272

[15]. Diekmann, C., Hupel, L., & Carle, G. (2015). Semantics-preserving simplification of real-world firewall rule sets. In *FM 2015: Formal Methods* (Vol. 9109, pp. 195-212). Springer. https://doi.org/10.1007/978-3-319-19249-9_13

[16]. Fakis, A., Karopoulos, G., & Kambourakis, G. (2020). Neither denied nor exposed: Fixing WebRTC privacy leaks. *Future Internet*, *12*(5), 92. https://doi.org/10.3390/fi12050092

[17]. Faysal, K., & Shamsunnahar, C. (2022). Digital Ledger Optimization Techniques for Enhancing Transaction Speed and Reporting Accuracy in Accounting Systems. *American Journal of Scholarly Research and Innovation*, *1*(02), 171–222. https://doi.org/10.63125/33t06k57

[18]. Franke, U., & Brynielsson, J. (2014). Cyber situational awareness — A systematic review of the literature. *Computers & Security*, *46*, 18-31. https://doi.org/10.1016/j.cose.2014.06.008

[19]. García-Alfaro, J., Cuppens, F., Cuppens-Boulahia, N., Martínez, S., & Cabot, J. (2013). Management of stateful firewall misconfiguration. *Computers & Security*, *39*, 64-85. https://doi.org/10.1016/j.cose.2013.01.004

[20]. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). *Attribute-based encryption for fine-grained access control of encrypted data* Proceedings of the 13th ACM Conference on Computer and Communications Security,

[21]. Grobauer, B., Walloschek, T., & Stöcker, E. (2011). Understanding cloud computing vulnerabilities. *IEEE Security & Privacy*, *9*(2), 50-57. https://doi.org/10.1109/msp.2010.115

[22]. Habibullah, S. M., & Zaheda, K. (2022). Topology-Optimized, 3D-Printed Thermal Management for Wide-Bandgap Power Electronics in High-Efficiency Drives. *Journal of Sustainable Development and Policy*, *1*(02), 134-167. https://doi.org/10.63125/p8m2p864

[23]. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

[24]. Hu, H., Ahn, G.-J., & Kulkarni, K. (2012). Detecting and resolving firewall policy anomalies. *IEEE Transactions on Dependable and Secure Computing*, *9*(3), 318-331. https://doi.org/10.1109/tdsc.2012.20

[25]. Hudic, A., Weippl, E., & Strembeck, M. (2017). Security assurance assessment methodology for hybrid clouds. *Computers & Security*, *70*, 191-205. https://doi.org/10.1016/j.cose.2017.03.009

[26]. Hwang, J., Xie, T., Chen, F., & Liu, A. X. (2012). Systematic structural testing of firewall policies. *IEEE Transactions on Network and Service Management*, *9*(1), 82-94. https://doi.org/10.1109/tnsm.2012.12.100092

[27]. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

[28]. Ikram, M., Vallina-Rodriguez, N., Seneviratne, S., Kaafar, M. A., & Paxson, V. (2016). *An analysis of the privacy and security risks of Android VPN permission-enabled apps* Proceedings of the 2016 ACM Internet Measurement Conference,

[29]. Jahangir, S., & Md Shahab, U. (2022). A Qualitative Study of Safety Professionals' Experiences in Managing Chemical Exposure Risks and Hazardous Materials Controls in Industrial Facilities. *Review of Applied Science and Technology*, *1*(04), 250–282. https://doi.org/10.63125/jmh69r20

[30]. Jensen, M., Schwenk, J., Gruschka, N., & Lo Iacono, L. (2009). *On technical security issues in cloud computing* 2009 IEEE International Conference on Cloud Computing,

[31]. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566. https://doi.org/10.2307/25750691

[32]. Jouini, M., Ben Arfa Rabai, L., & Khédri, R. (2015). A multidimensional approach towards a quantitative assessment of security threats. *Procedia Computer Science*, *52*, 507-514. https://doi.org/10.1016/j.procs.2015.05.024

[33]. Khan, M. T., DeBlasio, J., Voelker, G. M., Snoeren, A. C., Kanich, C., & Vallina-Rodriguez, N. (2018). *An empirical analysis of the commercial VPN ecosystem* Proceedings of the Internet Measurement Conference 2018,

[34]. Khosravi-Farmad, M., & Ghaemi-Bafghi, A. (2020). Bayesian decision network-based security risk management framework. *Journal of Network and Systems Management*, *28*, 1794-1819. https://doi.org/10.1007/s10922-020-09558-5

[35]. Kreutz, D., Ramos, F. M. V., Veríssimo, P. E., Rothenberg, C. E., Azodolmolky, S., & Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, *103*(1), 14-76. https://doi.org/10.1109/jproc.2014.2371999

[36]. Kumari, R., & Sahoo, A. K. (2014). Cross-domain search for policy anomalies in firewall. *International Journal of Computer Applications*, *104*(6), 20-24. https://doi.org/10.5120/18205-9337

[37]. Liu, A. X., & Gouda, M. G. (2005). *Complete redundancy detection in firewalls* Proceedings of the IFIP/IEEE International Conference on Network and Service Management,

[38]. Manadhata, P. K., & Wing, J. M. (2011). An attack surface metric. *IEEE Transactions on Software Engineering*, *37*(3), 371-386. https://doi.org/10.1109/tse.2010.60

[39]. Neil, M., Fenton, N., & Osman, M. (2019). Using Bayesian networks to model risk in cybersecurity: A quantitative approach based on the FAIR model. *Computers & Security*, *86*, 101659. https://doi.org/10.1016/j.cose.2019.101659

[40]. Pendleton, M., Garcia-Lebron, R., Cho, J.-H., & Xu, S. (2016). A survey on systems security metrics. *ACM Computing Surveys*, *49*(4), 1-35. https://doi.org/10.1145/3005714

[41]. Perta, V. C., Barbera, M. V., Tyson, G., Haddadi, H., & Mei, A. (2015). A glance through the VPN looking glass: IPv6 leakage and DNS hijacking in commercial VPN clients. *Proceedings on Privacy Enhancing Technologies*, *2015*(1), 77-91. https://doi.org/10.1515/popets-2015-0006

[42]. Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic security risk management using Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, *9*(1), 61-74. https://doi.org/10.1109/tdsc.2011.34

[43]. Ratul, D. (2022). Engineering Resilient Flood Mitigation Using Geosynthetic and Composite Barrier Materials Performance Modeling and Environmental Impact Assessment. *Review of Applied Science and Technology*, *1*(03), 100–148. https://doi.org/10.63125/052q7d44

[44]. Ratul, D., & Subrato, S. (2022). Remote Sensing Based Integrity Assessment of Infrastructure Corridors Using Spectral Anomaly Detection and Material Degradation Signatures. *American Journal of Interdisciplinary Studies*, *3*(04), 332-364. https://doi.org/10.63125/1sdhwn89

[45]. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). *Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds* Proceedings of the 16th ACM Conference on Computer and Communications Security,

[46]. Rosado, D. G., Gómez, R., Mellado, D., & Fernández-Medina, E. (2012). Security analysis in the migration to cloud environments. *Future Internet*, *4*(2), 469-487. https://doi.org/10.3390/fi4020469

[47]. Shacham, H., & Waters, B. (2008). *Compact proofs of retrievability* Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security,

[48]. Sommestad, T., Ekstedt, M., & Johnson, P. (2010). A probabilistic relational model for security risk analysis. *Computers & Security*, *29*(6), 659-679. https://doi.org/10.1016/j.cose.2010.02.002

[49]. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

[50]. Tahmina Akter Bhuya, M., & Rebeka, S. (2022). AI-Assisted Underwriting Models for Improving Risk Assessment Accuracy in U.S. Insurance Markets. *American Journal of Interdisciplinary Studies*, *3*(01), 65-102. https://doi.org/10.63125/kegg1076

[51]. Takabi, H., Joshi, J. B. D., & Ahn, G.-J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), 24-31. https://doi.org/10.1109/msp.2010.186

[52]. Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

[53]. Vasilakos, A. V., & Imran, M. (2016). Security in software-defined networking: Threats and countermeasures. *Mobile Networks and Applications*, *21*(5), 764-776. https://doi.org/10.1007/s11036-016-0676-x

[54]. Wang, J. A., & Guo, M. (2010). *Vulnerability categorization using Bayesian networks* Proceedings of the 6th Annual Workshop on Cyber Security and Information Intelligence Research,

[55]. Wang, L., Islam, T., Long, T., Singhal, A., & Jajodia, S. (2008). An attack graph-based probabilistic security metric. In *Data and Applications Security XXII* (Vol. 5094, pp. 283-296). Springer. https://doi.org/10.1007/978-3-540-70567-3_22

[56]. Workman, M., Bommer, W. H., & Straub, D. W. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816. https://doi.org/10.1016/j.chb.2008.04.005

[57]. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583-592. https://doi.org/10.1016/j.future.2010.12.006