International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 04-11-2020; Accepted: 07-12-2020
www.allmultidisciplinaryjournal.com
Volume 1; Issue 5; November-December 2020; Page No. 457-467

Conceptual Model improving Endpoint Security across mixed Operating System Environments

Nwankwo Constance Obiuto [1*], Ugwu-Oju Ukamaka Mary [2], Okeke Obinna ThankGod [3]
[1] Faculty of Engineering, Nnamdi Azikiwe University, Awka, Nigeria
[2] Healthy Appetite Confectioneries, Abuja, Nigeria
[3] Ventlio, Lagos Nigeria

Corresponding Author: **Nwankwo Constance Obiuto**

DOI: https://doi.org/10.54660/.IJMRGE.2020.1.5.457-467

Abstract
Enterprises increasingly operate in mixed operating system (OS) environments encompassing Windows, macOS, Linux distributions, mobile platforms, and cloud-connected endpoints. This heterogeneity enhances flexibility and productivity but simultaneously introduces security fragmentation, inconsistent policy enforcement, and heightened vulnerability exposure. The proposed conceptual model addresses these challenges by establishing a unified and adaptive framework designed to improve endpoint security across diverse OS ecosystems. The model integrates technological, procedural, and organizational dimensions to ensure consistent protection, visibility, and control regardless of platform differences. Central to the conceptual model is a unified security telemetry layer, which aggregates and normalizes cross-OS logs, configurations, and behavioral signals to provide holistic visibility. This is supported by a centralized policy and configuration management framework that enables consistent baseline enforcement, automated patching, and compliance validation across all endpoint types. An AI-driven threat detection and response engine further enhances security by correlating signals from heterogeneous environments, detecting anomalies, and orchestrating rapid, automated containment and remediation. Complementing these components is a cross-platform identity and access control architecture, grounded in zero-trust principles and designed to ensure uniform authentication, authorization, and device posture validation across multiple OS ecosystems. The model also incorporates an OS-agnostic application and API integration layer, enabling secure interoperation between enterprise apps while reducing attack surface exposures. Together, these components provide a cohesive, scalable, and resilient foundation for defending against evolving threats in increasingly distributed digital environments. By addressing the complexities inherent in mixed OS operations, the conceptual model offers a pathway toward strengthened organizational security posture, improved operational efficiency, and enhanced regulatory compliance. The framework sets the stage for future advancements involving edge computing, generative AI–augmented threat intelligence, and deeper zero-trust integration within native OS architectures.

Keywords: Mixed Operating System Environments, Endpoint Security, Unified Telemetry, Zero-trust architecture, Cross-platform Policy Management, AI-driven threat detection, Interoperability

1. Introduction
The modern enterprise computing landscape is characterized by an unprecedented proliferation of mixed operating system (OS) environments. Organizations today routinely manage a diverse array of endpoints, including Windows-based workstations, macOS devices, Linux servers, Android and iOS mobile platforms, and an expanding range of cloud-connected or IoT endpoints (Morrison *et al*., 2019; Mueller *et al*., 2019). This heterogeneity is driven by strategic imperatives such as device flexibility, employee productivity, specialized workload requirements, and the adoption of modern development and operational practices (Vetter *et al*., 2018; Gunasekaran *et al*., 2019). While the use of multiple OS platforms enhances agility and supports diverse business functions, it simultaneously complicates enterprise security management. Each OS ecosystem possesses distinct architectures, security models, update mechanisms, and vulnerability profiles, creating a complex environment in which traditional, centralized, or homogenous security strategies are increasingly inadequate (Tao *et al*., 2018; Martin *et al*., 2018).
Parallel to the rise of mixed OS environments is the accelerating sophistication of cyber threats. Adversaries now leverage cross-platform malware, polymorphic payloads, supply-chain compromise techniques, and AI-assisted attack strategies that exploit

inconsistencies across OS-layer defenses (Huang *et al*., 2018). Threat actors target gaps in policy enforcement, differences in patch cycles, and visibility blind spots created by fragmented monitoring systems. Advanced persistent threats (APTs) and ransomware operators, in particular, exploit the weakest link within heterogeneous environments, often moving laterally across OS types to escalate privileges or exfiltrate sensitive data (Stellios *et al*., 2018; Alshamrani *et al*., 2019). As organizations expand remote and hybrid work models, the distributed nature of endpoints further amplifies these risks, making endpoint security one of the most critical pillars of enterprise cybersecurity.

In this context, the need for unified, adaptive, and OS-agnostic security frameworks has become increasingly evident. Traditional endpoint protection approaches, which rely on OS-specific tools and siloed monitoring architectures, cannot keep pace with evolving threat complexity or operational scale (Petrik *et al*., 2018; Watada *et al*., 2019). A next-generation approach must integrate telemetry, identity controls, threat detection, and remediation workflows across diverse platforms while preserving the unique capabilities and constraints of each OS. Such a framework requires interoperability, automation, zero-trust principles, and AI-driven analytics to maintain consistent security postures in environments marked by constant change (Kushala and Kurunthachalam, 2019; Board, 2019).

The conceptual model presented in this work aims to address these challenges by providing a holistic and integrated blueprint for improving endpoint security across mixed operating system environments. Its purpose is to enhance enterprise-wide visibility by aggregating and normalizing cross-platform security signals; to strengthen coordination through centralized policy management, identity governance, and automated orchestration; and to improve resilience through adaptive threat detection, real-time remediation, and cross-layer interoperability. By unifying technology, processes, and governance structures, the model seeks to create a cohesive security ecosystem that remains robust in the face of platform diversity and dynamic threat landscapes. Ultimately, this conceptual model provides organizations with a strategic pathway for evolving their endpoint security capabilities to meet the demands of modern, heterogeneous computing environments.

2. Methodology

The PRISMA methodology was applied to develop a comprehensive and evidence-informed conceptual model for improving endpoint security across mixed operating system environments. The process began with a systematic identification of relevant literature across leading academic databases, including IEEE Xplore, ACM Digital Library, Scopus, SpringerLink, and ScienceDirect. Search terms such as "mixed operating system security," "cross-platform endpoint protection," "OS-agnostic security frameworks," "zero-trust endpoint architecture," "AI-driven threat detection," and "unified security telemetry" were used in various combinations to capture studies addressing heterogeneous OS environments and contemporary security architectures. No date restriction was applied initially to ensure adequate historical grounding, but studies published within the last ten years were prioritized to maintain relevance to evolving technologies and threat landscapes.

The screening process followed PRISMA's multi-stage structure. Title and abstract screening removed studies that did not focus on endpoint security, OS integration, or enterprise contexts. Full-text screening further excluded papers lacking empirical evidence, practical frameworks, or conceptual relevance to cross-OS environments. Duplicate entries were identified and removed using reference management tools. Studies were included if they met criteria such as addressing security challenges in heterogeneous OS ecosystems, proposing or evaluating endpoint security strategies, discussing telemetry integration, or analyzing AI-enabled threat detection and response. Papers focused solely on consumer devices, unrelated network security topics, or narrow OS-specific vulnerabilities were excluded to maintain conceptual consistency.

Data extraction was conducted using a structured template capturing study objectives, methodologies, security mechanisms, architectural components, and findings related to cross-platform coordination. Extracted data were synthesized using an integrative approach, allowing the combination of empirical evidence, architecture models, and theoretical insights. Themes emerging from the synthesis included cross-OS telemetry unification, centralized policy management, behavior-based detection, identity governance, zero-trust enforcement, automation and orchestration, and interoperability challenges. These themes provided the foundation for constructing the conceptual model.

The final conceptual model was developed through iterative refinement, integrating insights from diverse studies to ensure completeness, practical relevance, and alignment with emerging enterprise security needs. The PRISMA-driven process ensured transparency, rigor, and reliability in deriving a model that supports enhanced visibility, coordination, and resilience across mixed operating system environments.

2.1. Background and Problem Context

The rapid diversification of enterprise computing environments has introduced significant complexity into endpoint security management. Organizations increasingly operate heterogeneous ecosystems composed of Windows, macOS, Linux distributions, mobile operating systems such as Android and iOS, and an expanding portfolio of cloud-connected and IoT devices (Qin *et al*., 2018; Mei and Guo, 2018). While this diversity provides operational flexibility, it also creates structural challenges that undermine the consistency and effectiveness of security controls. Understanding the background and problem context behind these challenges is essential for constructing a conceptual model capable of improving endpoint security across mixed operating system environments.

One of the most prominent issues is the fragmentation of security tools, policies, and enforcement mechanisms across different OS ecosystems. Each OS family has distinct characteristics, including system architecture, kernel design, security primitives, and application execution models. Consequently, enterprises often deploy multiple endpoint protection tools, each tailored to a specific platform. This results in siloed dashboards, inconsistent policy implementation, and difficulty establishing unified visibility. For instance, while Windows environments may rely heavily on Active Directory–integrated security controls, macOS and Linux endpoints require separate frameworks, and mobile devices depend on MDM or EMM tools. The lack of cross-platform uniformity contributes to monitoring blind spots and reduces an organization's ability to correlate threats across

systems, allowing adversaries to exploit inconsistencies as entry points for lateral movement (Rydén and El Sawy, 2019; McGuigan, 2019).

Closely related to this fragmentation are challenges arising from inconsistent patching practices, configuration drift, and divergent security baselines. Operating systems differ in their patch release cycles, vulnerability disclosure processes, and update deployment mechanisms. These disparities create opportunities for attacks when one OS receives security updates more rapidly than another or when devices fall out of compliance due to delayed patches. Configuration drift where endpoint settings deviate from approved security configurations over time further exacerbates risk, particularly in environments lacking automated compliance enforcement. Additionally, maintaining consistent baseline configurations across OS types is difficult, as certain security controls available in one platform may not have functional equivalents in another (DeKoven *et al*., 2019; Zandberg *et al*., 2019). This inconsistency weakens enterprise efforts to maintain standardized hardening practices and undermines defense-in-depth strategies.

The problem is intensified by the complexity of integrating legacy systems, proprietary OS ecosystems, and modern cloud-connected devices. Many enterprises still operate legacy Windows servers, specialized Linux-based industrial control systems, or proprietary operating systems embedded in critical infrastructure components. These systems often lack modern security features, receive infrequent updates, or require specialized tools for monitoring. At the same time, cloud-connected devices ranging from SaaS-managed workstations to IoT sensors introduce new interfaces, APIs, and remote management constraints. Integrating these disparate systems within a unified security architecture requires extensive interoperability, customized connectors, and multiple layers of abstraction. Moreover, proprietary OS ecosystems and vendor-restricted environments limit visibility and restrict security tool deployment, complicating endpoint monitoring and response. The resulting heterogeneity creates architectural patchworks that demand significant administrative effort and heighten the likelihood of misconfigurations or oversight (Franklin *et al*., 2018; Fürstenau *et al*., 2019).

Given these issues, the importance of holistic endpoint security as a core component of enterprise risk management and compliance has never been greater. Regulatory frameworks such as GDPR, HIPAA, PCI-DSS, ISO 27001, and emerging zero-trust guidelines require consistent enforcement of access controls, data protection measures, and auditability across all systems handling sensitive information. Fragmented OS environments complicate compliance by introducing variability in logging formats, control capabilities, and policy enforcement mechanisms. Without unified visibility and standardized controls, enterprises struggle to accurately assess exposure, detect anomalous behavior, or provide reliable evidence during audits. Furthermore, the rise of hybrid work and distributed devices increases attack surfaces, making endpoint security a frontline defense in protecting organizational assets and ensuring business continuity.

The consequences of inadequate cross-OS security coordination are significant. Attackers increasingly exploit vulnerabilities in less-monitored or inconsistently protected OS platforms to bypass defenses. Ransomware campaigns often target Linux servers after compromising Windows endpoints, while mobile devices become vectors for credential theft that enables access to cloud systems (Al-Hawawreh *et al*., 2019; Hassan, 2019). The lack of integrated threat detection across OS environments limits an organization's ability to correlate indicators of compromise (IOCs) and identify multi-stage attack chains. As threat actors adopt more sophisticated techniques and AI-assisted tools, gaps created by OS diversity pose escalating risks.

Therefore, the problem context underscores a pressing need for a modern, unified, and adaptive approach to endpoint security one capable of addressing fragmentation, enforcing consistent baselines, integrating diverse systems, and supporting enterprise-wide risk management. Such a conceptual model must leverage interoperability, automation, centralized policy management, and advanced analytics to establish a cohesive security posture across all operating system environments. This establishes the foundation for improved resilience, faster response to threats, and more effective compliance with evolving regulatory standards.

2.2. Foundations of Endpoint Security in Mixed OS Environments

Ensuring robust endpoint security in mixed operating system (OS) environments requires a multilayered foundation that integrates technical, organizational, and operational elements. As enterprises increasingly manage heterogeneous ecosystems comprising Windows, macOS, Linux, Android, iOS, and cloud-connected devices the security landscape becomes more complex. Each platform introduces unique vulnerabilities, operational constraints, and management workflows, necessitating a coherent foundation that supports consistent protection across diverse endpoints. Understanding these foundational components is essential for designing a conceptual model capable of strengthening security posture and resilience in contemporary enterprise environments.

The technical foundations begin with acknowledging the distinct OS-specific vulnerabilities and attack surfaces inherent in each platform. Windows environments, for example, are frequent targets due to their widespread enterprise use and integration with Active Directory (Weissman *et al*., 2019; Parker and Gregg, 2019). They expose attack surfaces via registry structures, legacy protocols, and extensive backward compatibility requirements. macOS systems, while benefiting from UNIX-based protections and a curated application ecosystem, remain vulnerable to privilege escalation flaws, supply-chain attacks, and Apple-specific misconfigurations. Linux distributions introduce their own challenges through diverse package managers, varying kernel versions, and privilege management systems that differ across implementations. Mobile operating systems further add heterogeneity: Android devices have fragmented patch cycles and diverse vendor overlays, whereas iOS devices employ strict sandboxing yet face risks related to zero-day exploits and mobile configuration weaknesses. These heterogeneous attack surfaces make unified policy enforcement difficult and create opportunities for adversaries to exploit the weakest platform within the environment.

In response to these varied threats, enterprises rely on multilayered endpoint protection technologies such as Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), sandboxing solutions, and hardware or software–based device control. EDR tools

provide behavioral monitoring, real-time threat detection, and automated remediation actions, but their effectiveness depends on consistent deployment and configuration across OS types (Stevens *et al*., 2018; Sjarif *et al*., 2019). XDR extends this by integrating telemetry from networks, cloud workloads, identity systems, and endpoints helping correlate threats that span multiple platforms. Sandboxing technologies isolate suspicious executables or documents, mitigating risks associated with cross-platform malware. Device control frameworks restrict peripheral devices such as USB storage, which are common vectors for lateral movement across mixed environments. Together, these technologies establish a technical foundation capable of monitoring diverse endpoints, identifying anomalies, and mitigating threats, but only when supported by coherent policies and management processes.

Building on this technical layer, organizational foundations play a critical role in structuring how endpoint security policies are defined, governed, and assessed. Effective security policies must outline baseline configurations, acceptable use rules, patching requirements, and authentication standards applicable across all OS platforms. Governance mechanisms ensure these policies remain aligned with regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS) and evolving threat landscapes. A strong governance structure also clarifies roles and responsibilities, ensuring accountability across IT, security, and compliance teams.

Complementing policy and governance activities are risk assessment models that evaluate the likelihood and impact of threats across heterogeneous devices. Mixed OS environments complicate risk assessment due to varying levels of built-in security, different exposure to external networks, and inconsistent telemetry availability. Mature risk frameworks incorporate OS-specific threat intelligence, asset criticality, and vulnerability severity to create accurate and actionable risk profiles. These organizational foundations establish the structural discipline required to align enterprise security goals with the technical capabilities deployed across diverse environments (Törngren and Grogan, 2018; Malatji *et al*., 2019).

Finally, operational foundations ensure that security controls and policies are effectively executed in day-to-day enterprise contexts. Central to this domain are IT service management (ITSM) workflows, which orchestrate activities such as incident logging, change management, configuration updates, and problem resolution. Consistent ITSM practices help reduce configuration drift, maintain security baselines, and ensure timely remediation of vulnerabilities across all OS types. Automated workflows, integrated ticketing systems, and standardized request processes improve coordination and reduce human error key advantages in environments with diverse platform requirements.

Incident response practices form another critical pillar of the operational foundation. Mixed OS environments require incident response teams to handle diverse log formats, telemetry types, containment procedures, and forensic tools. For example, containing a ransomware infection on Windows may involve registry isolation and process termination, whereas on Linux it may require isolating containers or halting services. Effective incident response requires cross-platform playbooks, rapid decision-making, and automated actions to reduce mean time to containment (MTTC).

Equally important is cross-team collaboration among IT operations, security analysts, system administrators, cloud teams, and application developers (Padur, 2018; Elumalai and Roberts, 2019). Collaboration ensures that insights from one platform inform defensive measures across others, reducing blind spots. For example, indicators of compromise (IOCs) discovered in a Linux server environment may reveal early stages of an attack later detected on macOS endpoints. Seamless communication and shared situational awareness enhance threat detection accuracy and improve enterprise resilience.

Together, these technical, organizational, and operational foundations create a comprehensive and unified basis for endpoint security in mixed OS environments. They enable enterprises to manage diverse platforms cohesively, reduce vulnerabilities, and respond effectively to the evolving cyber threat landscape.

2.3. Core Components of the Conceptual Model

The proposed conceptual model for improving endpoint security across mixed operating system (OS) environments is built on five interdependent components designed to unify visibility, strengthen control, and enhance adaptive defense capabilities. These components address the heterogeneity of Windows, macOS, Linux, and mobile platforms by creating an OS-agnostic architecture that supports centralized governance, automated protection, and intelligent threat detection. Together, they provide a coherent foundation for mitigating increasingly complex cyber risks while supporting enterprise scalability and compliance.

The Unified Security Telemetry Layer serves as the primary mechanism for consolidating security-relevant data across diverse OS ecosystems. In traditional infrastructures, endpoint logs and telemetry vary in format, granularity, and accessibility, contributing to blind spots and delayed incident detection. This layer standardizes cross-OS log collection through agents or agentless connectors that extract system events, authentication logs, application activity, and network behavior from each endpoint type. Once collected, the data undergoes normalization and correlation using a common schema, enabling analysts and automated tools to interpret patterns consistently. Integration with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms amplifies this benefit by enabling unified dashboards, automated alert triage, and coordinated response workflows (Goundar and Bhardwaj, 2019; Nina and Ethan, 2019). By centralizing telemetry in a cohesive structure, the model enhances visibility, reduces analytic complexity, and accelerates threat detection across heterogeneous environments.

A second foundational element is the Centralized Policy and Configuration Management component, which aims to eliminate inconsistencies caused by divergent OS-specific security baselines. Fragmented policies often result in configuration drift and unmanaged vulnerabilities, particularly in large or distributed enterprises. A centralized approach defines common baseline controls such as encryption requirements, firewall rules, application permissions, and logging settings that are then adapted for OS-specific implementations. Automated compliance checks continuously validate adherence to defined baselines, flag deviations, and initiate remediation workflows. Patch orchestration is also integrated into this component, ensuring synchronized update cycles across operating systems while accounting for OS-specific patch availability and testing

requirements. This coordinated configuration and compliance management significantly reduces risk exposure and supports regulatory obligations by ensuring uniform security posture across the endpoint fleet.

At the analytical core of the model is the Adaptive Threat Detection and Response Engine, which leverages artificial intelligence to interpret behavior across diverse OS environments. Traditional signature-based detection is insufficient for detecting modern, polymorphic, and fileless attacks, especially when attacker tactics vary based on OS characteristics. AI-driven behavior analytics identify deviations from normal endpoint activity, enabling early detection of unknown threats. The engine performs anomaly detection across telemetry sources and correlates indicators of compromise to create high-confidence alerts. Integrating real-time threat intelligence further strengthens detection capabilities, ensuring rapid identification of emerging threat vectors. Automated response mechanisms including endpoint isolation, malicious process termination, credential revocation, and script-based remediation enable swift containment across platforms, minimizing dwell time and operational disruption (Indu *et al*., 2018; Pattaranantakul e al., 2018).

The model also includes a Cross-Platform Identity and Access Control Framework, recognizing that identity has become a primary attack surface across all operating systems. This component enforces unified authentication requirements, such as multi-factor authentication and continuous device posture assessment, using identity providers that support all major OS types. Least-privilege access policies ensure that users and applications only obtain permissions essential for their functions, reducing attack pathways arising from privilege misuse or lateral movement. Importantly, the framework operates independently of the underlying OS, enabling consistent enforcement of zero-trust principles across Windows, macOS, Linux, and mobile devices. This cross-platform identity layer strengthens access governance and mitigates risks associated with credential theft, insider threats, and unauthorized resource access.

Finally, the Secure Application and API Integration Layer supports resilient and OS-agnostic application security. Security risks emerge not only from OS vulnerabilities but also from inconsistent application behavior, third-party integrations, and interdependent API ecosystems. This layer enforces application controls that limit software execution, validate permissions, and sandbox untrusted applications across platforms. It also incorporates container security policies for workloads operating in hybrid and cloud-integrated environments. Secure API gateways enforce standardized authentication, encryption, and communication protocols, reducing exposure associated with inter-application data exchange. By supporting secure development and deployment practices across operating systems, this integration layer enhances overall ecosystem security and reduces application-level attack surfaces.

Collectively, these five components create a comprehensive, adaptive, and OS-agnostic conceptual model capable of addressing the challenges of securing modern mixed-OS enterprise environments (Marti *et al*., 2018; Kocoloski *et al*., 2019). They provide unified visibility, enforce consistent policies, enable intelligent threat detection, strengthen identity protection, and ensure secure application integration ultimately supporting stronger resilience, reduced complexity, and improved operational efficiency.

2.4. Supporting Enablers

The effectiveness of a conceptual model designed to improve endpoint security across mixed operating system (OS) environments depends not only on its core architectural components but also on several essential enablers that reinforce operational efficiency, governance alignment, and human-centered resilience. These enablers automation and orchestration, interoperable architecture, governance and compliance alignment, and user awareness and training ensure that the model functions cohesively within real-world enterprise ecosystems. They address the practical demands of maintaining security across Windows, macOS, Linux, and mobile operating systems, where complexity, diversity, and rapid technological change require integrated and adaptive support mechanisms.

Automation and Orchestration represent a foundational enabler for maintaining consistent security posture across heterogeneous environments. In mixed OS ecosystems, manual interventions are insufficient for keeping pace with the volume of updates, threat alerts, and configuration checks needed to mitigate evolving risks. Automated patch management ensures that security updates are deployed consistently across all platforms, reducing exposure windows associated with unpatched vulnerabilities. Automation also extends to system hardening, allowing predefined security baselines to be applied continuously to endpoints, ensuring configurations do not drift over time (Mistry *et al*., 2018; Tedeschi *et al*., 2019). Orchestration further enhances these capabilities by coordinating response workflows across tools and teams. For example, when a threat is detected, automated workflows can isolate affected endpoints, gather forensic data, trigger remediation scripts, and notify relevant analysts. This integration of automation and orchestration reduces human error, accelerates response times, and supports scalable security operations even in large, distributed, and platform-diverse organizations.

The second enabler, Interoperable Architecture, ensures that the conceptual model remains adaptable and cohesive across varied OS ecosystems. Fragmentation is a recurring challenge in endpoint security, often caused by vendor-specific tools, incompatible log formats, and limited cross-platform visibility. An interoperable architecture built on open standards, cross-platform security agents, and API-driven extensibility enables seamless integration between security components. Open standards provide a common language for telemetry exchange, policy enforcement, and data correlation, regardless of the endpoint's underlying operating system. Cross-platform agents ensure consistent collection of logs, telemetry, and device posture information, while API-driven extensibility allows the model to integrate with emerging technologies, cloud-services, and external threat intelligence platforms. This flexibility is particularly important as enterprises increasingly adopt hybrid and multi-cloud environments, IoT devices, and containerized workloads that introduce additional layers of heterogeneity. An interoperable architecture thus provides the structural backbone that unifies the model's components and ensures its long-term scalability and adaptability.

Governance and Compliance Alignment is another crucial enabler that ensures the conceptual model supports enterprise duties related to legal, regulatory, and industry-specific requirements. Modern organizations must comply with diverse frameworks such as ISO 27001, NIST SP 800-53, GDPR, PCI DSS, and regional data-protection laws.

Effective endpoint security must therefore map its controls and processes directly to these regulatory requirements. The conceptual model facilitates this alignment by embedding compliance-aware mechanisms such as centralized policy management, automated auditing, standardized reporting, and continuous monitoring. Automated compliance checks verify whether endpoints adhere to security baselines, encryption standards, and access control policies across OS types. Additionally, unified telemetry and orchestration support forensic investigations and incident reporting obligations. These capabilities reduce compliance risk, enhance audit readiness, and support transparent governance processes that are increasingly required in modern digital enterprises (Clark and Kollwitz, 2018; Tiberius and Hirth, 2019).

The fourth enabler, User Awareness and Training, addresses the human dimension of endpoint security, which remains a critical determinant of security performance. In mixed OS environments, users interact with devices differently based on platform conventions, applications, and workflows. Tailored security education programs help users understand system-specific risks, safe usage practices, and warning signs of compromise relevant to their OS environment. This includes training on secure authentication, phishing avoidance, mobile device protection, application permissions, and incident reporting protocols. Because user behavior often directly influences endpoint security such as installing unauthorized applications or neglecting updates targeted education supports proactive risk reduction. Moreover, training improves collaboration between users and IT security teams, facilitating accurate reporting of anomalies and fostering a security-aware culture that complements the technological components of the model.

Collectively, these supporting enablers strengthen the conceptual model's ability to function effectively within complex enterprise ecosystems. Automation and orchestration enhance operational efficiency and reduce response times. Interoperable architecture ensures cohesive integration across diverse OS platforms. Governance and compliance alignment embed regulatory adherence into daily operations. User awareness and training reinforce human-centered security and reduce behavioral risk. Together, they enable a unified, adaptive, and resilient endpoint security strategy capable of responding to evolving threats while supporting enterprise-scale operational and regulatory demands.

2.5. Expected Outcomes

The implementation of a unified conceptual model for improving endpoint security across mixed operating system (OS) environments is expected to yield substantial advancements in enterprise cybersecurity maturity, operational efficiency, and risk mitigation (Serpanos and Wolf, 2018; Son *et al*., 2019). As organizations increasingly rely on diverse endpoint ecosystems ranging from Windows and macOS to Linux distributions and mobile platforms the ability to enforce consistent security controls, detect threats rapidly, and maintain compliance becomes a strategic priority. The outcomes outlined below reflect the measurable improvements that emerge when enterprises adopt a coordinated, intelligence-driven, and OS-agnostic security architecture.

One of the primary expected outcomes is reduced vulnerability exposure and improved incident detection speed. Mixed OS environments often suffer from inconsistent patching cycles, varying security baselines, and tool fragmentation, all of which widen the attack surface. By integrating a unified security telemetry layer, centralized policy controls, and automation-driven remediation, the conceptual model shortens the time between vulnerability disclosure, patch deployment, and endpoint hardening. Automated patch orchestration ensures that all platforms receive updates according to predefined schedules and priority levels, reducing the likelihood of exploitation through unpatched systems. Additionally, AI-enhanced threat detection provides behavioral analytics and anomaly scoring across OS types, enabling rapid identification of suspicious activities that traditional signature-based tools may overlook. The combination of centralized visibility and automated detection ultimately accelerates the time to detect (TTD) and time to respond (TTR), minimizing potential damage and improving overall security responsiveness.

A second expected outcome is enhanced cross-OS visibility and diagnostic accuracy. Historically, enterprises have struggled with siloed endpoint logs, incompatible data formats, and limited insight into OS-specific events. The conceptual model's unified telemetry and monitoring architecture aggregates, normalizes, and correlates data from all endpoints including laptops, servers, mobile devices, and cloud-connected systems into a cohesive view. This multidimensional visibility enables analysts to pinpoint attack vectors, correlate events across platforms, and identify lateral movement patterns with improved precision. Diagnostic accuracy increases as security teams gain access to standardized dashboards, enriched threat intelligence, and cross-platform behavior models that illuminate systemic weaknesses and emerging threat trends. Enhanced visibility also supports proactive risk assessment, enabling enterprises to prioritize vulnerabilities, configurations, and user behaviors that pose the highest exposure across the entire operating environment (Colicchia *et al*., 2019; Kure and Islam, 2019).

Another significant expected outcome is streamlined policy enforcement and increased operational consistency. Mixed OS environments traditionally require separate tools and procedures for enforcing security policies, resulting in configuration drift, inconsistent compliance levels, and manual overhead. The conceptual model's centralized policy and configuration management framework facilitates uniform enforcement of security baselines such as encryption requirements, firewall rules, application control policies, and identity verification protocols across all OS platforms. Automated compliance validation further reduces manual effort, ensuring that deviations are detected and remediated quickly. As a result, organizations achieve higher levels of operational uniformity, minimize configuration discrepancies, and reduce the risk of human error. Beyond improving security posture, streamlined policy enforcement significantly enhances operational efficiency, reduces administrative overhead, and ensures that security operations align more closely with enterprise governance standards.

The model also contributes directly to a stronger organizational cybersecurity posture and improved regulatory compliance. As global regulatory frameworks impose stricter requirements on data protection, privacy, access control, and incident reporting, enterprises operating in heterogeneous OS environments face heightened compliance challenges. By integrating the conceptual

model's components especially identity and access control frameworks, automated compliance checks, and enhanced auditability organizations can meet regulatory obligations more consistently and with greater confidence. The model supports traceable, transparent, and verifiable security processes that align with standards such as ISO 27001, NIST CSF, GDPR, HIPAA, and industry-specific requirements. Improved compliance reduces legal and financial risks while strengthening stakeholder confidence and organizational reputation. Additionally, the adoption of OS-agnostic identity enforcement, zero-trust principles, and real-time threat intelligence elevates the organization's readiness against advanced persistent threats, ransomware, insider risks, and supply-chain attacks.

Collectively, these expected outcomes converge to create a more resilient, efficient, and adaptive security environment. Reduced vulnerability windows and rapid detection enhance the defensive capability of enterprise systems. Unified visibility and diagnostic accuracy support more informed decision-making and proactive security planning. Streamlined policy enforcement ensures operational predictability and governance alignment. Finally, improved compliance and strengthened cybersecurity posture increase organizational resilience in an era of expanding digital ecosystems and intensifying cyber threats. Through these outcomes, the conceptual model provides a strategic foundation for enterprises seeking to secure mixed OS environments while enabling scalability, agility, and sustained protection (Rapuzzi and Repetto, 2018; Cherukuri, 2019).

2.6. Challenges and Considerations

Implementing a conceptual model designed to improve endpoint security across mixed operating system (OS) environments presents significant opportunities for strengthening enterprise protection, yet it also introduces a series of challenges and considerations that must be addressed to ensure effectiveness and long-term sustainability. Mixed OS ecosystems comprising Windows, macOS, Linux variants, mobile platforms, Internet-of-Things (IoT) devices, and cloud-connected endpoints are inherently complex. As organizations attempt to apply unified, cross-platform security frameworks, they must confront structural, technical, and ethical constraints that influence the feasibility and performance of proposed solutions.

A primary challenge arises from integration complexities with legacy and proprietary OS systems. Many enterprises operate long-standing infrastructure components such as outdated Windows versions, unsupported Linux distributions, or proprietary industrial control system (ICS) operating environments with limited API availability. These systems often lack modern security capabilities, making them incompatible with contemporary telemetry standards, patch orchestration mechanisms, or AI-driven monitoring tools. Proprietary OS ecosystems such as those embedded in specialized hardware or niche enterprise applications may restrict third-party agent installation or expose minimal diagnostic data, limiting the depth of visibility and control. Integrating these diverse systems into a unified security architecture therefore requires custom connectors, middleware layers, or hybrid monitoring strategies, all of which add complexity and increase maintenance overhead (Buyya and Srirama, 2019; Alam *et al*., 2019). Moreover, legacy endpoints frequently serve critical operational roles, meaning that intrusive security updates or agent deployments risk disrupting essential services.

Another challenge concerns the potential performance overhead introduced by monitoring agents used to collect telemetry, enforce policies, and support AI-enabled threat detection. Continuous monitoring, behavioral analysis, and real-time data synchronization can impose significant CPU, memory, and network demands on endpoints particularly older devices, resource-constrained IoT systems, or mobile platforms with limited battery life. Excessive agent activity may degrade user experience, slow critical processes, or cause system instability, leading to resentment from end-users and reluctance to adopt the new security model. Balancing monitoring depth with acceptable system performance requires careful calibration, adaptive sampling techniques, and selective data collection strategies. Furthermore, the more diverse the OS environment, the more difficult it becomes to create lightweight, efficient, and universally compatible agents without sacrificing analytical precision (Wydmuch *et al*., 2018).

A third major consideration involves privacy concerns associated with unified telemetry collection. Aggregating logs, behavioral indicators, configuration data, and identity attributes from multiple OS platforms raises questions about data minimization, consent, and lawful processing. Endpoints used in hybrid work models blur the boundaries between personal and corporate devices, amplifying the risk of collecting sensitive personal information inadvertently. Privacy regulations such as the GDPR, CCPA, and regional data protection laws impose strict requirements regarding what data can be collected, how it must be stored, and who can access it. Unified telemetry platforms must therefore incorporate robust anonymization, pseudonymization, role-based access control, and data retention policies. Transparent communication with employees is essential to maintain trust and prevent perceptions of invasive surveillance. Failure to appropriately safeguard telemetry data not only erodes user confidence but also creates potential legal liabilities and compliance violations (McKenna *et al*., 2019; Alemany *et al*., 2019).

Equally important is the need for continuous updates to adapt to evolving OS ecosystems. Operating systems evolve rapidly, with frequent changes in kernel architecture, security models, application frameworks, and system APIs. Cloud-connected devices and mobile OSs introduce additional complexity through automatic updates that may break integration points or alter monitoring behaviors. Security agents, policy engines, and detection models must therefore be continuously updated to maintain compatibility and coverage. AI-driven analytics require periodic retraining to recognize new threat patterns without increasing false positives. Moreover, as new OS versions, device types, and virtualization layers emerge such as ARM-based enterprise laptops, containerized workspaces, and edge devices security frameworks must be adaptive enough to incorporate them without major redesigns (Geier and Chakraborty, 2019; Zhao and Mannan, 2019). This perpetual update cycle demands sustained investment in development, testing, and version alignment across all components of the security architecture. Additional considerations include organizational readiness, availability of skilled personnel, and the risk of increased system complexity. Enterprises may face resistance from IT teams accustomed to traditional OS-specific security tools or from employees who perceive increased security controls as

intrusive or restrictive. Successfully implementing the model requires coordinated change management, training programs tailored to OS diversity, and consistent cross-team collaboration. Furthermore, centralizing security functions can create single points of failure if redundancy and resilience mechanisms are not carefully engineered.

While unified endpoint security models offer substantial benefits for protecting heterogeneous OS environments, their implementation must carefully address integration challenges, performance trade-offs, privacy concerns, and the ongoing need for adaptability. A balanced approach that incorporates technical optimization, policy safeguards, and continuous refinement is essential for sustaining long-term effectiveness in rapidly evolving enterprise ecosystems (Mohammed, 2018; Aisyah *et al*., 2019).

2.7. Future Directions

The future of endpoint security in mixed operating system (OS) environments will be shaped by accelerating technological shifts, increasingly complex enterprise architectures, and the expanding sophistication of cyber threats. As organizations adopt distributed computing models, integrate artificial intelligence into security operations, and embrace adaptive zero-trust approaches, the conceptual model proposed in this study must evolve to maintain relevance, accuracy, and effectiveness. The following future directions outline key trajectories that will influence the ongoing refinement and practical application of endpoint security frameworks in heterogeneous OS landscapes.

A critical future direction involves examining the role of edge computing and distributed endpoints in expanding the threat landscape. Modern enterprises increasingly deploy edge devices ranging from IoT sensors and industrial controllers to mobile workstations and remote micro-data centers to support real-time analytics, automation, and operational resilience. These devices operate outside traditional perimeter controls, often in resource-constrained environments with limited physical security, inconsistent patching, and variable connectivity. In mixed OS ecosystems, edge devices may run lightweight Linux variants, proprietary embedded systems, or customized firmware, further complicating uniform security enforcement (Ali *et al*., 2019; Airehrour *et al*., 2019). The proliferation of such endpoints enlarges the attack surface and amplifies opportunities for adversaries to exploit unmonitored devices. Future iterations of the conceptual model must therefore incorporate edge-aware telemetry aggregation, decentralized identity validation, and autonomous, self-healing security agents capable of operating independently of central infrastructure. Additionally, research is needed to determine how distributed security orchestration can maintain real-time consistency across thousands of geographically dispersed endpoints, each operating diverse OS types and versions.

Another major direction is the integration of generative AI for predictive threat modelling, transforming reactive defense mechanisms into proactive, anticipatory security operations. Existing security models often rely on behavioral analytics, heuristic engines, and anomaly detection; however, generative AI offers the ability to simulate attack paths, forecast emerging vulnerabilities, and generate synthetic threat scenarios tailored to specific OS configurations. By learning from cross-OS telemetry, adversarial behavior patterns, and vulnerability databases, generative AI systems can craft high-fidelity predictions that guide patch prioritization, configuration hardening, and adaptive policy adjustments. Further research is required to explore the reliability, explainability, and security implications of generative AI models, particularly given their susceptibility to data poisoning, adversarial manipulation, and hallucination. Ensuring responsible deployment will demand rigorous validation methods, transparent model governance frameworks, and continuous alignment with evolving regulatory expectations related to AI safety and accountability.

The evolution of zero-trust architectures natively embedded into OS platforms represents another transformative direction influencing endpoint security. Current implementations of zero-trust security often rely on external tools, service overlays, or cloud-based access brokers that enforce identity verification, device posture checks, and contextual authorization (Bellefleur and Wang, 2018; Tanya and Rahul, 2019). As OS vendors increasingly integrate built-in zero-trust capabilities such as hardware-rooted identity, continuous authentication mechanisms, secure enclaves, and policy-driven resource segmentation future security models must capitalize on these native features. This requires harmonizing conceptual frameworks with OS-level primitives, leveraging unified attestation standards, and orchestrating cross-OS trust scoring that reflects device health, behavioral consistency, and environmental risk. Embedding zero-trust capabilities directly into the OS fabric will enable more seamless, efficient, and tamper-resistant security operations. However, it also necessitates deeper collaboration between OS manufacturers, cybersecurity researchers, and enterprise architects to ensure interoperability, transparency, and scalability across multiple platforms.

Finally, cross-industry validation and refinement of the conceptual model is essential for ensuring robustness, adaptability, and empirical relevance. Industries such as healthcare, finance, manufacturing, energy, and government operate unique endpoint ecosystems with specialized OS requirements, varying regulatory constraints, and distinct threat profiles. Validating the conceptual model across these contexts will illuminate gaps, highlight edge cases, and reveal opportunities for optimization. Comparative case studies, real-world pilot implementations, and longitudinal assessments can provide insights into model scalability, operational burden, and return on security investment. Additionally, cross-industry collaboration can accelerate the standardization of telemetry schemas, API specifications, and interoperability frameworks necessary for consistent cross-OS security management. Academic-industry partnerships will play a crucial role in advancing research, fostering innovation, and ensuring that the conceptual model evolves in alignment with technological, organizational, and adversarial developments.

Future endpoint security strategies must adapt to the rising complexity of distributed OS environments, the potential of generative AI, the maturation of OS-native zero-trust architectures, and the need for broad, cross-industry validation. By anticipating these developments, the conceptual model can continue to serve as a foundation for resilient, adaptive, and intelligent security architectures capable of protecting heterogeneous enterprise ecosystems in an increasingly dynamic threat landscape (Ross *et al*., 2019; Linkov and Kott, 2019).

3. Conclusion

The increasing diversity of enterprise computing environments underscores the necessity for unified, adaptive security approaches capable of protecting heterogeneous operating system (OS) ecosystems. As organizations operate across Windows, macOS, Linux, mobile platforms, and distributed edge devices, the complexity of achieving consistent security governance, reliable threat detection, and coherent policy enforcement continues to rise. This environment demands security models that transcend OS-specific tools and fragmented practices, integrating cross-platform visibility, identity governance, and automated defense mechanisms into a cohesive, enterprise-wide framework. Reaffirming this need is central to understanding the strategic value of the conceptual model presented in this study.

The proposed conceptual model provides a foundational architecture for enhancing resilience, reducing risk exposure, and improving operational efficiency. By unifying telemetry collection, centralizing configuration and policy management, and applying adaptive threat intelligence across diverse OS environments, the model strengthens an organization's capacity to detect, respond to, and contain security threats with greater speed and accuracy. Its incorporation of AI-enabled analytics, zero-trust identity controls, and OS-agnostic application security promotes more consistent protection while minimizing configuration drift and reducing administrative overhead. Furthermore, the model supports enterprise compliance objectives by embedding standardized security practices within an interoperable, governance-aligned framework.

However, the security landscape is dynamic, shaped by rapid advancements in OS architectures, emerging edge computing paradigms, and increasingly sophisticated adversarial behaviors. For this reason, continuous evolution of the conceptual model is essential. Future improvements must incorporate new forms of telemetry, leverage generative AI for predictive security, integrate deeper OS-native zero-trust capabilities, and adapt to emerging endpoint categories. Ongoing research, cross-industry validation, and iterative refinement will ensure that the conceptual model remains robust, scalable, and relevant in protecting mixed OS ecosystems. Through this continual adaptation, enterprises can maintain strong cyber resilience in an ever-evolving digital environment.

4. References

1. Airehrour D, Gutierrez JA, Ray SK. SecTrust-RPL: a secure trust-aware RPL routing protocol for Internet of Things. Future Gener Comput Syst. 2019;93:860-76.
2. Aisyah N, Hidayat R, Zulaikha S, Rizki A, Yusof ZB, Pertiwi D, *et al*. Artificial intelligence in cryptographic protocols: securing e-commerce transactions and ensuring data integrity. 2019.
3. Alam I, Sharif K, Li F, Latif Z, Karim MM, Nour B, *et al*. IoT virtualization: a survey of software definition & function virtualization techniques for Internet of Things. arXiv. 2019:arXiv:1902.10910.
4. Alemany P, Kalalas C, Raul M, Vilalta R, Kafchitsas A, Sandia S, *et al*. INtelligent Security and PervasIve tRust for 5G and Beyond. 2019.
5. Al-Hawawreh M, den Hartog F, Sitnikova E. Targeted ransomware: a new cyber threat to edge system of brownfield industrial Internet of Things. IEEE Internet Things J. 2019;6(4):7137-51.
6. Ali I, Sabir S, Ullah Z. Internet of things security, device authentication and access control: a review. arXiv. 2019:arXiv:1901.07309.
7. Alshamrani A, Myneni S, Chowdhary A, Huang D. A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities. IEEE Commun Surv Tutorials. 2019;21(2):1851-77.
8. Bellefleur R, Wang D. IoT-enabled smart city security considerations and solutions. 2018.
9. Defense Innovation Board. AI principles: recommendations on the ethical use of artificial intelligence by the Department of Defense: supporting document. Washington, DC: United States Department of Defense; 2019.
10. Buyya R, Srirama SN, editors. Fog and edge computing: principles and paradigms. Hoboken, NJ: John Wiley & Sons; 2019.
11. Cherukuri BR. Future of cloud computing: innovations in multi-cloud and hybrid architectures. 2019.
12. Clark P, Kollwitz E. Regulatory compliance in workforce planning: a digital HR perspective. 2018.
13. Colicchia C, Creazza A, Menachof DA. Managing cyber and information risks in supply chains: insights from an exploratory analysis. Supply Chain Manag. 2019;24(2):215-40.
14. DeKoven LF, Randall A, Mirian A, Akiwate G, Blume A, Saul LK, *et al*. Measuring security practices and how they impact security. In: Proceedings of the Internet Measurement Conference; 2019 Oct; Amsterdam, Netherlands. p. 36-49.
15. Elumalai A, Roberts R. Unlocking business acceleration in a hybrid cloud world. McKinsey Digital. 2019 Aug.
16. Franklin JF, Johnson KN, Johnson DL. Ecological forest management. Long Grove, IL: Waveland Press; 2018.
17. Fürstenau D, Baiyere A, Kliewer N. A dynamic model of embeddedness in digital infrastructures. Inf Syst Res. 2019;30(4):1319-42.
18. Geier M, Chakraborty S. Challenges in IT operations management at a German university chair–ten years in retrospect. In: Proceedings of the 2019 ACM SIGUCCS Annual Conference; 2019 Oct-Nov; New Orleans, LA. p. 97-103.
19. Goundar S, Bhardwaj A. A framework for effective threat hunting. Netw Secur J. 2019.
20. Gunasekaran A, Yusuf YY, Adeleye EO, Papadopoulos T, Kovvuri D, Geyi DAG. Agile manufacturing: an evolutionary review of practices. Int J Prod Res. 2019;57(15-16):5154-74.
21. Hassan N. Ransomware revealed. Berkeley, CA: Apress; 2019. p. 47-68.
22. Huang K, Siegel M, Madnick S. Systematically understanding the cyber attack business: a survey. ACM Comput Surv. 2018;51(4):1-36.
23. Indu I, Anand PR, Bhaskar V. Identity and access management in cloud environment: mechanisms and challenges. Eng Sci Technol Int J. 2018;21(4):574-88.
24. Kocoloski B, Lange J, Pedretti K, Brightwell R. Hobbes: a multi-kernel infrastructure for application composition. In: Operating systems for supercomputers and high performance computing. Singapore: Springer Singapore; 2019. p. 241-67.
25. Kure H, Islam S. Cyber threat intelligence for improving cybersecurity and risk management in critical

infrastructure. J Univers Comput Sci. 2019;25(11):1478-502.
26. Kushala K, Kurunthachalam A. Enhancing cloud security in healthcare and finance: zero trust and homomorphic encryption for data privacy and risk management. Int J Bus Manag Econ Rev. 2019;2(6):118.
27. Linkov I, Kott A. Fundamental concepts of cyber resilience: introduction and overview. In: Cyber resilience of systems and networks. Cham: Springer; 2019. p. 1-25.
28. Malatji M, Von Solms S, Marnewick A. Socio-technical systems cybersecurity framework. Inf Comput Secur. 2019;27(2):233-72.
29. Marti M, Tavares De Almeida Soares D. Looking for the next start-up fairy tale in India: cultural and institutional problems Swiss start-ups face when internationalising to India. 2018.
30. Martin A, Raponi S, Combe T, Di Pietro R. Docker ecosystem–vulnerability analysis. Comput Commun. 2018;122:30-43.
31. McGuigan L. Automating the audience commodity: the unacknowledged ancestry of programmatic advertising. New Media Soc. 2019;21(11-12):2366-85.
32. McKenna AT, Gaudion AC, Evans JL. The role of satellites and smart devices: data surprises and security, privacy, and regulatory challenges. Penn State Law Rev. 2019;123:591.
33. Mei H, Guo Y. Operating systems for Internetware: challenges and future directions. In: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS); 2018 Jul; Vienna, Austria. p. 1377-84.
34. Mistry S, Lalwani P, Potdar M. Endpoint protection through Windows operating system hardening. Int J Comput Appl Technol Res. 2018. doi:10.7753/IJCATR0702.1005.
35. Mohammed A. Best practices for auditing security operations centers (SOC) for compliance and threat detection. Adv Comput Sci. 2018;1(1).
36. Morrison GR, Ross SJ, Morrison JR, Kalman HK. Designing effective instruction. Hoboken, NJ: John Wiley & Sons; 2019.
37. Mueller ST, Hoffman RR, Clancey W, Emrey A, Klein G. Explanation in human-AI systems: a literature meta-review, synopsis of key ideas and publications, and bibliography for explainable AI. arXiv. 2019:arXiv:1902.01876.
38. Nina P, Ethan K. AI-driven threat detection: enhancing cloud security with cutting-edge technologies. Int J Trend Sci Res Dev. 2019;4(1):1362-74.
39. Padur SKR. Empowering developer & operations self-service: Oracle APEX+ORDS as an enterprise platform for productivity and agility. Int J Sci Res Sci Eng Technol. 2018;4(11):364-72.
40. Parker JT, Gregg M. Host security. 2019.
41. Pattaranantakul M, He R, Song Q, Zhang Z, Meddahi A. NFV security survey: from use case driven threat analysis to state-of-the-art countermeasures. IEEE Commun Surv Tutorials. 2018;20(4):3330-68.
42. Petrik R, Arik B, Smith JM. Towards architecture and OS-independent malware detection via memory forensics. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018 Oct; Toronto, Canada. p. 2267-9.
43. Qin Z, Zhang H, Qin X, Xu K, Dimitrov KNA, Wang G, *et al*. Classification and software culture. In: Fundamentals of software culture. Singapore: Springer Singapore; 2018. p. 83-136.
44. Rapuzzi R, Repetto M. Building situational awareness for network threats in fog/edge computing: emerging paradigms beyond the security perimeter model. Future Gener Comput Syst. 2018;85:235-49.
45. Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R. Developing cyber resilient systems: a systems security engineering approach. NIST Special Publication 800-160 Vol. 2 (Draft). Gaithersburg, MD: National Institute of Standards and Technology; 2019.
46. Rydén P, El Sawy OA. Real-time management in the digital economy. Time issues in strategy and organization. 2019:59-93.
47. Serpanos D, Wolf M. Internet-of-Things (IoT) systems: architectures, algorithms, methodologies. 2018.
48. Sjarif NNA, Chuprat S, Mahrin MNR, Ahmad NA, Ariffin A, Senan FM, *et al*. Endpoint detection and response: why use machine learning? In: 2019 International Conference on Information and Communication Technology Convergence (ICTC); 2019 Oct; Jeju, Korea. p. 283-8.
49. Son LH, Jha S, Kumar R, Chatterjee JM, Khari M. Collaborative handshaking approaches between internet of computing and internet of things towards a smart world: a review from 2009–2017. Telecommun Syst. 2019;70(4):617-34.
50. Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J. A survey of IoT-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun Surv Tutorials. 2018;20(4):3453-95.
51. Stevens R, Votipka D, Redmiles EM, Ahern C, Sweeney P, Mazurek ML. The battle for New York: a case study of applied digital threat modeling at the enterprise level. In: 27th USENIX Security Symposium (USENIX Security 18); 2018 Aug; Baltimore, MD. p. 621-37.
52. Tanya B, Rahul C. Data at rest, data at risk: evaluating encryption and access control mechanisms in cloud storage systems. Int J Trend Sci Res Dev. 2019;3(6):1462-78.
53. Tao M, Zuo J, Liu Z, Castiglione A, Palmieri F. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Gener Comput Syst. 2018;78:1040-51.
54. Tedeschi S, Emmanouilidis C, Mehnen J, Roy R. A design approach to IoT endpoint security for production machinery monitoring. Sensors (Basel). 2019;19(10):2355.
55. Tiberius V, Hirth S. Impacts of digitization on auditing: a Delphi study for Germany. J Int Account Audit Tax. 2019;37:100288.
56. Törngren M, Grogan PT. How to deal with the complexity of future cyber-physical systems? Designs. 2018;2(4):40.
57. Vetter JS, Brightwell R, Gokhale M, McCormick P, Ross R, Shalf J, *et al*. Extreme heterogeneity 2018-productive computational science in the era of extreme heterogeneity: report for DOE ASCR workshop on extreme heterogeneity. Washington, DC: USDOE Office of Science; 2018.
58. Watada J, Roy A, Kadikar R, Pham H, Xu B. Emerging

trends, techniques and open issues of containerization: a review. IEEE Access. 2019;7:152443-72.
59. Weissman Z, Tiemann T, Moghimi D, Custodio E, Eisenbarth T, Sunar B. Jackhammer: efficient rowhammer on heterogeneous FPGA-CPU platforms. arXiv. 2019:arXiv:1912.11523.
60. Wydmuch M, Kempka M, Jaśkowski W. VizDoom competitions: playing Doom from pixels. IEEE Trans Games. 2018;11(3):248-60.
61. Zandberg K, Schleiser K, Acosta F, Tschofenig H, Baccelli E. Secure firmware updates for constrained IoT devices using open standards: a reality check. IEEE Access. 2019;7:71907-20.
62. Zhao L, Mannan M. TEE-aided write protection against privileged data tampering. arXiv. 2019:arXiv:1905.10723.