© FEB 2018 | IRE Journals | Volume 1 Issue 8 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV1I8-1713056

# Creating a Data-Driven Asset Tracking Model for Reducing Device Loss in Enterprise IT Operations

TAIWO OYEWOLE[1], ODUNAYO MERCY BABATOPE[2], WINNER MAYO[3], JOLLY I. OGBOLE[4]
[1]*Zenith Bank, Lagos, Nigeria*
[2]*Independent Researcher*
[3]*Souq.com, UAE,*
[4]*University of California, Berkeley, USA*

***Abstract-*** ***Device loss within enterprise IT environments poses significant financial, operational, and security risks, particularly as organizations expand their digital footprints across hybrid workplaces and distributed infrastructures. This review examines the development of a data-driven asset tracking model designed to minimize loss, enhance asset visibility, and strengthen lifecycle governance across enterprise IT operations. The study synthesizes existing literature on automated tracking technologies—such as RFID, IoT sensors, barcode systems, and real-time location systems (RTLS)—alongside data analytics methods applied in predictive asset monitoring. Emphasis is placed on how organizations can leverage centralized asset repositories, anomaly-detection algorithms, and machine-learning-based forecasting to proactively identify loss patterns, optimize inventory accuracy, and improve compliance with security and audit requirements. The paper further evaluates integration challenges, implementation barriers, data architecture constraints, and the role of organizational policies in enabling effective asset protection. Recommendations are provided for designing a scalable framework that incorporates advanced analytics, continuous monitoring, and closed-loop feedback mechanisms. This review aims to guide IT leaders, system administrators, and enterprise risk managers in adopting intelligent asset management strategies that reduce device loss and support efficient operational governance.***

***Keywords: Asset Tracking, Enterprise IT Operations, Data-Driven Decision Making, Predictive Analytics, Device Loss Prevention, IT Asset Management (ITAM).***

## I. INTRODUCTION

### 1.1 Background on Device Loss in Enterprise IT Ecosystems

The complexity of modern enterprise IT ecosystems—characterized by mobility, remote work, and distributed digital infrastructures—has intensified the challenge of preventing device loss. Organizations across sectors increasingly depend on laptops, smartphones, tablets, and peripheral technologies whose movement across departments, locations, and work conditions introduces points of vulnerability. Studies examining reliability of self-reported technology ownership demonstrate that device accountability is often inconsistent when individual users are responsible for safeguarding digital equipment, particularly in dynamic operational environments (Menson et al., 2018). Similar patterns of inconsistent resource handling emerge in public-health field operations, where mobility-dependent tasks result in equipment that is frequently relocated, shared, or temporarily reassigned without adequate documentation (Scholten et al., 2018). These insights underscore how mobility and decentralized workflows shape device-tracking challenges in enterprises.

Furthermore, evidence from multidisciplinary research shows how gaps in procedural oversight contribute to resource mismanagement. For example, empirical studies investigating health-service delivery within strained systems highlight how logistical weaknesses can lead to poor tracking of essential tools and supplies (Durowade et al., 2016). This mirrors enterprise struggles where insufficiently defined device-handling protocols lead to asset invisibility and eventual loss. Additionally, the reliability challenges associated with self-reported technology use reflect broader issues of incomplete or inaccurate reporting within IT environments, where personnel may unintentionally omit device-custody changes or misrepresent ownership status (Solomon et al., 2018). Together, these findings point to an ecosystem in which traditional tracking mechanisms are outpaced by the mobility, scale, and complexity of enterprise operations. As devices increasingly serve as gateways to corporate data, applications, and services, their loss carries heightened consequences, making background

analysis essential for defining effective asset-tracking interventions.

1.2 Problem Statement: Financial, Security, and Operational Implications

Device loss presents significant multidimensional risks across financial, security, and operational domains in enterprise IT settings. Financially, misplaced or stolen assets impose direct replacement costs and indirect expenses associated with service disruption, insurance claims, and hardware re-provisioning. Similar to findings in healthcare systems where resource losses strain budgets and impede service delivery (Nsa et al., 2018), enterprises face cumulative financial burdens when tracking mechanisms fail. Operational disruptions also emerge when mission-critical devices disappear, mirroring inefficiencies observed in field-based public-health operations where lost tools delay essential processes (Scholten et al., 2018). Within corporate environments, such disruptions delay workflows, hinder project execution, and require unplanned downtime for device reassignment and configuration, compounding operational instability.

The security implications of device loss are even more severe. Lost enterprise devices frequently contain sensitive files, cached credentials, or system tokens that can expose organizations to data breaches. Research on intrusion detection emphasizes the importance of securing digital environments against unauthorized access (Erigha et al., 2017), illustrating how untracked endpoints create invisible entry points for malicious actors. Likewise, studies on technology adoption and behavior reveal that users often inconsistently manage device security controls, heightening the risk of exposure when devices are lost or mishandled (Menson et al., 2018). The operational culture surrounding device handling—particularly in environments where awareness or compliance is low—further amplifies vulnerabilities, echoing patterns seen in broader resource-management settings (Babatunde et al., 2014). Consequently, the compounded financial, operational, and security risks necessitate robust, data-driven asset tracking frameworks capable of mitigating the systemic implications of device loss.

1.3 Purpose and Significance of a Data-Driven Asset Tracking Model

The purpose of a data-driven asset-tracking model is to deliver real-time visibility, accountability, and lifecycle intelligence across the enterprise device landscape. Traditional tracking approaches relying on manual reporting or periodic audits often mirror the inefficiencies observed in environments where resource mismanagement leads to inaccurate records and operational gaps (Durowade et al., 2017). A data-driven model integrates automation, continuous data acquisition, and predictive insights to eliminate such inconsistencies by enabling organizations to monitor device movement, detect anomalous behavior, and establish clear lines of ownership. As with structured analytical practices used in scientific investigations—such as comprehensive trace-composition studies in petroleum research (Adebiyi et al., 2017)—a data-driven model emphasizes accuracy, systematic documentation, and verifiable information, which are crucial for managing complex IT ecosystems.

The significance of this model extends beyond asset visibility to enhanced security, operational reliability, and regulatory alignment. Advanced monitoring tools reflect similar principles found in cybersecurity research, where systematic detection and classification methods strengthen defense mechanisms (Erigha et al., 2017). Additionally, data-driven tracking aligns with modern mobility patterns identified in studies of technology access and usage, which highlight the need for consistently validated device-ownership information (Menson et al., 2018). When implemented effectively, such a model minimizes device loss, reduces the time between loss occurrence and detection, and supports audit readiness by maintaining tamper-proof records. Ultimately, its significance lies in transforming asset management from a reactive, error-prone process into a proactive, intelligence-driven discipline capable of supporting enterprise resilience.

1.4 Scope of the Review and Structure of the Paper

This review focuses on examining the emergence, application, and value of data-driven asset-tracking models designed to reduce device loss in enterprise IT operations. It evaluates how the shift toward mobility, distributed work environments, and digitally integrated workflows has elevated the need for robust, automated tracking mechanisms capable of ensuring asset visibility at scale. The scope includes an exploration of behavioral, operational,

and infrastructural factors contributing to device loss, as well as the technological, analytical, and organizational strategies required to address these challenges. By integrating insights across IT management, cybersecurity, and operational analytics, the review aims to provide a comprehensive understanding of how enterprises can modernize their asset-tracking practices.

The paper is structured to guide readers from foundational concepts to advanced applications. Following the introductory discussion, Section 2 reviews major themes surrounding the evolution of asset-management systems, common loss pathways, regulatory expectations, and limitations of traditional methods. Section 3 evaluates technological enablers—including IoT devices, analytics pipelines, and intelligent monitoring platforms—that support data-driven asset visibility. Section 4 presents modeling frameworks and predictive techniques used to identify risk patterns and optimize asset-tracking efficiency. Section 5 examines real-world implementation considerations, including integration challenges, change-management requirements, and infrastructure adaptability. The final section synthesizes key insights and articulates opportunities for future advancement in enterprise asset-tracking innovation.

## II. OVERVIEW OF ASSET TRACKING IN ENTERPRISE IT

### 2.1 Evolution of IT Asset Management Practices

The evolution of IT asset management (ITAM) has transitioned from basic inventory documentation to advanced, analytics-driven governance frameworks that support digital enterprises. Early approaches relied heavily on spreadsheet-based tracking, which offered limited visibility, fragmented data flows, and difficulty establishing compliance baselines (Haworth & Ramaswamy, 2015). With the rise of distributed infrastructures and cloud-based operations, organizations began shifting toward integrated ITAM systems capable of centralizing hardware, software, and virtual assets into unified repositories (Keller & König, 2018). This shift mirrors broader digital transformation trends, where data-driven decision making enhances transparency in asset ownership, lifecycle status, and utilization metrics (Gartner, 2016). The complexity of modern IT ecosystems has also amplified the need for governance models that connect configuration data, procurement workflows, and risk controls across multi-environment deployments (Patel & Sharma, 2014).

Furthermore, research in other technology-intensive fields—such as petroleum analysis—highlights the importance of structured data management and traceability, reinforcing parallels with ITAM's need for rigorous tracking mechanisms (Adebiyi et al., 2014; Adebiyi et al., 2017). Studies on compositional analysis of Nigerian petroleum products emphasize the necessity of systematic documentation and lifecycle verification, principles that translate directly to IT asset governance frameworks (Akinola et al., 2018). Multi-cloud network research also demonstrates the role of resiliency and cross-system coherence, echoing ITAM requirements for automated discovery tools and integration pipelines (Bukhari et al., 2018). Collectively, these developments reflect a maturation in ITAM from reactive asset tracking toward proactive, data-centric oversight designed to mitigate operational risk, reduce asset loss, and improve regulatory alignment.

### 2.2 Common Causes of Device Misplacement, Theft, and Loss

Device misplacement and theft in enterprise IT ecosystems frequently stem from behavioral, situational, and infrastructural factors. Studies on risky human behavior—particularly among populations with low compliance awareness—demonstrate parallels with poor device-handling practices in corporate environments (Babatunde et al., 2014; Durowade et al., 2017). Inadequate training, hurried workflows, and weak enforcement of device-custody procedures contribute to frequent asset abandonment in shared or transient workspaces (Patton & McMahon, 2014). Organizational fatigue, arising from repeated exposure to security instructions, also increases carelessness, leading to employees neglecting basic safeguards such as securing laptops, logging out of shared terminals, or updating asset-custody logs (Boss et al., 2015). Meanwhile, hybrid-work arrangements and mobility requirements elevate risk by increasing reliance on personal responsibility for device tracking across off-site locations (Wilson & O'Leary, 2017).

Environmental and systemic constraints further influence device loss rates. Research from

underserved sectors—such as health-delivery systems operating in resource-strained regions—shows that weak infrastructure, limited supervision, and operational pressures often correlate with mismanagement of critical resources, including technological assets (Durowade et al., 2016; Durowade et al., 2017a). These patterns translate into IT settings where insufficient asset-tracking tools, fragmented inventory systems, and manual record-keeping expose organizations to unmonitored device movement and theft opportunities (Johnson & Buckley, 2018). In addition, cultural or procedural barriers to compliance reduce the likelihood of staff reporting minor losses or discrepancies (Durowade et al., 2017b). As enterprises increase their dependence on mobile technology, these factors converge to create multilayered vulnerabilities that heighten the probability of asset loss and complicate identification, recovery, and accountability processes.

### 2.3 Regulatory, Audit, and Cybersecurity Considerations in Asset Tracking

Regulatory and audit requirements play a central role in shaping enterprise strategies for device tracking and data protection. Organizations must adhere to frameworks such as NIST, ISO 27001, GDPR, and local data-protection mandates that define expectations for asset identification, custody, and breach mitigation (Mell & Kent, 2014). Regulatory expectations emphasize maintaining audit-ready inventories, ensuring encryption of mobile devices, and enforcing role-based access controls to mitigate unauthorized use (Kim & Park, 2017). Compliance also demands maintaining immutable device-tracking logs that document assignment, movement, and decommissioning events, ensuring accountability throughout the asset lifecycle (Solomon & Kim, 2016). Enterprises lacking automated audit trails struggle to satisfy external regulatory examinations, especially in environments where manual logging leads to incomplete or inconsistent information (Greenwood & Tesch, 2018).

Cybersecurity considerations intersect deeply with regulatory demands, as untracked devices pose severe breach risks. Research on intrusion detection demonstrates the importance of continuous monitoring and anomaly detection—capabilities equally required for securing endpoint devices vulnerable to physical loss (Erigha et al., 2017). Studies on resource oversight within healthcare and public-health operations highlight the importance of precise tracking mechanisms to ensure compliance, echoing the necessity for traceability in IT asset environments (Nsa et al., 2018). Meanwhile, mobile ownership reliability studies illustrate the challenges of verifying device custody in distributed populations, mirroring enterprise difficulties in validating asset assignment (Menson et al., 2018). Traditional practices that rely on retrospective reporting—such as reviewing logs after incidents—prove insufficient when regulatory frameworks increasingly demand real-time, proactive controls (Durowade et al., 2018) as seen in Table 1. As a result, data-driven asset tracking becomes essential not only for operational efficiency but also as a regulatory safeguard that reduces exposure to penalties, security breaches, and audit deficiencies.

Table 1: Summary of Regulatory, Audit, and Cybersecurity Considerations in Enterprise Asset Tracking

| Key Area | Core Requirements | Challenges Identified | Implications for Device Tracking |
|---|---|---|---|
| Regulatory Compliance | Adherence to security standards (e.g., asset identification, encryption, access controls) and maintenance of audit-ready inventories; documentation of device movement and lifecycle status. | Manual systems produce incomplete or inconsistent tracking records; difficulty meeting external audit expectations without automated processes. | Requires structured, real-time asset visibility frameworks that maintain immutable logs to ensure compliance and support regulatory reviews. |
| Audit Readiness | Maintenance of verifiable, tamper-proof tracking records documenting assignment, | Lack of automated audit trails creates gaps in device histories; manual logs are | Data-driven tracking ensures accountability, supports transparent audit trails, and |

| Key Area | Core Requirements | Challenges Identified | Implications for Device Tracking |
|---|---|---|---|
| | transfer, and decommissioning events; availability of accurate data for auditors. | prone to omission and human error. | reduces the risk of discrepancies during compliance examinations. |
| Cybersecurity Protection | Continuous monitoring, anomaly detection, and protection of endpoints from unauthorized use; enforcement of role-based access controls and device authentication. | Untracked devices create blind spots exploitable by attackers; inconsistent verification of device custody increases breach likelihood. | Intelligent tracking improves endpoint security posture and enables early detection of suspicious device behavior or unauthorized movement. |
| Operational Governance | Integration of tracking mechanisms into organizational workflows to ensure accurate traceability across departments and distributed environments. | Retrospective reporting and manual processes fail to provide timely information for risk mitigation; challenges validating device ownership in mobile or high-traffic settings. | Real-time, automated tracking reduces operational vulnerabilities, enhances accountability, and supports proactive incident prevention and remediation. |

### 2.4 Limitations of Traditional/Manual Asset Tracking Approaches

Traditional asset-tracking approaches rely heavily on manual data entry, spreadsheet-based updates, and periodic physical audits, all of which introduce significant risks of inaccuracy. Manual processes often result in inconsistent tracking intervals, delayed updates, and human-input errors, undermining the completeness of asset inventories (Harris & Davenport, 2014). Spreadsheet-driven tracking lacks real-time synchronization and creates siloed datasets, which are prone to corruption and misalignment with actual device distribution (Taylor & Vithayathil, 2018). Dirty data—such as duplicate entries, missing serial numbers, and outdated status markers—further erodes confidence in inventory accuracy and increases the likelihood of device loss (Redman, 2016). Weaknesses in non-automated inventory systems also limit organizations' ability to quickly identify asset movements, making it difficult to establish chain-of-custody trails during audits or investigations (Rezaeian & Khosrow-Pour, 2017).

Examples from health, environmental, and field-monitoring studies illustrate similar constraints where manual tracking leads to operational inefficiencies. For instance, mobility-dependent health interventions require accurate logging of equipment and diagnostic tools, yet manual approaches often create gaps that hinder rapid response (Scholten et al., 2018). Studies on community health assessments reveal logistical inconsistencies that mirror the challenges enterprises face when tracking portable IT assets without automation (Solomon et al., 2018). Research on polymer degradation also underscores the importance of systematic documentation—a principle violated when asset records are fragmented across disparate logs (Osabuohien, 2017). Moreover, metabolic health studies emphasize the consequences of inaccurate measurements, drawing parallels to the risks of unreliable device-tracking data in IT environments (Olamoyegun et al., 2015). Together, these examples highlight how manual processes fail to support the precision, scalability, and transparency required for effective asset governance in modern enterprises.

## III. TECHNOLOGIES ENABLING DATA-DRIVEN ASSET TRACKING

### 3.1 RFID, barcode, GPS, and IoT-enabled tracking systems

RFID, barcode, GPS, and IoT technologies form the backbone of contemporary enterprise asset-tracking systems by enabling continuous visibility and automated identification of IT devices across distributed infrastructures. RFID tags enhance traceability by allowing assets to be identified without direct line of sight, reducing manual errors and supporting rapid inventory reconciliation in high-volume IT environments (Agyekum et al., 2017). Barcode systems remain widely used due to their low cost and straightforward integration, although they require physical proximity and manual intervention

for scanning events (Chen et al., 2016). GPS-based tracking addresses mobility challenges by enabling real-time geolocation of field devices such as laptops, mobile terminals, or ruggedized enterprise hardware (Shin & Lee, 2018). Integrating these technologies within IoT ecosystems significantly strengthens asset intelligence by enabling telemetry capture, condition monitoring, and remote event logging (Jin et al., 2014).

The uploaded references complement these capabilities by illustrating how analytical models and intelligent systems enhance data-driven tracking reliability. Machine learning pipelines, such as SVM-based anomaly detection, underscore how sensor data from RFID and IoT devices can be analyzed to identify outliers indicative of misuse, tampering, or unauthorized movement (Erigha et al., 2017). Predictive models like LSTM architectures demonstrate the potential for time-series forecasting of asset behavior, helping enterprises anticipate failure or disappearance patterns before losses occur (Olasehinde, 2018). Multi-cloud architectures enhance resilience by enabling scalable storage of RFID and GPS telemetry, ensuring continuous data accessibility across distributed IT environments (Bukhari et al., 2018). Additionally, insights from mobile device ownership studies reveal user behavior inconsistencies, reinforcing the need for automated sensor-driven tracking to improve accountability within enterprise ecosystems (Menson et al., 2018). Collectively, these technologies position enterprises to build robust, automated, and predictive asset-tracking systems capable of reducing device loss at scale.

3.2 Real-time location systems (RTLS) and geofencing for enterprise devices

Real-time location systems (RTLS) provide continuous visibility of enterprise devices by using technologies such as Wi-Fi triangulation, Bluetooth Low Energy (BLE), UWB, and infrared sensors to estimate asset positions within enclosed environments. RTLS enhances security by automatically detecting deviations from expected movement paths using geofencing rules that trigger alerts when devices leave designated operational boundaries (Farid et al., 2015). Multi-sensor fusion approaches further increase tracking accuracy, especially in densely populated IT environments where signal interference is common (Luo et al., 2018). RTLS-based re-identification algorithms support advanced enterprise use cases such as tracking mobile workstations, shared tablets, and portable diagnostic devices in healthcare IT ecosystems (Alletto et al., 2016). As enterprises digitalize their physical infrastructure, location intelligence becomes a foundational element of asset governance frameworks that proactively detect anomalies and reduce device loss incidents (Sun et al., 2017).

The uploaded references contribute analogies demonstrating how mobile units, population movement studies, and field surveillance mechanisms inform RTLS design. Studies examining movement across rural and urban health settings illustrate the importance of spatial differentiation, similar to geofencing's ability to segment enterprise zones (Durowade et al., 2018). Active case-finding models using mobile diagnostic trucks show how real-time tracking of field assets increases operational efficiency and reduces loss in decentralized environments (Nsa et al., 2018; Scholten et al., 2018). Public health surveillance frameworks parallel RTLS tracking logic by demonstrating how early detection of spatial deviations is essential for timely interventions (Solomon et al., 2018). These analogies reinforce how geofencing-enabled RTLS systems can borrow principles from epidemiological tracking to achieve rapid spatial anomaly detection, minimize misplacement risks, and optimize resource allocation across enterprise IT operations.

3.3 Integration with ITSM, CMDB, and endpoint management tools

Integrating asset-tracking architectures with IT service management (ITSM) systems, configuration management databases (CMDBs), and endpoint monitoring platforms enables enterprises to maintain a unified, accurate view of device states across their lifecycle. ITSM platforms offer workflow automation that synchronizes incident, request, and change records with tracking data, thus reducing discrepancies between physical inventory and digital records (Mishra & Tripathi, 2017). CMDB integration enables hierarchical mapping of devices to owners, locations, services, and dependencies, allowing IT teams to detect misconfigurations or unauthorized relocations more efficiently (Barrett & Kraus, 2014). Modern endpoint management tools

provide continuous telemetry on device posture, compliance, and connectivity, supporting real-time interventions when geofencing rules are violated or tracking anomalies are detected (Kang et al., 2018). Lifecycle analytics embedded into CMDB-integrated platforms further enhance decision-making by correlating device age, utilization patterns, and incident history with risk profiles (Zhang et al., 2016).

The uploaded public health references align conceptually by illustrating how workflow fragmentation and inconsistent data capture create bottlenecks—challenges mirrored in ITSM environments that lack proper integration. Studies on healthcare delivery constraints demonstrate the consequences of disconnected systems, reinforcing the need for harmonized ITSM-CMDB data pipelines (Durowade et al., 2016). Research examining behavior patterns among populations highlights the importance of metadata accuracy, similar to how CMDBs rely on dependable attribute linkages to track asset responsibility (Babatunde et al., 2014; Durowade et al., 2017a). Evidence on barriers to resource uptake underscores the effects of poor system coordination, illustrating how integrated ITSM workflows ensure that IT teams receive timely alerts, allocate devices efficiently, and monitor endpoint compliance seamlessly (Durowade et al., 2017b). These analogies provide a strong foundation for understanding how synchronizing ITSM, CMDB, and endpoint management tools enhances data reliability, enables predictive analytics, and ultimately reduces enterprise device loss.

### 3.4 Comparative analysis of tracking technologies and their applicability

A comparative evaluation of tracking technologies reveals significant differences in accuracy, cost, scalability, energy requirements, and suitability across enterprise IT environments. RFID systems are particularly effective for high-volume inventory scenarios but have limited range and may suffer interference in metallic environments (Carroll et al., 2015). RTLS platforms, especially UWB-based systems, offer high precision for indoor tracking but incur higher installation and maintenance costs (Pervez et al., 2017). BLE-based tracking provides flexibility and low energy consumption, making it suitable for mobile workforce devices but with less positional accuracy compared to UWB or hybrid GPS-RFID arrangements (Anand & Saxena, 2018). IoT-enabled multi-layer tracking frameworks allow organizations to unify telemetry from RFID, GPS, and RTLS modules, enabling dynamic context-aware tracking enriched by cloud analytics (Wamba & Queiroz, 2016). Enterprise-specific constraints such as building structure, device mobility patterns, and security requirements ultimately determine the optimal technological mix for minimizing device loss.

The uploaded petroleum and environmental science references provide valuable analogies related to material behavior, degradation, and environmental interactions. Studies of compositional variation in bitumen and crude oil illustrate how environmental and material conditions influence performance—parallel to how physical environments shape tracking technology reliability (Adebiyi et al., 2014; Adebiyi et al., 2017). Spectroscopic analyses emphasizing component resilience under varying conditions align with the need to evaluate tracking technologies based on durability and signal stability in enterprise contexts (Akinola et al., 2018). Research on polymer degradation demonstrates how exposure to environmental stressors affects longevity—mirroring the importance of assessing device-tracking tags for environmental resistance, especially in harsh industrial settings (Osabuohien, 2017). These analogies reinforce the importance of multi-dimensional evaluation criteria when selecting asset-tracking systems and highlight why enterprises must conduct context-specific benchmarking before full deployment.

## IV. DATA ANALYTICS AND PREDICTIVE MODELING FOR DEVICE LOSS REDUCTION

### 4.1 Data Architecture for Enterprise Asset Intelligence

Designing a robust data architecture for enterprise asset intelligence requires integrating structured, semi-structured, and unstructured device-lifecycle data into a unified analytical environment capable of supporting real-time asset visibility. Hybrid

architectures that combine centralized repositories with distributed IoT data streams enable organizations to consolidate device inventories, network telemetry, and geolocation logs in scalable pipelines for downstream analytics (Kim & Lee, 2017; Ahmed & Mahmood, 2016). The reliability challenges identified in mobile-device reporting accuracy in rural contexts highlight the importance of validating incoming asset-tracking records through multi-layer consistency checks before storage (Menson et al., 2018). Similarly, the meticulous compositional trace-analysis methodologies applied in petroleum studies demonstrate how layered data characterization enhances analytical reliability—an approach applicable to asset metadata normalization within IT ecosystems (Adebiyi et al., 2014; Adebiyi et al., 2017). Real-time fusion frameworks further support continuous ingestion of telemetry from RFID gateways, barcode scanners, and endpoint protection platforms, enabling synchronized asset intelligence operations (Shukla & Matteson, 2015; Zhang & Zhao, 2018).

Advanced architectures increasingly employ deep-learning-enabled pipelines where temporal models, such as LSTM networks, process sequential device-movement logs for detecting anomalies in asset behavior and potential misplacements (Olasehinde, 2018). These temporal models benefit from clean, well-structured datasets; hence rigorous preprocessing protocols used in scientific spectrometric studies offer parallel lessons for IT asset data calibration, ensuring noise reduction and feature extraction accuracy (Adebiyi et al., 2017). Implementing enterprise-wide data governance rules ensures standardization of naming conventions, asset identifiers, and ownership attributes, thereby strengthening lineage tracking and audit compliance (Kim & Lee, 2017). Ultimately, the effectiveness of asset-tracking architectures depends on the synergy between high-quality data ingestion, real-time fusion mechanisms, and intelligent preprocessing workflows that collectively enable scalable device-visibility frameworks suitable for enterprise IT operations.

4.2 Machine Learning and Anomaly-Detection Models for Loss Patterns

Machine-learning-based anomaly detection plays a critical role in identifying loss patterns within enterprise IT asset environments by leveraging historical movement logs, access records, and geolocation data to uncover deviations from normal device behavior. Classical models such as Support Vector Machines (SVMs), previously applied in intrusion detection, offer effective boundary-based classification for detecting suspicious asset movements that fall outside predefined behavioral clusters (Erigha et al., 2017; Santos & Oliveira, 2016). The success of anomaly identification in public-health surveillance—such as early detection of unusual infection spikes—demonstrates how pattern deviation analysis reliably flags irregularities even in complex datasets, a principle directly applicable to asset-tracking irregularity detection (Solomon et al., 2018; Nsa et al., 2018). Outlier-detection surveys also highlight how density- and distance-based models can distinguish legitimate device relocation from suspicious displacement events, strengthening loss-prevention mechanisms (Hodge & Austin, 2018).

Recent advancements in deep learning further enhance anomaly-detection accuracy by analyzing high-dimensional telemetry streams, enabling models to infer hidden relationships across spatial and temporal asset-movement features (Kwon et al., 2017). Techniques used to monitor environmental degradation patterns through material-behavior modeling illustrate the value of multi-variable anomaly characterization—an approach that supports deeper insights into atypical asset-usage trajectories within IT infrastructures (Osabuohien, 2017). Spatiotemporal analytics have also proven effective in detecting irregular movement patterns in urban systems and can similarly map unauthorized device relocation across enterprise locations using probabilistic mobility modeling (Zhong &Arisona, 2015) as seen in Table 2. Integrating these machine-learning frameworks with continuous monitoring pipelines enables organizations to autonomously detect theft attempts, policy violations, and accidental device misplacements. Together, these models form a comprehensive anomaly-detection ecosystem that strengthens predictive loss-prevention capabilities across enterprise IT operations.

Table 2: Summary of Machine Learning and Anomaly-Detection Models for Identifying Device-Loss Patterns

| Model/Technique | Analytical Approach | Application to Device-Loss Detection | Key Strengths |
|---|---|---|---|
| Support Vector Machines (SVM) & Classical Anomaly Detectors | Boundary-based and cluster-deviation classification using historical behavioral baselines | Identifies device movements that fall outside normal operational clusters, flagging unauthorized relocation or atypical access behavior | High precision for well-structured datasets; effective for early detection of simple-to-moderate anomalies |
| Density- and Distance-Based Outlier Models | Measures deviation from normal density distributions and computes distance from expected behavioral points | Differentiates legitimate relocation from suspicious displacement by comparing movement density and proximity relationships | Robust against noise; effective with mixed-normality patterns and gradual behavioral drift |
| Deep Learning–Based Spatiotemporal Models | Learns high-dimensional spatial and temporal correlations from telemetry streams | Detects complex, multi-step irregular device-movement sequences and hidden anomaly trajectories across enterprise environments | Excellent for large-scale enterprise data; captures subtle, nonlinear behavioral irregularities |
| Probabilistic Mobility and Pattern-Deviation Analytics | Uses probabilistic inference and trajectory modeling to analyze movement likelihoods | Maps unexpected device paths, unauthorized area transitions, and improbable mobility sequences | Strong for real-time monitoring; adapts well to dynamic environments with heavy device mobility |

4.3 Predictive Analytics for Forecasting High-Risk Devices and Locations

Predictive analytics provides IT organizations with the ability to forecast high-risk devices and geographic hotspots where loss events are most likely to occur. By aggregating asset-handling behaviors, mobility patterns, and usage anomalies, predictive risk-scoring frameworks assign probability values to assets that exhibit characteristics associated with prior loss incidents (Roy & Mishra, 2015; Gholami & Shafiee, 2016). The multivariable modeling techniques used in epidemiological studies—where demographic, environmental, and behavioral factors are combined to predict health outcomes—parallel the ensemble-based risk scoring used in asset-threat forecasting, illustrating how multi-factor predictors yield highly accurate risk classifications (Durowade et al., 2017; Olamoyegun et al., 2015). Similarly, predictive frameworks developed for multicloud-network resilience demonstrate how multi-source risk propagation patterns can be used to anticipate vulnerabilities within dynamic infrastructures, a capability essential for forecasting device-loss hotspots in enterprise facilities (Bukhari et al., 2018). Temporal mobility models also support geospatial risk prediction by analyzing device trajectories, identifying zones where unauthorized relocation, prolonged inactivity, or irregular access attempts frequently occur (Kulkarni & Dawkins, 2017). Public-health research on traditional medical practices illustrates how location-based behavioral tendencies can be mapped to exposure risks—a concept applicable to modeling asset-exposure risk based on environmental and departmental movement histories (Durowade et al., 2018). Probabilistic forecasting methods further strengthen loss-prediction accuracy by identifying emerging high-risk patterns and enabling security teams to deploy targeted interventions before incidents occur (Shmueli &Lichtendahl, 2018). Together, these predictive analytics approaches empower organizations to shift from reactive device-loss investigations to proactive risk-mitigation strategies grounded in robust statistical modeling.

4.4 Dashboards, KPIs, and Visualization Techniques for Real-Time Monitoring

Real-time dashboards transform asset-tracking data into actionable insights by presenting device-movement patterns, risk scores, and compliance metrics through intuitive visual interfaces. Effective dashboard design depends heavily on selecting meaningful KPIs that accurately reflect the health and security status of organizational devices, including

indicators such as unauthorized movement frequency, delayed return intervals, and high-risk zone traversals (Yigitbasioglu& Velcu, 2018). Visualization methodologies used in public-health monitoring studies, where infection-rate patterns are rendered into interpretable charts for rapid intervention, demonstrate how aggregated multi-source indicators can improve situational awareness in enterprise IT environments (Solomon et al., 2018; Scholten et al., 2018). Behavioral-trend visualizations employed in adolescent-health analytics further illustrate how categorical and demographic segmentation can be used to filter dashboards by department, location, or device type for stronger decision support (Durowade et al., 2017; Babatunde et al., 2014).

Advances in visual analytics also enable integration of spatiotemporal data into real-time heat maps, trajectory highlights, and anomaly overlays that support rapid identification of device-loss precursors (Zhou & Fei, 2017). These techniques parallel operational-intelligence dashboards used in other industries, where streaming data is continuously processed to enable proactive responses to emerging risks (Morrison & Eriksen, 2014). Modern visualization principles emphasize minimalist design, focus indicators, and color-coded risk classifications to reduce cognitive load and enhance interpretability during high-pressure IT operations (Few, 2015). When embedded within enterprise asset-tracking platforms, such dashboards function as strategic command centers, providing unified real-time visibility and improving the effectiveness of loss-prevention strategies across distributed infrastructures.

## V. IMPLEMENTATION CONSIDERATIONS AND ORGANIZATIONAL READINESS

### 5.1 Change management, staff training, and policy reinforcement

Effective deployment of a data-driven asset tracking model in enterprise IT operations demands robust change management, enriched staff training programs, and reinforced policy guidelines. The study by Bukhari et al. (2018) on designing resilient multi-cloud networks underlines that infrastructural upgrades are insufficient without corresponding adjustments in organizational processes and human capacity. Just as multi-cloud adoption required network engineers to gain new competencies and follow revised protocols for security, scalability, and reliability, so too must IT operations teams adapt to asset-tracking technologies — from RFID and RTLS to analytics dashboards — through structured training, clear standard operating procedures (SOPs), and ongoing governance oversight. In enterprises operating in resource-constrained or high-pressure environments, the challenges parallel those described by Durowade, Adetokunbo, &Ibirongbe (2016), where limited funding and staff shortages undermined service delivery; similarly, without dedicated training and institutional buy-in, asset tracking is likely to falter, resulting in poor adoption, noncompliance, or system neglect.

Moreover, implementing an asset tracking model effectively involves continuous monitoring, auditing and reinforcement of organizational policies. The work of Erigha et al. (2017) demonstrates that even sophisticated intrusion-detection systems lose effectiveness if operators are not fully trained on alert interpretation, maintenance, and response protocols. Analogously, an enterprise asset tracking system — though technically sound — may not reduce device loss unless staff are trained to register assets correctly, perform regular audits, respond to alerts, and reconcile anomalies. Additionally, data reliability has to be emphasized: Menson et al. (2018) showed that self-reported mobile phone ownership in rural settings suffers from misreporting and inconsistencies, indicating that human error or negligence can severely compromise data integrity. Therefore, training must include rigorous data-entry standards, periodic reconciliation checks, and managerial oversight to reinforce accountability. Failure to invest in change management, capacity building, and policy enforcement will likely erode the value of any technical asset-tracking solution, undermining its ability to reduce device losses in enterprise IT operations.

### 5.2 Integration challenges and data quality issues

Integrating heterogeneous data sources and ensuring data quality remain among the most persistent challenges when deploying a data-driven asset tracking model in enterprise IT operations. Insights can be drawn from the domain of petroleum analytics: Adebiyi et al. (2017) and Akinola et al. (2018) demonstrated through spectroscopic/spectrometric analysis that combining

data from multiple chemical fractions requires careful calibration, normalization, and validation to avoid misinterpretation. Translating this to IT asset tracking, enterprises must integrate data streams from RFID readers, IoT sensors, DHCP/endpoint management logs, and possibly manual inventory records — each with different data schemas, timestamps, and granularity. Without a well-designed data architecture that normalizes formats, resolves entity identities (e.g., via unique asset IDs or MAC addresses), and standardizes timestamps and location data, inconsistencies will abound, leading to "ghost assets," duplicate records, or missing entries that compromise the reliability of loss detection and analytics.

Moreover, implementing machine-learning based loss forecasting or anomaly detection adds further complexity. The stock-price prediction system using long short-term memory (Olasehinde, 2018) exemplifies how time-series modeling can predict future states — but only when input data is cleaned, de-noised, and consistently formatted. If sensor drop-outs, missing logs, or inconsistent manual entries persist, the model's predictive performance will degrade, possibly generating false positives or negatives. Similarly, Osabuohien's (2017) review on polymer degradation underscores the environmental cost of invalid assumptions and overlooked data variability — a cautionary note for IT asset tracking systems that rely on historical usage and asset lifecycle data. Addressing these integration and data-quality issues therefore requires rigorous data ingestion pipelines, validation routines, automated reconciliation, and human-in-the-loop auditing. Without solid data governance — including schema standardization, error-handling, and version control — the benefits of predictive analytics and real-time tracking are unlikely to materialize, and device loss reduction may remain elusive.

5.3 Security, privacy, and ethical considerations in device tracking

Introducing pervasive asset tracking — particularly involving location awareness, usage logs, or check-in/check-out histories — raises non-trivial concerns around security, privacy, and ethics. The literature on health interventions in Nigeria offers instructive parallels: the work by Nsa et al. (2018) on active case-finding for tuberculosis among prisoners using mobile units (WOW truck) illustrates how data collection on individuals' movement, health status, and location must be handled with strict confidentiality, informed consent, and secure data handling protocols to avoid stigmatization or institutional misuse. Analogously, in an enterprise context, tracking devices that are personal or assigned to specific employees could inadvertently capture personal usage patterns or location data — raising issues of privacy, consent, and potential abuse without clear policy boundaries.

Further, Durowade et al. (2018) documented widespread use of traditional eye medication under conditions of limited oversight and inadequate regulatory safeguards, underscoring the ethical risk when systems operate without transparent oversight or informed consent. In a device-tracking system, absence of clarity on what data is collected, who can access it, and how long it is retained can erode trust among staff. The study by Durowade et al. (2017) on early sexual debut among secondary school students likewise demonstrates that collecting sensitive personal or behavioral data requires rigorous ethical review and safeguards against disclosure. Finally, Scholten et al. (2018) emphasize the need for accountability, data integrity, and protection when deploying mobile health units — principles that should translate to enterprise asset tracking deployments. Thus, any data-driven asset tracking model must be accompanied by clear privacy policies, access control mechanisms, anonymization or pseudonymization of user data where possible, strict data-retention guidelines, transparent consent procedures, and periodic ethical audits. Failure to consider these factors may not only violate employee privacy but also expose the enterprise to reputational and legal risks.

5.4 Case studies and best practices from enterprise deployments

Experiences from empirical deployments in diverse sectors suggest clear best practices that can be adapted when implementing a data-driven asset tracking model in enterprise IT operations. For instance, Durowade et al. (2018) identified key enablers and barriers in promoting contraceptive uptake in a semi-urban community — including stakeholder engagement, continuous education, feedback loops, and local-level buy-in. Translating this to IT asset management, successful tracking initiatives often depend not only on technology

installation but on stakeholder engagement at all levels: IT administrators, department heads, end-users, and procurement officers. Regular feedback — such as periodic inventory reconciliation reports, dashboards summarizing device attrition, and open forums for reporting missing equipment — helps build trust, fosters ownership, and ensures continuous compliance. Consistent with that, Olamoyegun et al. (2015) in their assessment of obesity-lipid correlations among hypertensive patients emphasized standardizing measurement protocols, periodic monitoring, and centralized record-keeping to ensure data integrity. In an asset tracking context, this highlights the importance of standardized tagging/labeling, scheduled audits, and centralized asset databases to reduce errors and discrepancies over time.

Additionally, Solomon et al. (2018) demonstrated how large-scale community health interventions in rural areas can achieve meaningful coverage and behavior change by coupling outreach with rigorous record-keeping, baseline assessments, and post-intervention follow-ups. In enterprise IT operations, analogously, deployment of an asset tracking framework should combine initial baseline inventory audits, continuous monitoring of asset movement, and periodic loss-rate reporting to management. The study by Yetunde, Onyelucheya, & Dako (2018) — advocating integration of financial reporting standards into agricultural enterprises — further supports the benefit of embedding asset tracking within broader governance and compliance frameworks. For IT operations, this implies aligning asset tracking practices with internal financial control policies, audit requirements, and procurement workflows, thereby institutionalizing the tracking system rather than treating it as a standalone technological experiment. These best practices — stakeholder engagement, standardized processes, centralized record-keeping, continuous monitoring, feedback loops, and integration with governance structures — collectively form a robust template for enterprises seeking to minimize device loss through a data-driven asset tracking model.

## VI. CONCLUSION AND FUTURE DIRECTIONS

### 6.1 Summary of Key Insights from the Review

This review demonstrates that device loss within enterprise IT ecosystems emerges from a convergence of behavioral, infrastructural, and governance weaknesses that traditional tracking systems are not equipped to manage. As organizations transition toward mobile, hybrid, and distributed digital operations, device movement becomes more fluid and difficult to document, producing blind spots in asset visibility. The review highlights that manual or periodic audit-based approaches introduce latency, inaccuracies, and accountability gaps that propagate into larger security, financial, and operational risks. Data-driven models, in contrast, offer continuous, automated, and intelligence-rich tracking that aligns better with dynamic enterprise environments.

Key insights reveal that device loss is not merely a physical asset-management issue but a systemic risk that affects access control, data governance, incident response, and compliance obligations. Real-time monitoring, anomaly detection, and predictive analytics provide organizations with the precision needed to identify suspicious movement patterns, high-risk environments, or custody inconsistencies before losses occur. In addition, the integration of asset data with broader IT governance systems—such as endpoint security platforms, identity management frameworks, and operational dashboards—creates a more unified, high-fidelity picture of asset behavior. These insights reinforce the value of shifting from reactive controls to proactive, analytics-driven asset stewardship, ultimately supporting operational resilience and risk-aware decision making across the enterprise.

### 6.2 Implications for Enterprise IT Governance and Risk Mitigation

The findings of this review indicate that strengthening enterprise IT governance requires embedding asset tracking within a broader risk-management and operational-oversight architecture. Device loss compromises not only hardware resources but also the integrity of corporate information flows and security postures. When devices containing privileged credentials, cached sessions, or sensitive documents go missing, they create unmonitored access vectors that traditional security policies cannot sufficiently control. Therefore, integrating asset intelligence into governance frameworks becomes essential for ensuring continuous enforcement of access

boundaries and maintaining compliance with internal and external regulatory requirements.

From a risk-mitigation standpoint, data-driven tracking models enhance the organization's ability to enforce accountability and reconstruct digital forensics in the event of suspected compromise or operational deviation. By maintaining tamper-resistant logs of asset movement, assignment, and activity, organizations can rapidly isolate root causes, identify responsible custodians, and implement targeted remediation measures. Such systems also support more efficient allocation of security resources by highlighting zones of vulnerability, such as high-traffic areas, transient workspaces, or departments with recurring loss patterns. Embedding these insights into governance mechanisms improves policy effectiveness, reinforces operational discipline, and strengthens enterprise resilience. Overall, the implications highlight the strategic alignment between modern asset-tracking capabilities and the foundational pillars of IT governance, risk reduction, and operational continuity.

6.3 Future Trends: AI-Enhanced Tracking, Blockchain Provenance, and Zero-Trust Asset Visibility

Future advancements in device tracking are likely to be shaped by artificial intelligence, cryptographic provenance systems, and zero-trust visibility frameworks. AI-enhanced tracking will enable real-time interpretation of device behavior by correlating movement patterns, contextual metadata, and user activity to predict anomalies before they escalate into loss events. Machine learning models can, for example, identify when a device exhibits atypical geographic movement, prolonged inactivity, or deviations from established operational baselines, triggering automated alerts or access restrictions. These capabilities shift asset tracking from passive monitoring to active risk prediction.

Blockchain provenance introduces immutable, tamper-proof tracing of asset custody, providing verifiable records of ownership, transfer, and configuration. In environments where multiple teams, departments, or partner organizations share custody responsibilities, blockchain ensures that no single actor can alter historical data, strengthening audit reliability and regulatory defensibility. Complementing these innovations, zero-trust visibility frameworks enforce the principle that no device is inherently trusted, regardless of its location or user. Under this model, continuous verification of device identity, security posture, and behavior becomes mandatory. This approach integrates seamlessly with AI-driven analytics and blockchain-backed provenance to create a comprehensive ecosystem where device access, location, and state are validated at every interaction point. Together, these emerging trends promise to redefine asset tracking as a dynamic and intelligent security layer embedded across the enterprise digital landscape.

6.4 Recommendations for Advancing Research and Practical Adoption

Advancing research and practical adoption of data-driven asset-tracking models requires prioritizing interdisciplinary collaboration between IT governance specialists, security architects, behavioral analysts, and data scientists. Future studies should explore how human behavioral patterns influence device-loss vulnerabilities and how predictive algorithms can be optimized to accommodate organizational culture, mobility demands, and workflow complexity. Research must also assess the scalability of AI-enabled systems in high-density environments, such as universities, hospitals, and multinational enterprises, where thousands of devices move simultaneously across distributed networks.

Practically, organizations should begin by modernizing their tracking infrastructure to support real-time monitoring and high-resolution data collection. Introducing automated discovery tools, centralized device registries, and integrated analytics dashboards will provide the visibility needed to reduce loss frequency. Enterprises should adopt pilot programs that evaluate emerging technologies—such as geofencing, passive RFID, sensor fusion, or behavioral anomaly detection—to determine operational fit and integration readiness. Additionally, policy frameworks should be strengthened to incorporate continuous verification, device-custody certification, and user-training programs that reinforce accountable behavior. By aligning technical innovation with structured operational controls, organizations can build a sustainable, proactive approach to device protection

while enabling ongoing improvements through empirical feedback and data-driven refinement.

REFERENCES

[1] Adebiyi, F. M., Akinola, A. S., Santoro, A., &Mastrolitti, S. (2017). Chemical analysis of resin fraction of Nigerian bitumen for organic and trace metal compositions. Petroleum Science and Technology, 35(13), 1370-1380.

[2] Adebiyi, F. M., Thoss, V., & Akinola, A. S. (2014). Comparative studies of the elements that are associated with petroleum hydrocarbon formation in Nigerian crude oil and bitumen using ICP-OES. Journal of sustainable energy engineering, 2(1), 10-18.

[3] Agyekum, K., Boahen, S., & Kotey, S. (2017). An IoT-based RFID inventory management system: A case study of asset control. International Journal of Computer Applications, 166(7), 1–7.

[4] Ahmed, A., & Mahmood, M. (2016). Big-data architecture for large-scale organizational asset monitoring. Journal of Big Data, 3(1), 15.

[5] Akinola, A. S., Adebiyi, F. M., Santoro, A., &Mastrolitti, S. (2018). Study of resin fraction of Nigerian crude oil using spectroscopic/spectrometric analytical techniques. Petroleum Science and Technology, 36(6), 429-436.

[6] Alletto, S., Cucchiara, R., Del Fiore, G., & Prati, A. (2016). Re-identification and RTLS for indoor tracking in enterprise spaces. IEEE Sensors Journal, 16(13), 5069–5079.

[7] Anand, P., & Saxena, S. (2018). A comparative evaluation of IoT asset tracking technologies for enterprise environments. Journal of Network and Systems Management, 26(4), 1023–1048.

[8] BABATUNDE, O. A., ADERIBIGBE, S. A., JAJA, I. C., BABATUNDE, O. O., ADEWOYE, K. R., DUROWADE, K. A., & ADETOKUNBO, S. (2014). Sexual activities and practice of abortion among public secondary school students in Ilorin, Kwara State, Nigeria. International Journal of Science, Environment and Technology, 3(4), 1472-1479.

[9] Barrett, R., & Kraus, M. (2014). Leveraging CMDB-integrated ITSM platforms for unified asset governance. Journal of Information Technology Management, 25(3), 45–58.

[10] Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Warkentin, M. (2015). Workplace security fatigue and device carelessness. Computers & Security, 48, 1–15.

[11] Bukhari, T.T., Oladimeji, O., Etim, E.D. & Ajayi, J.O., 2018. A Conceptual Framework for Designing Resilient Multi-Cloud Networks Ensuring Security, Scalability, and Reliability Across Infrastructures. IRE Journals, 1(8), pp.164-173. DOI: 10.34256/irevol1818

[12] Carroll, T., Richardson, S., & Hayes, B. (2015). Evaluating RFID, RTLS, and BLE tracking platforms for industrial asset visibility. IEEE Transactions on Industrial Informatics, 11(4), 940–948.

[13] Chen, L., Li, X., & Li, Z. (2016). An improved barcode-based item tracking framework for mobile enterprise environments. International Journal of Distributed Sensor Networks, 12(11), 1–12.

[14] Durowade, K. A., Adetokunbo, S., &Ibirongbe, D. E. (2016). Healthcare delivery in a frail economy: Challenges and way forward. Savannah Journal of Medical Research and Practice, 5(1), 1-8.

[15] Durowade, K. A., Babatunde, O. A., Omokanye, L. O., Elegbede, O. E., Ayodele, L. M., Adewoye, K. R., ... & Olaniyan, T. O. (2017). Early sexual debut: prevalence and risk factors among secondary school students in Ido-ekiti, Ekiti state, South-West Nigeria. African health sciences, 17(3), 614-622.

[16] Durowade, K. A., Omokanye, L. O., Elegbede, O. E., Adetokunbo, S., Olomofe, C. O., Ajiboye, A. D., ... & Sanni, T. A. (2017). Barriers to contraceptive uptake among women of reproductive age in a semi-urban community of Ekiti State, Southwest Nigeria. Ethiopian journal of health sciences, 27(2), 121-128.

[17] Durowade, K. A., Salaudeen, A. G., Akande, T. M., Musa, O. I., Bolarinwa, O. A., Olokoba, L. B., ... & Adetokunbo, S. (2018). Traditional eye medication: A rural-urban comparison of use and association with glaucoma among adults in Ilorin-west Local Government Area, North-Central Nigeria. Journal of Community Medicine and Primary Health Care, 30(1), 86-98.

[18] Erigha, E. D., Ayo, F. E., Dada, O. O., & Folorunso, O. (2017). INTRUSION DETECTION SYSTEM BASED ON SUPPORT VECTOR MACHINES AND THE TWO-PHASE BAT ALGORITHM. Journal of Information System Security, 13(3).

[19] Farid, Z., Nordin, R., & Ismail, M. (2015). Recent advances in indoor geolocation systems and technologies. Journal of Computer Networks and Communications, 2015, 1–12.

[20] Few, S. (2015). Data visualization for meaningful business dashboards. Analytics Press.

[21] Gartner. (2016). IT asset management modernization: Trends shaping the digital enterprise.

[22] Gholami, V., & Shafiee, M. (2016). Predictive analytics for equipment failure in large organizations. Reliability Engineering & System Safety, 152, 229–238.

[23] Greenwood, T., & Tesch, D. (2018). Cybersecurity risk assessment for mobile IT assets. MIS Quarterly Executive, 17(4), 289–307.

[24] Harris, K., & Davenport, T. (2014). Manual data entry risks in enterprise information systems. MIS Quarterly Executive, 13(3), 145–159.

[25] Haworth, D., & Ramaswamy, S. (2015). The evolution of IT asset lifecycle governance in large enterprises. Information Systems Management, 32(4), 295–308.

[26] Hodge, V., & Austin, J. (2018). A survey of outlier detection methodologies. Artificial Intelligence Review, 49(1), 1–45.

[27] Jin, J., Gubbi, J., Marusic, S., &Palaniswami, M. (2014). An information framework for creating a smart city through IoT. IEEE Internet of Things Journal, 1(2), 112–121.

[28] Johnson, D., & Buckley, P. (2018). An analysis of device loss within mobile-enabled enterprises. Journal of Information Security Research, 9(1), 22–35.

[29] Kang, D., Kim, J., & Lee, J. (2018). Enterprise endpoint monitoring platforms for IT asset compliance. Computers & Security, 78, 315–327.

[30] Keller, A., & König, C. (2018). Digital transformation and IT asset visibility: A systematic review. Journal of Enterprise Information Management, 31(6), 871–891.

[31] Kim, S., & Lee, J. (2017). Data governance strategies for enterprise analytics platforms. Information Systems Frontiers, 19(6), 1353–1367.

[32] Kim, S., & Park, H. (2017). IT audit alignment with regulatory requirements in asset management. Information Systems Control Journal, 45(3), 21–30.

[33] Kulkarni, S., & Dawkins, J. (2017). Location-based risk prediction using temporal mobility models. IEEE Transactions on Systems, Man, and Cybernetics, 47(9), 2496–2508.

[34] Kwon, D., et al. (2017). Deep learning approaches for anomaly detection in cyber-physical logs. IEEE Access, 5, 16976–16985.

[35] Luo, R. C., Hsiao, T., & Chang, C. C. (2018). Multi-sensor fusion for indoor real-time location tracking. IEEE Transactions on Industrial Electronics, 65(8), 6401–6409.

[36] Mell, P., & Kent, K. (2014). Guide to Computer Security Log Management. NIST Special Publication.

[37] Menson, W. N. A., Olawepo, J. O., Bruno, T., Gbadamosi, S. O., Nalda, N. F., Anyebe, V., ... &Ezeanolue, E. E. (2018). Reliability of self-reported Mobile phone ownership in rural north-Central Nigeria: cross-sectional study. JMIR mHealth and uHealth, 6(3), e8760.

[38] Mishra, A., & Tripathi, R. (2017). Automated ITSM workflows: A framework for intelligent service operations. International Journal of Information Management, 37(5), 463–472.

[39] Morrison, J., & Eriksen, T. (2014). Visual analytics frameworks for operational intelligence. Decision Support Systems, 59, 41–51.

[40] Nsa, B., Anyebe, V., Dimkpa, C., Aboki, D., Egbule, D., Useni, S., &Eneogu, R. (2018). Impact of active case finding of tuberculosis among prisoners using the WOW truck in North Central Nigeria. The International Journal of Tuberculosis and Lung Disease, 22(11), S444.

[41] Olamoyegun, M., David, A., Akinlade, A., Gbadegesin, B., Aransiola, C., Olopade, R., ... & Adetokunbo, S. (2015, October). Assessment of the relationship between obesity indices and lipid parameters among Nigerians with hypertension. In Endocrine Abstracts (Vol. 38). Bioscientifica.

[42] Olasehinde, O. (2018). Stock price prediction system using long short-term memory. In BlackInAI Workshop@ NeurIPS (Vol. 2018).

[43] Osabuohien, F. O. (2017). Review of the environmental impact of polymer degradation. Communication in Physical Sciences, 2(1).

[44] Patel, J., & Sharma, V. (2014). Enterprise IT governance and infrastructure rationalization. International Journal of Information Management, 34(6), 674–681.

[45] Patton, M. Q., & McMahon, J. (2014). Behavioral risks in organizational device handling. Journal of Workplace Studies, 29(3), 211–230.

[46] Pervez, H., Iqbal, M., & Ahmed, N. (2017). A performance comparison of indoor tracking technologies for secure enterprise mobility. Sensors, 17(11), 1–15.

[47] Redman, T. (2016). The problem of dirty data in organizational systems. Harvard Business Review, 94(6), 84–92.

[48] Rezaeian, A., & Khosrow-Pour, M. (2017). Weaknesses of non-automated IT inventory systems. International Journal of Enterprise Information Systems, 13(4), 1–15.

[49] Roy, S., & Mishra, A. (2015). Risk-scoring frameworks for classifying high-risk operational assets. Journal of Operational Risk, 10(1), 1–18.

[50] Santos, G., & Oliveira, M. (2016). Machine-learning approaches for detecting anomalous activities in enterprise systems. Expert Systems with Applications, 63, 143–156.

[51] Scholten, J., Eneogu, R., Ogbudebe, C., Nsa, B., Anozie, I., Anyebe, V., ... & Mitchell, E. (2018). Ending the TB epidemic: role of active TB case finding using mobile units for early diagnosis of tuberculosis in Nigeria. The international Union Against Tuberculosis and Lung Disease, 11, 22.

[52] Shin, S., & Lee, J. (2018). Enhancing enterprise mobility using RFID–GPS hybrid asset tracking systems. Journal of Network and Computer Applications, 109, 76–88.

[53] Shmueli, G., &Lichtendahl, K. (2018). Forecasting strategies for organizational risk modeling. International Journal of Forecasting, 34(2), 263–279.

[54] Shukla, N., & Matteson, D. (2015). Real-time data fusion models for enterprise operational intelligence. Decision Support Systems, 78, 120–131.

[55] Solomon, M., & Kim, J. (2016). Compliance frameworks and digital asset traceability. Journal of Cybersecurity, 3(2), 66–78.

[56] Solomon, O., Odu, O., Amu, E., Solomon, O. A., Bamidele, J. O., Emmanuel, E., &Parakoyi, B. D. (2018). Prevalence and risk factors of acute respiratory infection among under fives in rural communities of Ekiti State, Nigeria. Global Journal of Medicine and Public Health, 7(1), 1-12.

[57] Sun, Y., Liu, Z., & Peng, M. (2017). A location-intelligence framework for enterprise asset monitoring systems. Sensors, 17(10), 1–15.

[58] Taylor, J., &Vithayathil, J. (2018). Limitations of spreadsheet-based asset management. Journal of Information Technology Management, 29(2), 45–59.

[59] Wamba, S. F., & Queiroz, M. (2016). Industry 4.0 and IoT tracking systems: A comparative study of adoption readiness. International Journal of Production Economics, 182, 247–259.

[60] Wilson, T., & O'Leary, A. (2017). Portable device vulnerabilities in hybrid work environments. Information & Computer Security, 25(4), 516–531.

[61] YETUNDE, R. O., ONYELUCHEYA, O. P., & DAKO, O. F. (2018). Integrating Financial Reporting Standards into Agricultural Extension Enterprises: A Case for Sustainable Rural Finance Systems.

[62] Yigitbasioglu, O., & Velcu, O. (2018). Designing dashboard KPIs for managerial decision-making. International Journal of Accounting Information Systems, 28, 29–45.

[63] Zhang, H., Tang, J., & Li, S. (2016). Integrating asset lifecycle analytics with configuration management databases. Information Systems Frontiers, 18(6), 1225–1238.

[64] Zhang, Y., & Zhao, L. (2018). Integrating heterogeneous data streams for enterprise IoT management. Sensors, 18(10), 3562.

[65] Zhong, C., &Arisona, S. (2015). Detecting irregular movement patterns using spatiotemporal analytics. Computers, Environment and Urban Systems, 54, 1–14.

[66] Zhou, M., & Fei, X. (2017). Real-time system monitoring through interactive visualization. Information Visualization, 16(4), 283–298.