
Safety and Security Challenges of RFID, IoT and Machine Learning in Smart Supply Chain Management Systems

Dr. Vikas Kumar

Head & Ass. Professor, Deptt. of Mathematics,
L.R. (P.G.) College, Sahibabad Ghaziabad, UP, India 201005

Dr Kalpana

Assistant professor

L. R. (PG) College
Sahibabad Ghaziabad

Mr. Lokesh Kumar

Research Scholar,

Deptt. of Mathematics,

L.R.(P.G.) College, Sahibabad Ghaziabad,

Abstract

Radio Frequency Identification (RFID), the Internet of Things (IoT) and machine learning (ML) are increasingly combined in smart supply chains to support automatic identification, real-time sensing, traceability, anomaly detection and predictive decision-making. RFID links physical goods to digital records. IoT extends this capability through connected readers, gateways, sensors, edge devices and cloud platforms. ML then analyzes the resulting event streams to identify unusual behavior, forecast operational conditions and support security monitoring. This integration also expands the attack surface. RFID tags remain exposed to unauthorized scanning, eavesdropping, cloning, replay attacks and physical tampering. IoT devices and gateways introduce risks involving weak credentials, insecure interfaces, vulnerable firmware, cloud misconfiguration and compromised communication channels. ML creates additional concerns including poor data quality, data poisoning, model drift, adversarial manipulation, false alarms and opaque automated decisions. This paper analyzes these interconnected safety and security challenges and proposes a defense-in-depth approach covering tag security, IoT device management, network protection, application controls, data governance, ML lifecycle assurance and partner governance. Existing analytical risk and control tables are retained, while an additional data-feature table defines RFID and IoT variables that can support ML-based anomaly detection. The study concludes that smart supply chains require security-by-design, privacy-by-design and model governance across the complete RFID-IoT-ML architecture rather than isolated controls at the tag level.

Keywords: RFID technology, Internet of Things, machine learning, smart supply chain, supply chain security, cybersecurity, anomaly detection, traceability, authentication, data privacy

1. Introduction

Smart supply chain management increasingly depends on connected technologies that identify goods, sense operating conditions and coordinate decisions across factories, warehouses, vehicles, distribution centers, retail sites and after-sales services. RFID remains a core identification

technology because tags can be read without direct line of sight and multiple items can be captured quickly. When RFID readers are connected to IoT gateways, environmental sensors, enterprise platforms and cloud services, the supply chain becomes a continuous cyber-physical data environment rather than a stand-alone identification system. Tan and Sidhu (2022) describe this RFID-IoT integration as an important step toward automated sensing, interoperability and ubiquitous data access in supply chain operations.

RFID improves traceability by linking a physical item to a digital identifier and a sequence of business events. A tagged product can be observed during production, receipt, storage, picking, loading, transport, delivery and retail. IoT sensors can add temperature, humidity, vibration, location or equipment-status data to these events. Warehouse management systems, enterprise resource planning systems and logistics platforms can then combine identity and sensor data for operational control. GS1 identification standards and EPCIS support standardized event exchange between trading partners, which is important when traceability data move across organizational boundaries.

The integration of RFID with IoT and ML also increases security dependency. A threat actor may target the radio link, an RFID reader, an IoT gateway, an application programming interface, a cloud service, a database or the data used to train an ML model. A compromised reader can generate false events at scale. A vulnerable IoT gateway can expose multiple downstream devices. Poor-quality or manipulated data can cause an ML model to miss genuine anomalies or generate excessive false alarms. Moustafa et al. (2023) and Rafique et al. (2024) show that intelligent intrusion detection can strengthen IoT security, but they also emphasize the importance of dataset quality, explainability, scalability and real-time evaluation.

This paper analyzes the principal safety and security challenges associated with RFID, IoT and ML in smart supply chain management. The analysis covers confidentiality, integrity, availability, authenticity, privacy, operational safety and resilience. It also evaluates controls for tags, readers, IoT devices, networks, cloud services, data pipelines and ML models. Emerging mechanisms such as blockchain, physically unclonable functions, edge analytics and zero-trust architecture are considered as supporting technologies rather than substitutes for fundamental cybersecurity controls.

2. RFID, IoT and Machine Learning in Smart Supply Chain Management

RFID tags can be classified by power source and communication capability. Passive tags do not contain a battery and draw energy from the reader's electromagnetic field. Active tags use an internal power source and can support longer communication ranges or additional sensing. Passive ultra-high-frequency RFID is widely used for item, case, pallet and asset identification because of its low unit cost and suitability for rapid reading. ISO/IEC 18000-63:2021 specifies the air interface for RFID devices operating in the 860-960 MHz band used for item management and provides an interoperability basis for compatible tags and readers.

In an integrated smart supply chain, RFID functions as the identity layer within a wider IoT architecture. A reader captures tag observations and sends them to middleware or an edge gateway. The middleware removes duplicate reads, associates identifiers with location and time, validates events and forwards them to enterprise applications. IoT gateways may also aggregate sensor measurements, device-health information and network telemetry. Cloud or enterprise systems then combine these streams with inventory, order, transport and supplier data. This layered architecture improves visibility but expands the security boundary from the tag-reader radio link to devices, gateways, networks, APIs, cloud services and business applications.

2.1 IoT integration and real-time sensing

IoT extends RFID by collecting continuous operational and environmental data from connected sensors and equipment. Typical variables include temperature, humidity, vibration, GPS position, door status, reader health, network status and vehicle conditions. These data can be joined with RFID identity events through shared timestamps, asset identifiers and location references. In cold-chain logistics, for example, real-time IoT monitoring can detect abnormal temperature behavior before product quality is lost. Gillespie et al. (2023) demonstrated a real-time IoT anomaly-detection approach for cold-chain transportation, illustrating how continuous sensing can support both operational response and risk reduction. IoT integration therefore improves situational awareness, but it also creates dependencies on device identity, secure communication, firmware maintenance, gateway security and cloud availability.

2.2 Machine learning and data analytics

ML converts high-volume RFID and IoT event streams into predictive or anomaly-detection outputs. Security models can learn normal patterns of tag reads, reader activity, device traffic, route progression and authentication behavior. Operational models can support demand forecasting, inventory optimization and disruption detection. Ashraf, Eltawil and Ali (2024) combined a deep autoencoder with a one-class support vector machine for disruption detection in a cognitive digital supply chain twin and used recurrent models to identify disrupted echelons and estimate time to recovery. Tang and Zha (2026) also reported strong predictive performance from an IoT-ML logistics framework, including 96.5% accuracy and a 97.8% F1-score in their experimental setting. These figures are study-specific and should not be treated as expected performance for every supply chain. Model quality depends on representative data, correct labels, stable features and continuous validation.

3. Major Safety and Security Challenges

3.1 Unauthorized scanning and eavesdropping

RFID tags may respond to radio-frequency interrogation whenever they are within range of a compatible reader. If access restrictions are weak, an unauthorized party can attempt to inventory nearby tags or collect identifiers without the asset owner's knowledge. Eavesdropping involves

passive interception of communication between tags and readers. These attacks can reveal identifiers, product categories, shipment patterns or operating activity. In competitive supply chains, illicit inventorying can expose stock levels and replenishment behavior. Privacy risks also arise when persistent identifiers can be linked to employees, consumers or locations.

3.2 Tag cloning, counterfeiting and substitution

Tag cloning occurs when information from a legitimate RFID tag is copied to another tag or emulated by an unauthorized device. If a supply chain treats possession of a valid identifier as proof of authenticity, a cloned identifier can support counterfeiting. This risk is significant in pharmaceutical, medical-device, aerospace, luxury-goods, food and electronic-component supply chains. Physical substitution creates a related problem because a genuine tag can be removed from one object and attached to another. Cryptographic challenge-response protocols, tamper-evident placement and verification against expected product history can reduce these risks.

3.3 Spoofing, impersonation and replay attacks

Spoofing occurs when an attacker impersonates an authorized tag, reader, service or user. A malicious reader may interrogate valid tags while a malicious tag can provide fabricated data to a legitimate reader. Replay attacks reuse messages captured during an earlier valid interaction. Systems based on static identifiers or reusable authentication messages are more exposed. Mutual authentication, random challenges, session-specific values, counters and secure key management can improve message freshness and reduce replay risk. Resource-constrained tag designs remain a challenge because strong cryptographic functions must operate with limited memory and processing capacity.

3.4 Denial-of-service and radio-frequency interference

RFID availability can be disrupted through radio-frequency jamming, repeated queries, false-read generation, reader damage, middleware attacks or network flooding. Non-malicious interference from metal, liquids, electromagnetic sources, tag collisions or poor reader placement can produce similar operational effects. Loss of reliable reads can delay receiving, stock verification, picking and shipping. Resilience therefore requires both cybersecurity measures and engineering controls such as site surveys, backup readers, radio-frequency monitoring, fallback procedures and tested business-continuity arrangements.

3.5 Physical tampering and environmental safety

RFID operates in physical environments where tags and readers can be removed, replaced, damaged, covered or exposed to moisture, temperature extremes, chemicals, vibration and impact. A damaged tag can produce missing or incorrect stock records even when no cyberattack has occurred. In safety-critical supply chains, false traceability can affect product release, recall execution and regulatory evidence. Controls should therefore include appropriate tag selection, secure placement, tamper-evident features, environmental qualification, protected reader

locations, maintenance schedules and regular reconciliation between physical inventory and digital records.

3.6 Reader, middleware and backend compromise

RFID readers commonly use embedded operating systems, network services, management interfaces and wired or wireless connections. Default credentials, outdated firmware, exposed services or insecure remote administration can provide an entry point to the wider supply chain network. Middleware and backend platforms are especially important because they aggregate events from many readers. A compromised service can inject false events, suppress legitimate reads or change product-location relationships. Readers and middleware should therefore be managed as enterprise endpoints through hardening, patching, authentication, segmentation, encrypted communication, logging and centralized monitoring.

3.7 Privacy, insider and third-party risks

A smart supply chain spans manufacturers, logistics providers, distributors, retailers, cloud vendors, service providers and regulators. Different organizations may access different parts of RFID and IoT data. Privacy problems arise when data are collected beyond a defined business purpose or retained longer than necessary. Insider misuse can involve excessive privileges, shared accounts, unauthorized exports or deliberate record falsification. Weak third-party controls can bypass strong internal safeguards. Least privilege, role-based access control, supplier assurance, audit logging, data minimization, retention limits and rapid access revocation are therefore essential governance measures.

3.8 IoT device, gateway and cloud risks

IoT integration creates attack paths beyond RFID readers. Sensors and gateways may use weak credentials, insecure web interfaces, exposed management ports or outdated firmware. A compromised gateway can alter sensor values, redirect traffic or impersonate multiple devices. Cloud risks include excessive permissions, insecure APIs, exposed storage and poor tenant configuration. Because RFID identity events and IoT sensor measurements are often combined, compromise of one layer can undermine the credibility of the complete traceability record. Strong device identity, secure onboarding, signed firmware, protected update mechanisms, certificate management, API security and segmented communication paths are required to reduce this exposure.

3.9 Machine-learning data and model risks

ML introduces risks that are different from conventional network attacks. Training data can be incomplete, mislabeled, biased or deliberately poisoned. Attackers may manipulate features so that malicious behavior resembles normal activity. Model drift can occur when supply chain processes change, making previously learned patterns less accurate. Excessive false positives can overwhelm operators while false negatives can allow real attacks or operational failures to pass unnoticed.

Sensitive training data may also be exposed through weak access controls or model interfaces. ML security therefore requires protected data provenance, validation checks, drift monitoring, adversarial testing, controlled retraining, explainable outputs and human review for high-impact decisions.

Table 1. Analytical risk assessment of major RFID threats in smart supply chains

Threat	Likelihood (1-5)	Impact (1-5)	Risk score	Risk level
Unauthorized scanning / eavesdropping	5	4	20	Very high
Tag cloning / counterfeiting	4	5	20	Very high
Reader spoofing / impersonation	4	4	16	High
Replay attacks	3	4	12	Moderate
Denial-of-service / RF jamming	3	4	12	Moderate
Physical tag tampering	4	4	16	High
Reader / middleware compromise	4	5	20	Very high
Backend database manipulation	3	5	15	High
Privacy / unauthorized tracking	4	4	16	High
Insider / third-party misuse	4	5	20	Very high

Note. Scores are an author-developed analytical synthesis for this paper and are not observed attack frequencies. Likelihood and impact use a 1 (low) to 5 (very high) scale. Risk score = likelihood x impact. IoT and ML risks are discussed separately in Sections 3.8 and 3.9 because the existing figure visualizes the core RFID threat set.

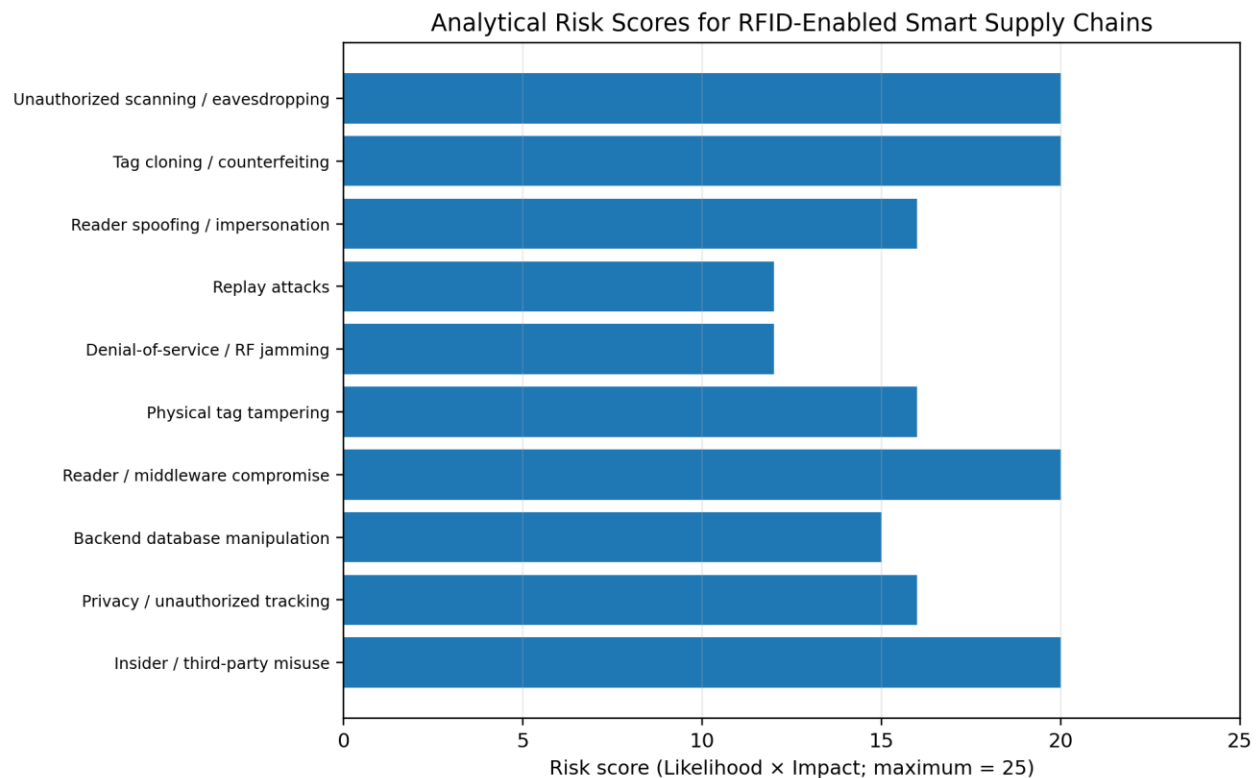


Figure 1. Comparative analytical risk scores for core RFID security threats.

4. Security Controls and Risk-Mitigation Strategies

Security for an RFID-IoT supply chain should follow defense-in-depth rather than rely on a single mechanism. Mutual authentication between tags and authorized readers can reduce impersonation. Lightweight cryptography can protect message confidentiality and integrity where tag resources permit it. Authentication protocols should include freshness controls that resist replay attacks and unauthorized tracking. Cryptographic keys require secure generation, storage, distribution, rotation, revocation and replacement because strong algorithms provide little protection when secret keys are exposed. Recent RFID-IIoT research also continues to emphasize lightweight mutual authentication for resource-constrained supply chain devices (Kumar & Das, 2025).

IoT devices and RFID readers should be treated as managed endpoints. Organizations should change default credentials, disable unnecessary services, maintain an accurate device inventory, restrict management interfaces and apply signed firmware updates through controlled processes. Gateways should authenticate connected devices before accepting data. Reader-to-gateway, gateway-to-cloud and middleware-to-application communication should use authenticated encryption where technically feasible. Network segmentation, firewalls and controlled gateways can limit lateral movement if one device is compromised. A security information and event management platform can correlate device logs, network events, authentication failures and

unusual traffic for faster detection.

Data and application controls are equally important. Role-based access control and least privilege should govern who can read, write, export or administer RFID and IoT data. Integrity checks, protected audit logs, backups, transaction validation and separation of duties reduce the risk of unauthorized modification. ML pipelines need additional controls. Training and validation datasets should have documented provenance, access restrictions and quality checks. Production models should be versioned and monitored for drift, false-positive rates, false-negative rates and changes in feature distributions. Explainable outputs can support analyst review when automated detection affects product release, shipment decisions or incident escalation (Moustafa et al., 2023).

Supply chain governance must extend to external partners. Security requirements should be written into contracts and integration interfaces should be tested before production use. High-risk partners should undergo periodic assurance reviews. Incident-response procedures should define actions for cloned tags, compromised readers, suspicious IoT devices, corrupted sensor data, ML model degradation, missing traceability events and radio-frequency outages. NIST RFID guidance emphasizes lifecycle security from requirements and architecture through operation, maintenance and retirement. The same lifecycle principle should be applied to IoT devices and ML models so that security remains effective as systems, data and business processes change.

Table 2. Comparative evaluation of core RFID security controls

Security control	Effectiveness (1-5)	Complexity (1-5)	Priority
Mutual tag-reader authentication	5	3	Critical
Encrypted reader-backend links	5	3	Critical
Cryptographic key management	5	4	High
Reader hardening / patching	4	3	High
Network segmentation	5	3	Critical
Role-based access control	5	2	Critical
Security monitoring / anomaly detection	4	3	High
Tamper-evident tag placement	3	2	Supporting
Privacy / data minimization controls	4	3	High
Supplier and partner security governance	4	3	High

Note. Effectiveness and implementation complexity are author-developed comparative scores based on the security functions described in the reviewed literature and standards. They are intended for prioritization and are not empirical performance measurements. IoT device assurance and ML model governance are discussed in the surrounding text because Figure 2 represents the original core control set.

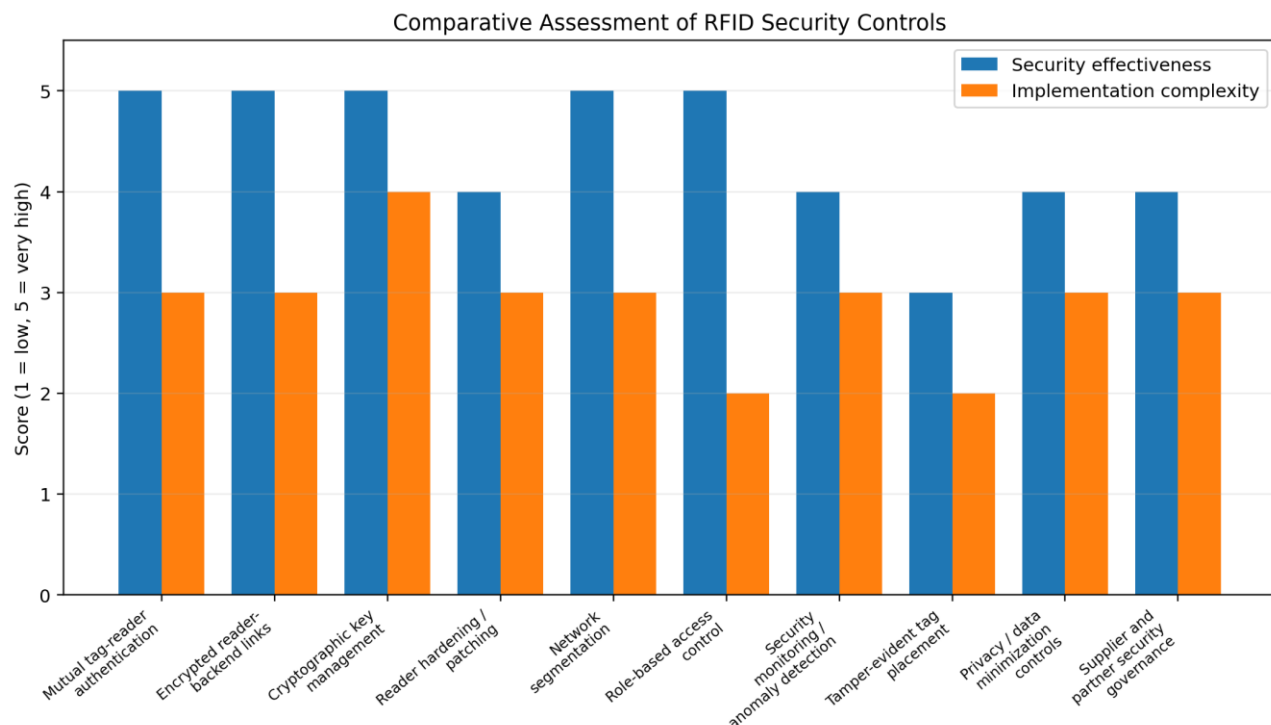


Figure 2. Comparative effectiveness and implementation complexity of core RFID security controls.

5. IoT and ML-Enabled Security and Emerging Technologies

Emerging technologies can strengthen RFID-IoT supply chains when they are added to a sound security baseline. Permissioned blockchain systems can provide tamper-evident sharing of selected traceability events across organizations. This can improve accountability because later modification of a validated event becomes more difficult. However, blockchain does not prove that the original physical observation was correct. A cloned tag, compromised reader or manipulated IoT sensor can still submit false data to an immutable ledger. The design problem therefore remains one of trusted data capture as well as trusted storage.

Physically unclonable functions (PUFs) provide another mechanism for strengthening device or tag identity. They use small manufacturing variations to generate device-specific responses that are harder to reproduce than static memory values. PUF-based authentication can improve resistance to physical cloning when enrollment, challenge-response design and lifecycle management are secure. Edge computing can also improve IoT security by filtering data close to

readers and sensors, reducing unnecessary cloud exposure and enabling low-latency anomaly detection. Edge nodes still require hardening, trusted software and secure update mechanisms because compromise at the edge can affect many connected devices.

ML can improve anomaly detection by learning normal patterns in tag reads, device communication, inventory movement, reader locations, shipment timing and sensor measurements. For IoT intrusion detection, Saran and Kesswani (2023) evaluated several supervised classifiers on the MQTT-IoT-IDS2020 dataset and reported 99.98% accuracy for both Random Forest and Decision Tree models. This demonstrates the potential of ML for IoT security, but the result is dataset-specific and does not remove the need for validation on local traffic. Broader reviews also identify important limitations involving class imbalance, data drift, real-time scalability, explainability and generalization to unseen attacks (Adhikari et al., 2024; Rafique et al., 2024).

5.1 RFID-IoT data for ML-based monitoring

A practical ML security pipeline needs structured data that connect the identity layer to the sensing and network layers. The most useful features are not limited to the Electronic Product Code. Time, location, reader identity, signal quality, read frequency, environmental measurements, authentication events and process duration can all provide context for distinguishing normal operations from suspicious behavior. Table 3 defines a compact data structure that can be generated from RFID readers, IoT gateways, sensors and enterprise applications. The table is a proposed analytical design for this paper rather than a collected dataset. Organizations should minimize personal data, apply retention limits and remove unnecessary identifiers before using these records for model training.

Table 3. Proposed RFID-IoT data features for ML-based supply chain monitoring

Data feature	Primary source	Example representation	ML and security use
EPC or tag identifier	RFID tag and reader	Categorical identifier	Links events to an asset and supports duplicate, cloning or impossible-movement checks.
Reader or gateway ID	RFID reader / IoT gateway	Device identifier	Detects unusual device behavior, unauthorized readers and location inconsistencies.
Timestamp and read rate	Reader middleware	Date-time; reads per minute	Supports replay detection, burst analysis, dwell-time analysis and sequence modeling.
RSSI or read quality	RFID reader	Numeric signal value	Helps identify abnormal proximity, poor reads, interference or unexpected reader-tag relationships.

Data feature	Primary source	Example representation	ML and security use
Location or route point	Reader, GPS or WMS	Zone, coordinates or route code	Supports geofencing, route-deviation detection and impossible travel analysis.
Temperature and humidity	IoT environmental sensor	Numeric sensor values	Detects cold-chain excursions, sensor faults and product-safety anomalies.
Authentication failures	Reader, gateway or IAM log	Count per time window	Supports intrusion detection, credential-abuse detection and device-compromise alerts.
Network telemetry	IoT gateway / firewall	Bytes, packets, ports, protocol	Supports ML-based detection of scanning, flooding, command-and-control or unusual traffic.
Dwell or transit time	RFID events plus logistics system	Minutes or hours	Identifies unexpected delay, diversion, theft risk or process disruption.
Outcome or anomaly label	SOC / operations review	Normal, attack, fault, disruption	Provides supervised-learning targets and supports evaluation of precision, recall and F1-score.

Note. Table 3 is a proposed data schema for analytical and implementation planning. It does not represent observed records from a specific company. Feature selection should be adapted to the local RFID frequency, IoT architecture, business process and privacy requirements.

5.2 ML evaluation and operational deployment

ML security performance should be evaluated with more than accuracy because attacks are usually imbalanced and false alarms have operational costs. Precision shows how many alerts classified as malicious are correct. Recall shows how many genuine malicious events are detected. The F1-score balances precision and recall. False-positive rate measures alert burden, while detection latency measures how quickly an anomaly is recognized. Production deployment should also track model drift and feature quality. A model that performs well during development can degrade when new readers are installed, warehouse layouts change, suppliers adopt different devices or seasonal traffic patterns alter event distributions. Continuous monitoring and controlled retraining are therefore part of security operations rather than one-time data-science activities.

6. Discussion

Table 1 shows that the most severe core RFID risks are distributed across several technical and organizational layers. Unauthorized scanning affects confidentiality and commercial privacy.

Cloning affects authenticity. Reader or middleware compromise can affect data integrity at scale. Insider and third-party misuse can bypass technical controls through legitimate access. The addition of IoT does not replace these risks. It adds device, gateway, API and cloud attack paths. The addition of ML creates another dependency because security decisions can be distorted by poor data, drift or deliberate manipulation. The resulting security problem is therefore cyber-physical, data-driven and organizational.

Risk treatment should reflect business impact. Counterfeiting in a pharmaceutical or medical-device supply chain may create direct patient-safety and regulatory consequences. Temporary unreadability in a low-value retail environment may primarily create efficiency losses. An IoT temperature anomaly in a cold chain can indicate product-quality risk. An ML false negative can suppress an alert that operators needed to investigate. Organizations should therefore evaluate product value, safety criticality, privacy sensitivity, reliance on automation, regulatory obligations and the availability of manual fallback procedures before selecting controls.

Table 2 and Figure 2 indicate that foundational controls such as mutual authentication, encrypted backend communication, network segmentation, role-based access control and key management should receive priority before investment in more complex technologies. For an RFID-IoT-ML architecture, these controls should be extended with device inventory, secure onboarding, signed updates, API protection, data provenance, model versioning and drift monitoring. Saran and Kesswani (2025) specifically frame industrial IoT-enabled supply chain security as an analytics problem in which machine-learning-based intrusion detection complements traditional controls. This supports a layered architecture where prevention, detection and response functions reinforce one another.

The proposed Table 3 also shows why data governance is a security requirement. RFID identity events become more useful when combined with time, location, signal quality, sensor measurements and network telemetry. The same enrichment can increase privacy exposure and the consequences of data manipulation. Organizations should therefore document data lineage from the physical observation to the model output. Security teams need to know which reader, gateway, transformation step and model version contributed to an alert. Explainability is particularly important when an automated decision affects shipment release, quarantine, supplier escalation or incident response.

Standards-based design remains important because global supply chains cross company and national boundaries. ISO/IEC 18000-63 supports interoperable UHF RFID communication while GS1 identification and EPCIS standards support consistent identity and event exchange. Interoperability provides economic value only when organizations also align identity management, access control, data protection, incident handling and partner assurance. The practical objective is trustworthy connectivity in which RFID observations, IoT sensor data and ML outputs can support operational and security decisions.

7. Conclusion

RFID, IoT and ML now form a complementary technology stack for smart supply chain management. RFID provides item identity and rapid event capture. IoT adds continuous sensing, device connectivity and real-time operational context. ML analyzes these data streams to detect anomalies, forecast disruptions and support faster decisions. The same integration increases dependency on trustworthy devices, secure communications, accurate data and controlled models. Unauthorized reading, eavesdropping, cloning, impersonation, replay attacks, denial-of-service, physical tampering, reader compromise, middleware manipulation, insecure IoT devices, cloud misconfiguration, privacy violations, insider misuse and third-party weaknesses can reduce trust in the supply chain. ML adds risks involving data poisoning, poor labels, model drift, adversarial manipulation, false alarms and opaque decisions. Effective protection requires a full-stack architecture that combines secure tags, mutual authentication, lightweight cryptography, key management, hardened readers, managed IoT devices, encrypted communication, segmentation, access control, continuous monitoring, data provenance, model governance, physical protection, incident response and supplier assurance. Blockchain, PUFs, edge analytics and zero-trust principles can strengthen selected functions when they are built on this foundation. Future smart supply chains should therefore implement RFID-IoT-ML systems according to security-by-design, privacy-by-design and responsible model-governance principles so that automation does not compromise authenticity, confidentiality, integrity, availability or safety.

References

1. Adhikari, D., Jiang, W., Zhan, J., Rawat, D. B., & Bhattarai, A. (2024). Recent advances in anomaly detection in Internet of Things: Status, challenges, and perspectives. *Computer Science Review*, 54, 100665. <https://doi.org/10.1016/j.cosrev.2024.100665>
2. Ashraf, M., Eltawil, A., & Ali, I. (2024). Disruption detection for a cognitive digital supply chain twin using hybrid deep learning. *Operational Research*, 24, Article 23. <https://doi.org/10.1007/s12351-024-00831-y>
3. Gillespie, J., da Costa, T. P., Cama-Moncunill, X., Cadden, T., Condell, J., Cowderoy, T., Ramsey, E., Murphy, F., Kull, M., Gallagher, R., & Ramanathan, R. (2023). Real-time anomaly detection in cold chain transportation using IoT technology. *Sustainability*, 15(3), 2255. <https://doi.org/10.3390/su15032255>
4. GS1. (2026). EPCIS and Core Business Vocabulary (CBV). GS1 Standards.
5. GS1. (2026). Radio Frequency Identification (RFID) standards and EPC Tag Data Standard. GS1 Standards.
6. International Organization for Standardization & International Electrotechnical Commission. (2021). ISO/IEC 18000-63:2021: Information technology - Radio frequency identification for

- item management - Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C.
7. Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, 24(2), 381-394. <https://doi.org/10.1109/JSAC.2005.861395>
 8. Karygiannis, T., Eydt, B., Barber, G., Bunn, L., & Phillips, T. (2007). Guidelines for securing Radio Frequency Identification (RFID) systems (NIST Special Publication 800-98). National Institute of Standards and Technology.
 9. Kumar, V., & Das, S. K. (2025). Enhancing security in IIoT: RFID authentication protocol for edge computing and blockchain-enabled supply chain. *Cyber Security and Applications*, 3, 100087. <https://doi.org/10.1016/j.csa.2025.100087>
 10. Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., & Tari, Z. (2023). Explainable intrusion detection for cyber defences in the Internet of Things: Opportunities and solutions. *IEEE Communications Surveys & Tutorials*, 25(3), 1775-1807. <https://doi.org/10.1109/COMST.2023.3280465>
 11. Rafique, S. H., Abdallah, A., Musa, N. S., & Murugan, T. (2024). Machine learning and deep learning techniques for Internet of Things network anomaly detection - current research trends. *Sensors*, 24(6), 1968. <https://doi.org/10.3390/s24061968>
 12. Saran, N., & Kesswani, N. (2023). A comparative study of supervised machine learning classifiers for intrusion detection in Internet of Things. *Procedia Computer Science*, 218, 2049-2057. <https://doi.org/10.1016/j.procs.2023.01.181>
 13. Saran, N., & Kesswani, N. (2025). An analytics-driven framework for securing industrial IoT-enabled supply chain management systems. *Supply Chain Analytics*, 11, 100128. <https://doi.org/10.1016/j.sca.2025.100128>
 14. Tajima, M. (2007). Strategic value of RFID in supply chain management. *Journal of Purchasing and Supply Management*, 13(4), 261-273. <https://doi.org/10.1016/j.pursup.2007.11.001>
 15. Tan, W. C., & Sidhu, M. S. (2022). Review of RFID and IoT integration in supply chain management. *Operations Research Perspectives*, 9, 100229. <https://doi.org/10.1016/j.orp.2022.100229>
 16. Tang, Y., & Zha, C. (2026). Application of Internet of Things (IoT) and machine learning (ML) in intelligent logistics supply chain. *Discover Internet of Things*, 6, Article 31. <https://doi.org/10.1007/s43926-026-00282-1>
 17. Unhelkar, B., Joshi, S., Sharma, M., Prakash, S., Mani, A. K., & Prasad, M. (2022). Enhancing supply chain performance using RFID technology and decision support systems in the Industry

- 4.0: A systematic literature review. *International Journal of Information Management Data Insights*, 2(2), 100084. <https://doi.org/10.1016/j.jjime.2022.100084>
18. Varriale, V., Cammarano, A., Michelino, F., & Caputo, M. (2021). Sustainable supply chains with blockchain, IoT and RFID: A simulation on order management. *Sustainability*, 13(11), 6372. <https://doi.org/10.3390/su13116372>