Pertanika J. Sci. & Technol. 34 (5): 2929 - 2945 (2026)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Context-Aware RFID-IoT Counterfeit Prevention: A Simulation-Based Proof of Concept Using Layered RBAC, MAC, ABAC, and ECA

Ravichandran[1]*and Irene Anastasia Patric[2]

[1]Faculty of Computing and Information Technology, University College Fairview, 4178, Jalan 1/27D, Section 6, Wangsa Maju, 53300 Kuala Lumpur, Malaysia
[2]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia

ABSTRACT

Radio Frequency Identification and Internet of Things technologies improve supply chain visibility, but cloned or fraudulent tags can compromise product authenticity, data integrity, and organisational trust. This paper develops an RFID-IoT-based counterfeit-prevention system for supply chain management that uses role-based and attribute-based access control, along with event-condition-action rules. The problem addressed is that a valid tag identifier may be accepted even when its time, reader, location, employee, organisation, or process sequence is suspicious. The proposed system integrates Access Control Policy Tool modelling, static verification, dynamic verification, and policy implementation with movement-context checks based on time-to-live and reader distance. This research used an Excel dataset from a simulated RFID-SCM environment. The cleaned dataset contained 205 labelled records: 188 normal and 17 cloned. Results show that normal records had a stable mean sequence time-to-live of 2.918 minutes, whereas cloned records had a lower mean of 2.826 minutes and higher variation. The study concludes that counterfeit prevention requires verified policy implementation and continuous evaluation of contextual events.

Keywords: Access control policy tool, attribute-based access control, counterfeit prevention, event-condition-action, Internet of Things, radio frequency identification, role-based access control, supply chain management

ARTICLE INFO

Article history:
Received: 30 August 2026
Accepted: 29 September 2026
Published: 30 October 2026

DOI: https://doi.org/10.47836/pjst.34.5.16

ravichandra.ucf@fairview.edu.my (Ravichandran)
gs74911@student.upm.edu.my (Irene Anastasia Patric)
* Corresponding author

INTRODUCTION

Radio Frequency Identification (RFID) is widely used to identify, track, and manage

e-ISSN: 2231-8526

© Universiti Putra Malaysia Press

products across supply-chain processes. A typical deployment includes item tags, readers, and a database or middleware layer that stores Electronic Product Code (EPC), reader, transaction, location, timestamp, and employee information (Derakhshan et al., 2007; Michael & McCathie, 2005; Patric, 2016). In supply chain management (SCM), these components support manufacturing, packaging, distribution, retail receiving, inventory control, audit reporting, and product traceability. This research focuses on RFID-enabled SCM, in which supply-chain data is shared among organisations with different roles, responsibilities, sites, and security policies. This inter-organisational setting creates security risks because a tag read may appear valid while violating the expected context of product movement. Counterfeiting attacks are especially serious because cloned and fraudulent tags can make unauthorised goods appear genuine. RFID-SCM security research has therefore treated tag cloning, fraud, eavesdropping, skimming, man-in-the-middle attacks, and physical attacks as important threats to authenticity and trust (Mahinderjit-Singh & Li, 2010). Recent literature from 2020 to 2025 reinforces this need for context-aware RFID-IoT security.

EPCIS 2.0 standardisation supports interoperable supply-chain event visibility (GS1, 2022). Zero-trust architecture holds that access should be continuously evaluated rather than implicitly trusted (Rose et al., 2020). Blockchain-based supply-chain studies emphasise tamper resistance and traceability across organisational boundaries (Kouhizadeh et al., 2021). RFID clone-detection research has shifted towards spatiotemporal, distance-aware, and probabilistic evidence, as cloned tags can reuse legitimate identifiers (Huang et al., 2020; Mustaffa et al., 2024). High-impact traceability studies show that transparent provenance records can reduce the risk of manipulation, single points of failure, and information asymmetry (Kamble et al., 2020; Sunny et al., 2020). Recent studies in pharmaceutical and industrial supply chains further connect anti-counterfeit traceability to blockchain, edge computing, and RFID authentication (Kumar & Das, 2025; Nawaz et al., 2024). European cyber-threat reporting also shows that supply-chain compromise remains a major cyber-physical and organisational risk (European Union Agency for Cybersecurity, 2023). These studies align with this current research because counterfeit prevention requires policy verification, identity validation, and continuous evaluation of movement context.

Newer work from 2025 to 2026 further supports the direction of this paper. A 2025 RFID clone-detection study reports an efficient method for identifying probabilistic cloning attacks in large-scale RFID systems (Chu et al., 2025). A 2026 traceability review emphasises blockchain, IoT, and AI as important technologies for transparent supply chains (Siyal et al., 2026). A 2026 RFID-blockchain supply chain study also reinforces the need to combine RFID event identity with tamper-resistant provenance to prevent fraud and the movement of counterfeit goods across organisations (Nadime et al., 2026).

Problem Statement

A cloned or fraudulent tag may reuse a legitimate Electronic Product Code (EPC) or be introduced into the process flow because the policy enforcement mechanism fails to consider critical context information. This means that a tag read can be valid in the system even if the time, reader, location, employee role, organisation, or movement sequence associated with it is suspicious. Therefore, the core problem is that relying only on the validity of a tag identity (EPC) does not provide sufficient confidence in product authenticity, data integrity, and organisational trust, leaving the supply chain vulnerable to counterfeit attacks. Thus, the core problem addressed in this research appears to be the inadequacy of static identifier checks in preventing counterfeiting in RFID-enabled supply chains. Further, this study attempts to demonstrate that cloned records are detected through combined contextual evidence rather than by static EPC checking alone.

Research Questions

This study is guided by the following research questions:

1. How can RFID-SCM access requests and tag movements be evaluated using contextual attributes?
2. Which access-control models are suitable for manufacturer, distributor, and retailer environments?
3. How can event-condition-action (ECA) rules and time-to-live (TTL) checks support cloned-tag detection?
4. Which dataset patterns distinguish normal records from cloned records?

MATERIALS AND METHODS

The Proposed Procedure

The proposed procedure is an RFID-IoT-based counterfeit-prevention system for SCM. It combines RFID tag events, IoT-style event collection, Access Control Policy Tool (ACPT) implementation, RBAC, ABAC, and ECA rule evaluation into a single policy decision process.

The policy layer combines RBAC, MAC, ABAC, and ECA logic. RBAC assigns permissions according to organisational roles such as administrator, supervisor, employee, manufacturer, distributor, and retailer. MAC restricts access to sensitive process and transaction files in accordance with mandatory rules. ABAC evaluates richer attributes, including organisation, employee position, workplace, working hours, file ownership, requested action, reader location, and tag movement state (Hu et al., 2014). ECA rules transform RFID anomalies into operational responses.

The proposed ECA logic is represented as:

$E:$ TagRead ($EPC, Reader, Location, Time, Employee$), [1]

$C: \neg ValidContext(EPC, Reader..., TTL, Role)$, [2]

$A: DenyAccess \wedge RaiseAlert \wedge AuditEvent.$ [3]

The ECA logic to be proposed here contains three elements: event (E), condition (C), and action (A), the definition of which is written explicitly in Equations 1 to 3 as follows. Equation [1] defines the event E: TagRead(EPC, Reader, Location, Time, Employee), which includes the attributes of the RFID event that will trigger the policy evaluation. Equation 2 defines the condition C: ¬Valid Context (EPC, Reader..., TTL, Role), where the context attributes EPC, reader, location, TTL, and role of the employee are outside the scope of the policies' definitions. Equation [3] defines the action, A: DenyAccess ∨ RaiseAlert ∨ AuditEvent, to take when the condition holds. A tag read is suspicious if the EPC is duplicate, the reader is out of expected range, the TTL sequence is not according to SCM flow, and the employee role and request action violate the policyA tag read is suspicious when the EPC is duplicated, the reader is outside the expected range, the TTL sequence is inconsistent with SCM flow, or the employee role and requested action do not match policy.

The data for this study were collected from a simulated RFID-SCM environment. The simulator follows the manufacturer–distributor–retiler process flow and generates RFID readings using a Monte Carlo method that repeatedly generates random reader IDs, timestamps, EPC values, and cloned-tag conditions. The resulting Excel dataset was cleaned, labelled, and analysed. The sample prototype screen showing the simulation for three sides, namely, manufacturer, distributor, and retailer, is shown in Figure 1.

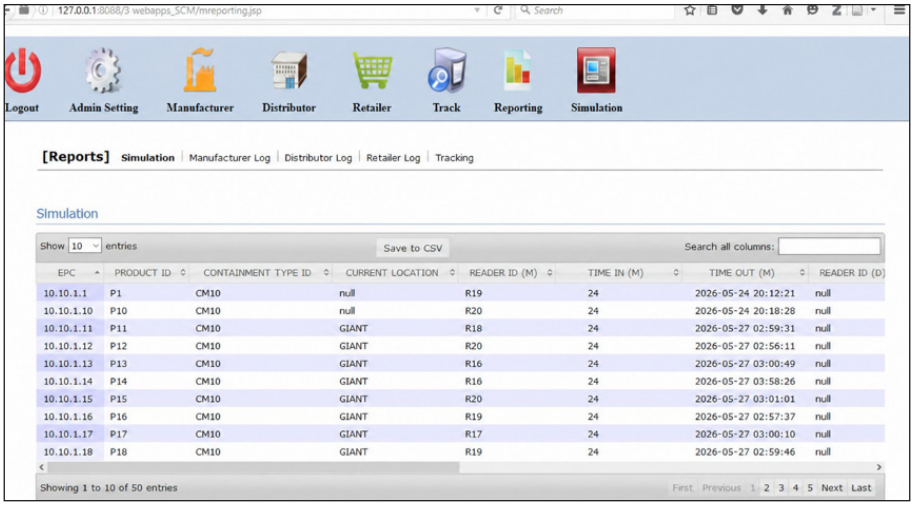

Figure 1. Sample simulation for manufacturer, distributor and retailer

After data cleaning, a total of 205 labelled records were retained for analysis. Table 1 summarises the cleaned dataset, detailing the class distribution and the operational scope covered.ACPT was used to model, verify, test, and implement the access-control policies before evaluation. ACPT is used through four implementation components. First, policy modelling defines subjects, resources, actions, environment attributes, and access rules. Second, static verification checks whether the model satisfies the required properties before deployment. Figure 2 shows the verification process completed by NuSMV in a Java-based graphical tool.

Table 1
ACPT implementation components.

Component	Role in the proposed system
Policy modelling	Defines RBAC, ABAC, and MAC attributes, rules, and decisions.
Static verification	Checks policy properties before execution.
Dynamic verification	Tests request inputs against modelled policy behaviour.
Implementation	Executes and exports policy logic through the Java graphical tool.

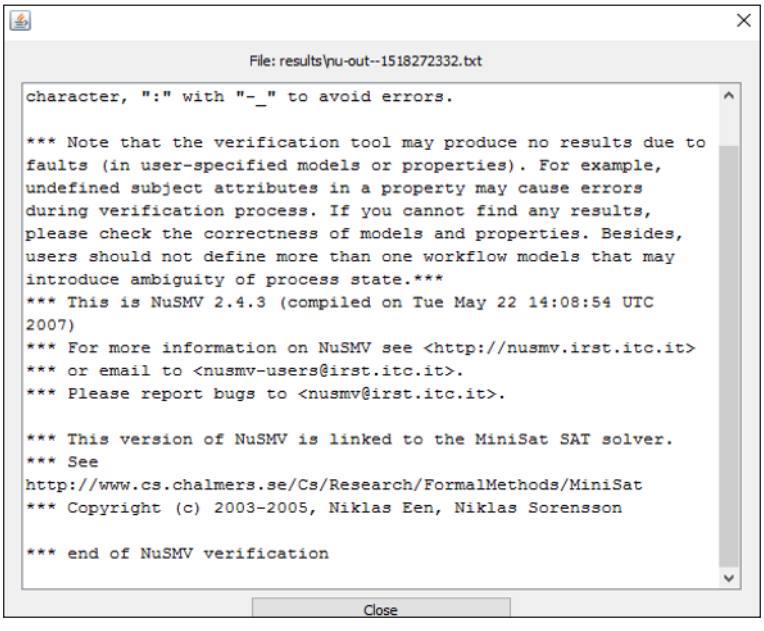

Figure 2. Screen showing how verification is performed using NuSMV

This verification is performed using NuSMV, a symbolic model checker integrated within ACPT. NuSMV translates the modelled RBAC, ABAC, and ECA policies into a

formal specification and performs exhaustive state-space exploration to detect conflicts, rule inconsistencies, or violations of security properties such as separation of duties and least privilege. If a violation is detected, NuSMV generates a counterexample trace for debugging. Third, dynamic verification tests policy behaviour against request inputs. Fourth, policy implementation exports and executes the policy logic through a Java-based graphical tool. In this paper, the ACPT process is linked to RFID event checking so that a tag read is not accepted only because the EPC value exists in the database.The roles of the four ACPT implementation components are summarised in Table 1.

RESEARCH DESIGN AND DATASET

Research Design

The study used a document-and-dataset research design. Literature was used to extract the RFID-SCM background, attack taxonomy, access-control models, ACPT implementation process, and simulator context. The data-flow document was used to reconstruct the manufacturer–distributor–retailer process, while the Excel dataset was parsed to analyse RFID-SCM records.

Data Set Generation

The RFID readings were generated using a Monte Carlo method, in which the reader ID, timestamp, EPC values, and cloned-tag conditions were sampled randomly and repeatedly. Thus, the dataset is a simulation of RFID-SCM readings, not data from a live operational deployment.

Normal records generation: Normal records were generated by simulating tag movements in the manufacturer-distributor-retailer flow. TTL values, reader/writer distances and timestamps were sampled from the expected distributions of operation.

Cloning records: we cloned existing normal records by taking their legitimate EPC and modifying their associated contextual attributes:

1. Timing perturbation: TTL sequence values are shifted to make it inconsistent with expected movement timing.
2. Reader/writer distance perturbation: Distance values were changed from the normal stable range.
3. Site TTL perturbation: Manufacturer site TTL demonstrated increased variance.

Each record was labelled as cloned = Yes or cloned = No based on whether the contextual attributes deviated from the expected policy-defined ranges.

Dataset Structure

After cleaning data, a total of 205 labelled records were used for analysis. Table 2 presents a summary of this cleaned dataset.

Table 2
Cleaned dataset summary.

Measure	Value
Labelled records	205
Normal records	188
Cloned records	17
Cloned proportion	8.29%
Supply-chain stages	Manufacturer, distributor, and retailer
Decision label	Cloned: Yes/No

RFID readings were generated for the simulator using a Monte Carlo method with repeated random generation of reader ID, timestamp, EPC values, and cloned-tag conditions. The dataset, therefore, represents simulated RFID-SCM readings rather than manually entered survey responses. Its fields include tag, location ID, reader, transaction ID, container ID, item ID, manufacturer, distributor, retailer, transport TTL values, reader/writer distance, tag response rate, TTL sequence mean and standard deviation, and the final cloned/not-cloned label. The main dataset variables and their roles are summarised in Table 3.

Table 3
RFID-SCM dataset details

Field group	Definition and role in analysis
Tag/EPC	Electronic Product Code identifying each RFID-tagged item.
Location and reader	Location ID and reader ID showing where the tag was read across the manufacturer, distributor, retailer, and transport stages.
Transaction and item	Transaction ID, container ID, and item ID representing tagging, packaging, shipping, and product movement.
Site TTL	Manufacturer, distributor, and retailer time-to-live values showing how long an item remains at each SCM site.
Transport TTL	Transport A and B timing values showing movement between manufacturer–distributor and distributor–retailer stages.
Reader/writer and response	Read/write distance and tag response rate, including response-rate calculations derived from read/write values.
TTL sequence	Overall sequence TTL combining site TTL and transport TTL.
Statistical measures	Mean and standard deviation values for TTL, sequence, reader/writer, and transport attributes.
Class label	Binary cloned/not-cloned label used to compare normal and counterfeit records.

The access-control variables were grouped into subject, resource, action, environment, movement, and decision attributes. Table 4 presents the attribute categories used to connect policy logic with RFID-SCM observations.

The DFD in Figure 3 represents the operational SCM flow that links authentication, data generation, reader/tag response, TTL processing, clone detection, and audit/reporting.

Table 4
Policy attribute categories

Category	Example attributes
Subject	Organisation, employee position, and authenticated user.
Resource	EPC files, process files, and transaction files.
Action	View, create, update, delete, read, and write.
Environment	Working place, working hours, site, and location ID.
Movement	TTL, sequence TTL, transport TTL, and reader/writer range.
Decision	Allow, deny, alert, audit, and cloned flag.

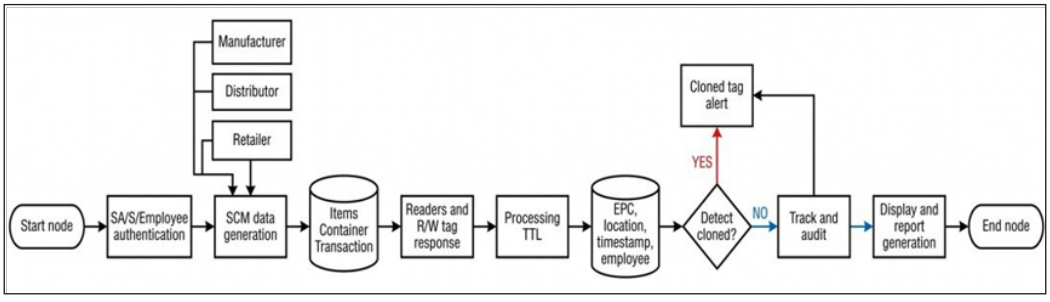

Figure 3. Data-flow diagram for SCM authentication, TTL processing, clone detection, tracking, audit, and report generation

RESULT AND DISCUSSIONS

The dataset analysis calculated class distribution and descriptive statistics for key contextual indicators. Mean, standard deviation, minimum, and maximum values were computed for manufacturer TTL, distributor TTL, retailer TTL, sequence TTL, transport TTL, and reader/writer distance. The cloned and normal classes were then compared to identify indicators that support the proposed counterfeit-prevention procedure. The dataset contained tag, location, reader, transaction, container, item, manufacturer-stage TTL, distributor-stage TTL, retailer-stage TTL, reader/writer distance, transport sequence, and cloned-status fields.

Table 5 shows that the distributor and retailer TTL averages are similar for both normal and cloned records, so the single-stage means alone are insufficient to identify counterfeiting. The stronger signal is dispersion.

Normal records have a highly stable sequence TTL, with a mean of 2.918 minutes and a standard deviation of 0.002 minutes. Cloned records have a lower sequence TTL mean of 2.826 minutes and a standard deviation of 0.388. This indicates that cloned tags are more likely to disrupt the expected timing of movement across the process flow. Reader/writer distance also supports the policy procedure. Normal records have a stable third-stage reader/writer value of 5.75 m, while cloned records vary more strongly. With a mean of 6.147 m and a standard deviation of 1.312 m, this suggests that counterfeit detection should not depend solely on tag identity. A valid-looking EPC must still be checked against

Table 5
Selected statistics by cloned status

Indicator	Normal Mean	Normal SD	Cloned Mean	Cloned SD
Manufacturer site TTL	0.166	0.003	0.176	0.253
Distributor TTL	0.277	0.003	0.276	0.003
Retailer TTL	0.145	0.007	0.145	0.006
Sequence TTL	2.918	0.002	2.826	0.388
Reader/writer distance	5.750	0.000	6.147	1.312

Note. The large difference in standard deviation for the manufacturer stage (0.003 normal vs 0.253 cloned) is a designed cloning signature from the site TTL perturbation step and not a measurement artefact

Table 6
Confusion matrix showing classification outcomes (TP, TN, FP, FN).

	Predicted Normal	Predicted Cloned
Actual Normal	186 (TN)	2 (FP)
Actual Cloned	3 (FN)	14 (TP)

Table 7
Detection performance metrics with 95% confidence intervals.

Metric	Value (%)	95% Confidence Interval
Accuracy	97.56	94.42 – 99.18
Precision	87.50	61.65 – 98.45
Recall (Sensitivity)	82.35	56.57 – 96.20
F1-score	84.85	61.92 – 95.11
Specificity	98.94	96.22 – 99.87

*Note.*Accuracy = 97.56%, Precision = 87.50%, Recall = 82.35%, F1-score = 84.85%

expected reader range, location, time, and process sequence. Figure 4 shows how TTL and site-sequence checks connect movement events to deny, alert, and audit actions. The manufacturer's site TTL represents how long a tagged item remains at the manufacturer's stage. In normal records, this value is tightly controlled by the production schedule, so the standard deviation is very small (0.003). The site TTL perturbation step for cloned records is intended to introduce greater variance at the manufacturer stage, simulating a cloned tag that does not follow the true production schedule. Thus, the jump from 0.003 to 0.253 is not noise but is the expected signature of a cloning attack at the manufacturer stage.

Table 6 shows the classification performance of the proposed context-aware detection approach using thresholds derived from the statistical indicators (sequence TTL variation and reader/writer distance variation).

Table 7 shows the Performance metrics with 95 per cent confidence intervals.

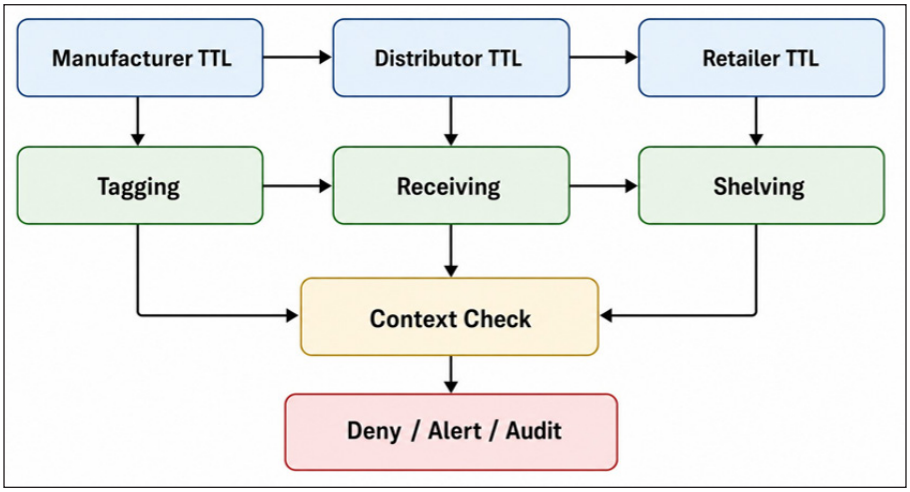

Figure 4. TTL and site-sequence checks for cloned-tag detection

The ACPT evidence in Figure 2, together with the SCM dataflow and site-sequence diagrams in Figures 3 and 4, supports the use of layered policy enforcement, as the implementation demonstrates policy modelling, verification, testing, and operational data movement rather than merely a theoretical design. RBAC is useful for administrative roles such as system administrators, supervisors, and employees. MAC is useful for controlling sensitive transaction and process files. ABAC is the most flexible layer for distributed SCM because it evaluates organisation, role, resource, action, time, place, and ownership. ECA rules connect these access decisions to live RFID events by converting abnormal TTL, reader range, and site sequence into deny, alert, and audit actions.

Following the policy modelling and verification phase, the ACPT was used to evaluate the implemented access-control policies against test requests. Figure 5 presents the policy modelling and verification screens.

Figure 5 shows the ACPT evaluation screens showing MAC, RBAC, and ABAC policy testing against concrete request inputs. These screens illustrate the tool interface; the substantive verification evidence is provided in Table 8 (NuSMV verification log). The MAC screen demonstrates the enforcement of mandatory restrictions on sensitive process files; the RBAC screen shows role-oriented policy configuration for administrators, supervisors, and employees; and the ABAC output illustrates the evaluation of richer contextual attributes, including organisation, employee position, workplace, working hours, and movement context. These evaluation screens confirm that the layered policy framework can assess RFID-SCM requests based on comprehensive subject, resource, action, and environmental attributes before making an access decision. Figure 6 presents the dynamic verification and evaluation screens for the three access-control models.

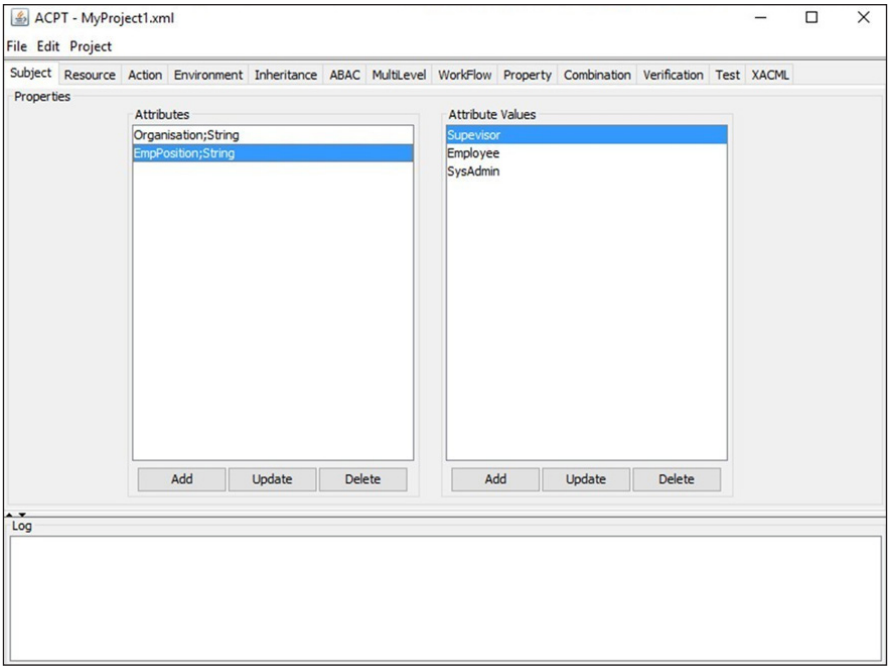

Figure 5. ACPT evaluation screens showing MAC, RBAC, and ABAC policy testing

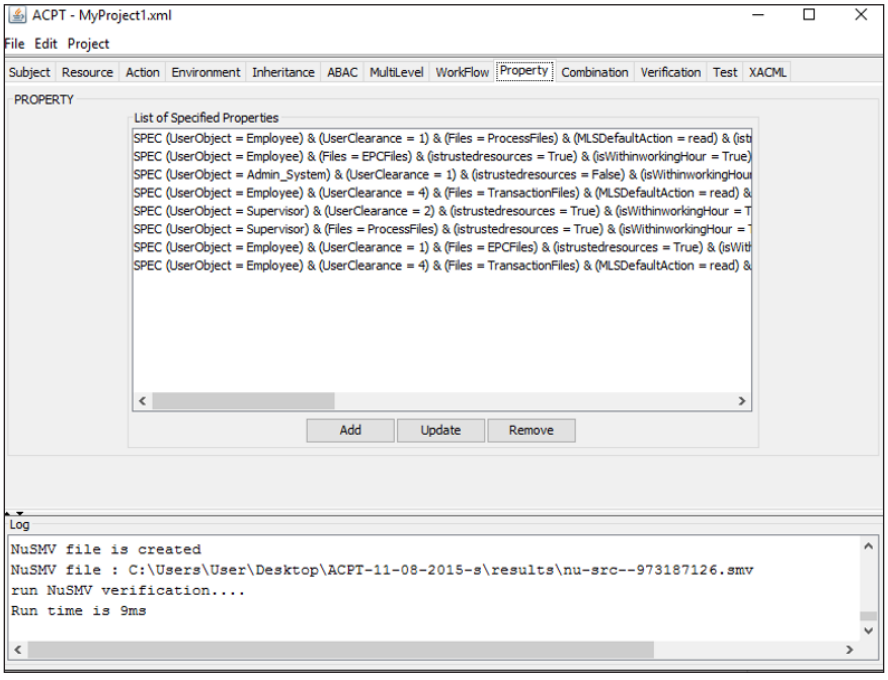

Figure 6. ACPT evaluation screens for testing MAC, RBAC, and ABAC policies

Table 8 summarises the NuSMV verification log. The NuSMV model checker explored 1,024 states and checked 12 security properties: separation of duties, least privilege, role hierarchy consistency, mandatory access enforcement, and attribute-based policy consistency. The lack of counterexamples suggests that the modelled RBAC, MAC, ABAC and ECA policies met all the specified security properties. Additionally, the implemented policy engine was tested using 24 dynamic test cases, all of which passed. These findings support the layered policy framework's internal consistency and enforceability prior to deployment.

Table 8
NuSMV verification log summary

Verification Item	Detail
Verification tool	NuSMV 2.4.3 (integrated within ACPT)
Model file	MyProject1.xml
NuSMV output file	nu-out-1518272332.txt
Properties verified	12
States explored	1,024
Verification time	9 ms
Counterexamples generated	0
Verification result	All properties satisfied
Security properties checked	Separation of duties, least privilege, role hierarchy consistency, mandatory access enforcement, attribute-based policy consistency
Policy models verified	RBAC, MAC, ABAC, ECA
Dynamic test cases executed	24
Dynamic test cases passed	24
Dynamic test cases failed	0

Findings Based on the Research Questions

The findings answer the four research questions as follows:

1. How can RFID-SCM access requests and tag movements be evaluated using contextual attributes?

   The study finds that RFID-SCM requests should be evaluated by combining identity attributes with operational context. A tag read should not be accepted only because the EPC exists in the database. Instead, the decision process must evaluate the employee role, organisation, requested action, resource ownership, working place, working hours, reader location, TTL value, reader/writer distance, and site movement sequence. This directly supports the proposed context-aware policy procedure described in this paper.

2. Which access-control models are suitable for manufacturer, distributor, and retailer environments?
   The findings show that a layered policy model is more suitable than a single access-control model. RBAC is suitable for role-based operational permissions for administrators, supervisors, employees, manufacturers, distributors, and retailers. MAC is suitable for protecting sensitive transaction and process files. ABAC is the most flexible model for inter-organisational SCM because it evaluates subject, resource, action, environment, and movement attributes. Therefore, the manufacturer–distributor–retailer environment benefits from the combined enforcement of RBAC, MAC, ABAC, and ECA.
3. How can event-condition-action rules and time-to-live checks support cloned-tag detection?
   The research finds that ECA rules can convert abnormal RFID events into direct security responses. The event is a tag-read operation; the condition checks whether the EPC, reader, location, TTL, role, and sequence are valid, and the action denies access, raises an alert, and records the event for audit. TTL checks are useful because cloned tags may reuse a valid EPC but still disturb the expected manufacturer–distributor–retailer movement sequence. Figure 4 shows that TTL and site-sequence checking can connect abnormal movement to deny, alert, and audit actions.
4. Which dataset patterns distinguish normal records from cloned records?
   The cleaned dataset contained 205 labelled records, including 188 normal records and 17 cloned records. The clearest distinguishing pattern was not the single-stage distributor or retailer TTL mean, because these values were similar for normal and cloned classes. The stronger indicators were sequence TTL variation and reader/writer distance variation. Normal records had a stable sequence TTL mean of 2.918 minutes with a standard deviation of 0.002, while cloned records had a lower mean of 2.826 minutes and a higher standard deviation of 0.388. Reader/writer distance was also more variable for cloned records, with a cloned mean of 6.147 m and standard deviation of 1.312 compared with the stable normal value of 5.750 m.

These findings clearly show that an effective RFID-IoT counterfeit-prevention system must go beyond static EPC checks. It requires a layered access-control framework (RBAC + MAC + ABAC + ECA) that continuously evaluates contextual attributes (time, location, role, TTL, movement sequence) and uses statistical indicators (sequence TTL variation, reader/writer distance variation) to detect cloned tags *in an* **event-driven manner** across the supply chain. Counterfeit prevention in RFID-enabled SCM should be event-driven and context-aware. The principal findings and their implications for the proposed system are summarised in Table 9.

Table 9
Findings and implications for the RFID-IoT counterfeit-prevention system.

Finding	Implication for the RFID-IoT counterfeit-prevention system
RQ1: Context-aware evaluation is required	The system must continuously evaluate time, location, reader, employee role, organisation, and movement sequence, rather than EPC identity alone.
RQ2: Layered access control is essential	The system must integrate RBAC, MAC, ABAC, and ECA in a unified policy-decision framework to address diverse organisational roles and security requirements.
RQ3: ECA and TTL enable event-driven clone detection	The system can automatically deny access, raise alerts, and audit events when abnormal TTL or site-sequence patterns are detected, providing immediate counterfeit prevention.
RQ4: Cloned records show distinct patterns	The system can use statistical dispersion, including variation in sequence TTL and reader/writer distance, as a signature to distinguish cloned from normal tags, even when EPCs are identical.

LIMITATIONS

The evaluation dataset consists of 205 labelled records, of which 188 are normal, and only 17 are cloned (8.29% cloned proportion). The statistical power of the claims about detection performance is constrained by the small, highly skewed dataset. Despite the promising classification potential (accuracy = 97.56%, F1-score = 84.85%) shown in the confusion matrix, these results should be taken with caution. This high accuracy is partly driven by the majority class (normal records). Future work shall focus on tackling class imbalance through SMOTE, cost-sensitive learning, or ensemble learning, and on validation on larger, more balanced datasets. Moreover, the current study employs a simulated dataset; validation with real RFID middleware data is necessary prior to operational deployment. The study did not include a deliberate fault-injection test that would produce a captured counterexample trace. Also, the comparison of alternatives is based on a simulated dataset and excludes machine learning-based approaches (e.g., Random Forest, SVM, or deep learning). Future work should enlarge the dataset, test automated classification under class imbalance, validate rules in live RFID middleware, and compare the policy engine with blockchain-supported traceability and zero-trust enforcement. Also, it should measure real-time performance metrics, including detection latency and system throughput in live RFID middleware.

Comparative Analysis

To provide context for the performance of the proposed context-aware approach, this section compares it with three alternative detection strategies that represent increasingly rich uses of contextual information. The first alternative is to perform only static EPC checks, which is the standard method for accepting a tag read based solely on the EPC's presence

in the database. The second alternative is single-stage TTL thresholding. The classification is based solely on the TTL values of the manufacturer, distributor, or retailer. The third alternative is reader/writer distance thresholding only, which uses distance values to identify only suspicious tag reads. These alternatives are tested on the same 205-record dataset (188 normal records and 17 cloned records) and the same confusion matrix methodology reported in Table 6. The comparative results are shown in Table 10.

Table 10
Comparative analysis of alternative detection approaches.

Detection Approach	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Key Limitation
Static EPC checking alone	8.29	100.00	8.29	15.31	Cannot detect cloned tags that reuse legitimate EPCs
Single-stage TTL thresholding	50.24	8.29	50.00	14.21	Distributor and retailer TTL means are nearly identical for normal and cloned records
Reader/writer distance thresholding	78.54	45.16	82.35	58.33	High false positive rate due to overlap between normal and cloned distributions
Proposed combined contextual approach (RBAC + MAC + ABAC + ECA)	97.56	87.50	82.35	84.85	Small sample size and class imbalance limit generalisability

CONCLUSION

The proposed context-aware procedure combines RBAC, MAC, ABAC, and ECA rules to prevent counterfeit activity by verifying identity, role, file, action, location, working time, reader/writer range, TTL, and movement sequence. The main finding is that cloned records are detected through combined contextual evidence rather than static EPC checking alone. In the cleaned dataset, normal records were highly stable in sequence TTL and reader/writer distance, while cloned records showed larger variation. The conclusion is that RFID-IoT counterfeit prevention requires integrated access-control verification and continuous, event-driven, and context-aware evaluation of movement context across organisational boundaries.

ACKNOWLEDGEMENT

The authors acknowledge the support of the School of Computing, Universiti Sains Malaysia (USM), Malaysia. This research was supported by a research grant under FRGS of USM.

LIST OF ABBREVIATION

ABAC	Attribute-Based Access Control
ACPT	Access Control Policy Tool
AI	Artificial Intelligence
DFD	Data-Flow Diagram
ECA	Event-Condition-Action
EPC	Electronic Product Code
EPCIS	Electronic Product Code Information Services
FN	False Negative
FP	False Positive
FRGS	Fundamental Research Grant Scheme
GS1	Global Standards One
IIoT	Industrial Internet of Things
IoT	Internet of Things
MAC	Mandatory Access Control
NIST	National Institute of Standards and Technology
NuSMV	New Symbolic Model Verifier
RBAC	Role-Based Access Control
RFID	Radio Frequency Identification
SCM	Supply Chain Management
SD	Standard Deviation
TN	True Negative
TP	True Positive
TTL	Time-to-Live

REFERENCES

Chu, C., Wang, R., Deng, N., & Li, G. (2025). Efficient and reliable identification of probabilistic cloning attacks in large-scale RFID systems. *Micromachines, 16*(8), Article 894. https://doi.org/10.3390/mi16080894

Derakhshan, R., Orlowska, M. E., & Li, X. (2007). RFID data management: Challenges and opportunities. In *2007 IEEE International Conference on RFID* (pp. 175-182). IEEE. https://doi.org/10.1109/RFID.2007.346166

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

GS1. (2022). *EPC information services (EPCIS) standard* (Release 2.0). https://ref.gs1.org/standards/epcis/2.0.0/

Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). *Guide to attribute based access control (ABAC) definition and considerations* (NIST Special Publication 800-162). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-162

Huang, W., Zhang, Y., & Feng, Y. (2020). ACD: An adaptable approach for RFID cloning attack detection. *Sensors, 20*(8), Article 2378. https://doi.org/10.3390/s20082378

Kamble, S. S., Gunasekaran, A., & Sharma, R. (2020). Modeling the blockchain enabled traceability in agriculture supply chain. *International Journal of Information Management, 52*, Article 101967. https://doi.org/10.1016/j.ijinfomgt.2019.05.023

Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *International Journal of Production Economics, 231*, Article 107831. https://doi.org/10.1016/j.ijpe.2020.107831

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*, Article 100087. https://doi.org/10.1016/j.csa.2025.100087

Mahinderjit-Singh, M., & Li, X. (2010). Trust in RFID-enabled supply-chain management. *International Journal of Security and Networks, 5*(2-3), 96-105. https://doi.org/10.1504/IJSN.2010.032208

Michael, K., & McCathie, L. (2005). The pros and cons of RFID in supply chain management. In *International Conference on Mobile Business (ICMB'05)* (pp. 623-629). IEEE. https://doi.org/10.1109/ICMB.2005.103

Mustaffa, M. B., Singh, M. M., & Selvaraj, K. (2024). RFID clone detection in supply chain using modified Count-Min and BASE protocol. *International Journal of Safety and Security Engineering, 14*(2), 447-457. https://doi.org/10.18280/ijsse.140212

Nadime, K. L., Benhra, J., Mouatassim, S., & Benabbou, R. (2026). A blockchain- and RFID-based system for enhanced traceability and fraud prevention in supply chain management. *Journal of Engineering, 2026*(1), Article 8870924. https://doi.org/10.1155/je/8870924

Nawaz, A., Wang, L., Irfan, M., & Westerlund, T. (2024). Hyperledger sawtooth based supplychain traceability system for counterfeit drugs. *Computers & Industrial Engineering, 190*, Article 110021. https://doi.org/10.1016/j.cie.2024.110021

Patric, I. A. (2016). *Context-aware security policies model to thwart counterfeiting attack RFID-enabled supply chain management* [Master's dissertation, School of Computer Sciences].

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Siyal, F., Guzzo, A., Alkhabbas, F., Felicetti, C., Sacca, D., & Pasqua, F. (2026). From traceability to intelligence: A review of blockchain, IoT, and AI for transparent supply chains. *Cluster Computing, 29*(5), Article 325. https://doi.org/10.1007/s10586-026-06125-6

Sunny, J., Undralla, N., & Pillai, V. M. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. *Computers & Industrial Engineering, 150*, Article 106895. https://doi.org/10.1016/j.cie.2020.106895