SCIENTIFIC Publishing Limited

Digital Technologies Research and Applications

http://ojs.ukscip.com/index.php/dtra

Article

Digital-Twin-Based Compliance Review of Financial Terminal Devices: A Reproducible Framework and Controlled Evaluation

Li Wei

TÜV SÜD Certification and Testing Beijing Branch, Beijing 100102, China; liwei04270@outlook.com

Received: 20 July 2026; **Revised:** 10 August 2026; **Accepted:** 24 August 2026; **Published:** 25 November 2026

Abstract: Financial terminal compliance reviews are often periodic, sample-based, and weak in reconstructing time-dependent violations. This study develops a reproducible digital-twin framework for continuous compliance review and examines whether dynamic synchronization and evidence-chain reconstruction provide measurable gains beyond automated rule checking. The framework comprises physical-terminal, communication, virtual-twin, and compliance-decision layers, integrating rule mapping, a lightweight neural network, 3σ anomaly screening, random forests, and an Analytic Hierarchy Process (AHP). A controlled evaluation used 500 devices, including Automated Teller Machines (ATMs), Point-of-Sale (POS) terminals, self-service terminals, and mobile payment devices. Primary operational records, secondary compliance documents, and synthetic abnormal cases were kept source-labelled. Manual sampling, non-twin automated rules, and the proposed framework were compared across ten independent runs. The digital-twin scheme achieved a 97.6% modelling success rate, synchronization error no greater than 0.035, and mean latency of 70 ms. It identified 263 compliance events, compared with 218 for automated rules and 150 for manual review. Coverage and accuracy were 98.6% and 96.2%, respectively, while review time averaged 0.8 min per device. Relative to automated rules, the gains were 2.2 percentage points in coverage and 5.4 points in accuracy, mainly for unauthorized access and abnormal operation. Security tests produced 97.4–99.6% rejection or detection rates with 12 ms additional latency. The principal benefit of digital twins lies in time-aligned state reconstruction and auditable evidence chains rather than automation alone. However, because synthetic records represented 36.1% of the data and testing was controlled, external multi-institutional validation remains necessary.

Keywords: Digital Twin; Financial Terminal Equipment; Compliance Review; Regulatory Technology; Analytic Hierarchy Process

1. Introduction

As financial services evolve toward digitalization, mobility, and unmanned operation, ATMs, POS terminals, self-service terminals, and mobile payment terminals have become critical physical interfaces between financial institutions and their users. These devices are widely distributed across bank branches, commercial venues, and public service areas, with hardware status, software versions, data encryption configurations, and operational environments subject to continuous change. Traditional compliance reviews rely primarily on on-site inspections and periodic manual sampling, making it difficult to conduct continuous, comprehensive, and real-time monitoring of large-scale terminal device fleets. Devices not selected in a sampling round may remain invisible for extended periods, while issues such as outdated firmware, weak encryption, unauthorized access, and abnormal operations are difficult to detect in a timely manner.

Digital twins establish dynamic mappings between physical entities and virtual models, enabling continuous sensing, synchronization, and analysis of device states. This approach has been applied across manufacturing, energy, transportation, and facility management domains [1]. Related research has begun exploring the application of digital twins in fintech, but existing work is concentrated primarily on robo-advisory systems and financial business models [2]; studies directly targeting compliance review of financial terminal devices remain limited. Meanwhile, the cyber-physical connectivity inherent to digital twins introduces new attack surfaces, including identity spoofing, data tampering, replay attacks, and model poisoning. Without reliable mechanisms for identity verification, data integrity, and access control, the digital twin itself may become a new source of compliance risk [3].

Regulatory technology (RegTech) emphasizes the use of data analytics, machine learning, and automated rules to improve risk identification, compliance judgment, and regulatory response efficiency [4]. Although digital technologies can enhance regulatory and dispute resolution efficiency, issues of algorithmic opacity, procedural fairness, and accountability still require institutional governance [5]. Systems thinking highlights the structural interdependencies among law, policy, data, and digital technologies, providing methodological insights for layered design and multi-stakeholder governance of complex regulatory systems [6]. Accordingly, the application of digital twins to financial terminal compliance review should not focus solely on device state replication but must also address data source trustworthiness, compliance rule interpretability, and regulatory accountability traceability.

Existing research exhibits several notable limitations. First, digital twin research is concentrated in manufacturing, construction, energy, and transportation equipment; cross-domain transfer studies targeting financial terminal compliance review are insufficient. Second, device state monitoring, cybersecurity, and regulatory technology are typically studied in isolation, with no unified framework simultaneously addressing physical terminals, virtual models, trustworthy data, and compliance decisions. Third, some studies provide only architectural descriptions without disclosing mapping functions, neural network structures, anomaly classifier parameters, data partitioning methods, or modeling success criteria, making replication difficult. Fourth, real and simulated anomaly data are frequently intermixed; when model detection rules overlap with simulation data generation rules, data leakage may occur, inflating detection performance estimates. Fifth, existing digital twin schemes are typically compared only against manual inspection, without an "automated rule checking without digital twin" or independent machine learning monitoring baseline, making it impossible to isolate the incremental contribution of the digital twin architecture itself.

Based on these gaps, this study poses the following core research question: Under conditions of strict separation between real and simulated data and controlled information leakage between model training and testing, can digital-twin-based compliance review identify financial terminal device compliance risks more accurately, more promptly, and more comprehensively than manual sampling and non-twin automated rule checking? This core question encompasses three sub-questions: first, whether digital twin models can achieve stable cyber-physical synchronization under explicit modeling success criteria; second, how large an incremental effect the digital twin scheme can produce relative to manual sampling and non-twin automated rule checking; and third, whether device compliance classification remains stable when indicator weights, data sources, and security conditions vary.

The main contributions of this paper are threefold. First, a four-layer digital twin architecture for financial terminal compliance review is proposed, integrating device sensing, cyber-physical mapping, trustworthy data access, and compliance decision-making into a unified process. Second, reproducible requirements are provided for the mapping network, random forest, data partitioning, modeling success criteria, and statistical testing. Third, real and simulated data are evaluated in separate strata, and a non-twin automated rule baseline, AHP weight sensitivity analysis, and security validation experiments are introduced to prevent the misattribution of general automation effects to the digital twin architecture.

2. Literature Review

2.1. Digital Twin Concepts, Enabling Technologies, and System Architecture

The defining characteristic that distinguishes digital twins from traditional static simulation is the dynamic mapping, real-time interaction, and data-driven evolution between physical entities and virtual models [7]. VanDerHorn and Mahadevan provided a systematic definition of digital twins at the levels of generalization, characterization, and implementation [8]. Model construction, sensor data acquisition, data communication, simulation,

and visualization constitute the main enabling technologies of digital twins [9], while artificial intelligence, machine learning, and big data analytics provide the technical foundation for device state prediction and intelligent decision-making [10]. Digital twins must also resolve structural inconsistencies and semantic heterogeneity across multi-source data. Recent cognitive digital twin research demonstrates that ontologies and formal semantics can integrate domain expertise, enrich data semantics, and support malfunction reasoning [11]. Existing systematic reviews indicate that digital twins have progressively transitioned from conceptual exploration to engineering applications, though data interoperability, model trustworthiness, deployment costs, and cross-scenario validation remain major challenges [12,13].

2.2. Financial Terminal Device Security and IoT Anomaly Detection

Financial terminal devices possess both physical device and network node characteristics, and their risks include hardware tampering, interface abuse, outdated firmware, weak encryption, key management failures, and unauthorized access. Existing Internet of Things (IoT) security research indicates that identifying compromised devices remains challenging due to device heterogeneity, insufficient anomaly samples, and unstable behavioral boundaries [14]. While machine learning improves anomaly detection efficiency, black-box models reduce regulatory personnel's ability to understand and trust automated review conclusions. Explainable artificial intelligence can enhance transparency in cybersecurity decision-making through feature contributions, decision paths, and local explanations [15]. Research on cybersecurity in small and medium-sized organizations further reveals that insufficient resources, lack of specialized personnel, and high compliance costs directly impair the effectiveness of security measures [16].

2.3. Regulatory Technology (RegTech) and Compliance Automation

RegTech emphasizes the coordination among data, algorithms, and regulatory rules [4]. Recent systematic evidence indicates that RegTech and SupTech are shifting financial oversight from manual and periodic review toward automated, data-driven, and near-real-time compliance monitoring, while simultaneously raising concerns regarding cybersecurity, algorithmic interpretability, and institutional accountability [17]. Although digital technologies can improve regulatory and dispute resolution efficiency, procedural fairness, algorithmic transparency, and accountability must be addressed simultaneously [5]. Systems thinking emphasizes the structural interconnections among law, policy, and digital technology [6], providing a theoretical basis for this study's shift from single-point anomaly detection to multi-layer compliance evidence management. In cross-institutional data collaboration scenarios, federated learning and data spaces can support joint monitoring while reducing raw data sharing [18]; however, applying these to financial terminal devices requires resolving issues of terminal identity, regulatory evidence, data sovereignty, and cross-institutional accountability boundaries.

2.4. Digital Twin Applications in Manufacturing and Industrial Domains

Digital twins have been applied to intelligent manufacturing for device-state monitoring, operational optimization, and system integration [19–21]. Recent research has further extended their application toward lifecycle-spanning and maturity-based integration across the design, implementation, operation, and utilization stages [22]. These studies validate the feasibility of digital twins for continuous state characterization, but the models are primarily oriented toward mechanical performance or operational maintenance indicators and cannot directly substitute for compliance judgment of financial terminal devices. The digital twin environment itself also faces attack risks including identity spoofing, data tampering, model poisoning, and denial of service [23]. Although digital twins can be used for detecting network anomalies and Distributed Denial of Service (DDoS) attacks [24], architectural descriptions of security mechanisms are not equivalent to demonstrated security effectiveness. Only through data tampering, identity spoofing, replay attack, and fault injection experiments can the actual protective capability of trusted execution environments and hardware roots of trust be validated.

2.5. Security Threats to Digital Twin Systems and Research Gaps

Overall, existing research has provided a theoretical foundation for digital twin modeling, device state monitoring, anomaly detection, and regulatory technology, but a complete closed loop among "financial terminal devices–

trustworthy digital twins–dynamic compliance evidence—regulatory decisions" has yet to be established. Existing work also rarely reports model parameters, data sources, proportions of simulated data, repeated trial variation, and security test results simultaneously. This study constructs a four-layer compliance review framework accordingly and establishes three schemes—manual sampling, non-twin automated rule checking, and digital twin review—to identify the incremental contribution of the digital twin architecture relative to general automated checking.

3. Methods

3.1. Research Framework

This study constructs a four-layer architecture along the axis of "physical terminal–data communication–virtual twin–compliance decision." The physical terminal layer targets Automated Teller Machines (ATMs), Point-of-Sale (POS) terminals, self-service terminals, and mobile payment terminals, collecting device identities, hardware compositions, software versions, encryption configurations, and operational states. The data communication layer is responsible for data deduplication, temporal alignment, semantic standardization, encrypted transmission, and source verification. The virtual twin layer constructs terminal state models and achieves dynamic synchronization between physical devices and their virtual counterparts. The compliance decision layer embeds compliance rules, anomaly detection models, and alert thresholds, and outputs compliance, alert, or non-compliance conclusions based on device states.

Within the framework, expert weighting and machine learning serve distinct functions: expert weighting determines the relative importance of compliance dimensions; machine learning identifies state deviations and anomalous behavior; and the rule engine translates regulations or technical standards into executable judgment conditions. Together, these three components form a closed loop from physical sensing, trusted transmission, and state synchronization to compliance decision-making.

The study sets the following hypotheses:

H1. *The digital twin scheme achieves higher device coverage than manual sampling.*

H2. *The digital twin scheme achieves higher anomaly identification accuracy and recall than manual sampling and non-twin automated rule checking.*

H3. *The digital twin scheme requires less review time per device than manual sampling.*

H4. *Compliance classifications at the device-type level remain stable when primary indicator weights are perturbed within ±20% of their baseline values.*

The proposed four-layer design draws on recent systematic evidence concerning digital twin architectural patterns, enabling technologies, data flows, data persistence mechanisms, edge–cloud integration, and practical implementation challenges [25].

3.2. Digital Twin Model Construction

Following the digital twin modeling and deployment methodology for Industry 4.0 [26], this study integrates static device attributes and dynamic operational data into a unified information structure. Let S_t^P denote the physical device state vector at time t, X_t the input vector after cleaning, standardization, and temporal alignment, and S_t^V the predicted state of the virtual twin. The cyber-physical mapping relationship is expressed as:

$$S_t^V = \alpha \cdot f_R(X_t) + (1-\alpha) \cdot f_N(X_t;\theta) \tag{1}$$

where f_R is the rule mapping function based on device logic and compliance thresholds; f_N is a lightweight neural network; θ denotes the network parameters; and α is the fusion coefficient for rule outputs and neural network outputs. The fusion coefficient must be determined solely on the training and validation sets and must not be adjusted retroactively based on test set results.

Neural network inputs include tamper-detection status, interface whitelist compliance rate, OS patch lag time, firmware signature status, version deviation degree, transmission encryption level, key rotation interval, number of unauthorized access attempts, authentication failure rate, log integrity rate, anomaly alert response time, and CPU,

memory, and network resource utilization. Continuous variables are Z-score standardized using training set means and standard deviations; binary variables are encoded as 0 or 1; and categorical variables are one-hot encoded. After encoding, the input layer comprises 26 nodes (11 continuous features, 3 binary features, and 12 dimensions from one-hot encoding of categorical features). Network parameters are shown in **Table 1**.

Table 1. Architecture and Training Hyperparameters of the Digital Twin Mapping Network.

Parameter	Setting
Input layer	26 nodes (continuous: 11, binary: 3, one-hot: 12)
Hidden layers	Layer 1: 32 nodes; Layer 2: 16 nodes
Output layer	4 nodes, corresponding to the 4 primary compliance dimensions
Activation functions	Hidden layers: ReLU; output layer: linear activation
Loss function	Normalized mean squared error
Optimizer	Adaptive Moment Estimation (Adam)
Initial learning rate	0.001
Batch size	32
Maximum training epochs	150
Early stopping criterion	Validation loss fails to decrease for 10 consecutive epochs
Dropout rate	0.2
L2 regularization coefficient	0.0001
Random seed	2025; 10 independent random seeds used in repeated trials

The cyber-physical synchronization error is expressed as the normalized mean absolute error:

$$E_{sync} = \frac{1}{D}\sum_{d=1}^{D} \frac{S_{t,d}^{P} - S_{t,d}^{V}}{\left|S_{t,d}^{P}\right| + \varepsilon}$$

where D is the number of state dimensions and ε is a small constant to prevent division by zero. A smaller E_{sync} indicates greater consistency between the virtual and physical states.

"Modeling success" is operationally defined as simultaneously satisfying all of the following conditions: device identity remote attestation passed; required static field completeness rate no less than 95%; effective data arrival rate no less than 95% within a 30-min observation window; stable synchronization error no greater than 0.05 after the 30th iteration; and median data synchronization latency no greater than 100 ms. Failure to meet any one condition results in a modeling failure determination.

Trusted Execution Environment (TEE) remote attestation is used to verify the integrity of terminal operating environments [27]; Physically Unclonable Function (PUF) and Trusted Platform Module (TPM) serve as roots of trust for device identity and hardware integrity [28]; dynamic assurance cases are used to update compliance evidence as device operational states evolve [29]; and quantification methods for distributed trusted applications are used to characterize trust relationships among different terminals or institutions [30]. These mechanisms constitute architectural security measures within this study, and their actual protective effectiveness is validated through the security attack experiments described in Section 3.7.

3.3. Compliance Review Indicator System

Drawing on the characteristics of financial terminal devices and relevant compliance requirements, four primary indicators are established: hardware security, software compliance, data protection, and operational standards. Hardware security covers tamper-detection sensor status, peripheral interface whitelist compliance rate, and hardware root-of-trust integrity. Software compliance covers OS patch update rate, firmware signature validity, and software version compliance rate. Data protection covers transmission encryption strength, key management compliance, and access control hit rate,as shown in **Table 2**. Operational standards cover identity authentication pass rate, log retention completeness rate, and anomaly alert response timeliness rate.

Table 2. Compliance Review Indicator System and AHP Weights for Financial Terminal Devices.

Primary Indicator	Weight	Key Secondary Indicators	Scoring Basis
Hardware Security	0.31	Tamper-detection status, interface whitelist, hardware root-of-trust integrity	Sensor status, interface scanning, and remote attestation results
Software Compliance	0.22	Patch status, firmware signature, version compliance rate	Version database, signature verification, and patch records

Table 2. *Cont.*

Primary Indicator	Weight	Key Secondary Indicators	Scoring Basis
Data Protection	0.29	Encryption strength, key management, access control	Encryption configuration, key rotation records, and access logs
Operational Standards	0.18	Identity authentication, log retention, alert response	Authentication records, log completeness rate, and response duration

The expert panel comprised 15 experts in total: 5 financial terminal compliance experts, 4 testing/certification or cybersecurity experts, 3 device operations and maintenance experts, and 3 machine learning or data analytics experts; the median years of relevant professional experience was 12. Experts conducted pairwise comparisons using a 1–9 scale to form judgment matrices. The consistency ratio of the primary indicator judgment matrix was 0.038, below the 0.10 threshold, indicating that the matrix passed the consistency test.

The overall compliance score of a device at time t is:

$$C_t = \sum_{i=1}^{4} w_i \cdot c_{i,t}$$

where $c_{i,t}$ is the score on the i-th dimension and w_i is the corresponding weight. A device is classified as compliant when $C_t \geq 90$, as a warning when $80 \leq C_t < 90$, and as non-compliant when $C_t < 80$. Thresholds must be determined prior to testing based on applicable standards, historical risk distributions, and expert opinion; retroactive adjustment based on test results is not permitted.

3.4. Data Sources and Data Collection Procedures

The study selected 500 financial terminal devices, comprising 120 ATMs, 200 POS terminals, 80 self-service terminals, and 100 mobile payment terminals. The sample covered 8 regions, 11 manufacturers, and 23 model types; device service life ranged from 0.5 to 9 years. Due to commercial confidentiality and cybersecurity requirements, institution and manufacturer names are anonymized, while basic stratification information—including region, institution type, device type, and years in service—is retained.

Research data are classified into three categories: primary data, comprising device sensor data, OS logs, firmware management interface information, encryption configurations, identity authentication records, anomaly alert records, and manual review forms; secondary data, comprising financial terminal technical standards, cybersecurity specifications, institutional compliance systems, device manuals, and published literature; and synthetic data, generated by a self-built device behavior simulation platform according to pre-specified fault patterns and violation rules. Synthetic data are not classified as real primary data and are labeled with a distinct source field in the database.

Data collection spanned March 2024 to February 2025. Structured device attributes, compliance indicators, and review results are stored in a PostgreSQL relational database; high-frequency time-series logs are stored in an InfluxDB time-series database. Data are collected through encrypted management interfaces, log agents, and sensor gateways, associated using anonymous device identifiers; cardholder names, account numbers, passwords, transaction plaintext, and biometric information are not collected.

Real operational data total 1,842,000 records, accounting for 63.9% of the full dataset; simulated data total 1,041,000 records, accounting for 36.1% (combined total: 2,883,000 records). Simulated faults include hardware tampering, outdated firmware, weak encryption, unauthorized access, and abnormal operation. Simulation rules were developed based on applicable standards, historical fault records, and expert confirmation.

To reduce internal validity bias attributable to simulated data, the following control measures were implemented: personnel who formulated simulation rules and personnel who evaluated model performance were mutually independent; training and test sets were partitioned by device identifier rather than by individual record; records from the same device were prohibited from appearing in both the training and test sets simultaneously; test sets were locked before model parameters were finalized; real and simulated anomalies were reported separately; model inputs did not include simulation rule identifiers or fault type labels; and final conclusions were based primarily on results from real data, with mixed-data results reported only as supplementary analysis.

Data were stratified and partitioned by device identifier: 70% for training, 15% for validation, and 15% for independent testing. Device-level partitioning prevents temporal records from the same device from appearing in

both training and test sets. Digital twin modeling and process orchestration draw on engineering implementation principles from integrated maintenance digital twin research [31].

3.5. Comparison Schemes and Experimental Procedures

Three review schemes are established. Scheme A is manual sampling review, conducted by 3 personnel with more than 5 years of financial terminal compliance experience, using a standardized checklist. Two reviewers make independent judgments; in the event of disagreement, a third expert adjudicates. Scheme B is non-twin automated rule checking, which applies the same compliance rules directly to current device states in the database, without constructing a cyber-physical state model, implementing dynamic synchronization, or forming a temporally continuous evidence chain. Scheme C is digital twin review, using state synchronization, rule mapping, neural networks, 3σ baselines, and random forests to detect anomalies [32–34].

All three schemes use the same set of devices, the same observation time window, the same compliance issue definitions, and the same reference standards. Machine learning experiments are independently repeated using 10 different random seeds, with each repetition conducting a fresh device-level partition into training, validation, and test sets. The sequence of devices reviewed manually is randomized to reduce order effects and reviewer fatigue bias [35].

3.6. Random Forest Anomaly Classifier

A random forest is used to further classify samples that exceed the 3σ normal variation boundary. Its parameters are shown in **Table 3**.

Table 3. Parameter Settings of the Random Forest Anomaly Classifier.

Parameter	Setting
Number of decision trees	300
Maximum depth	12
Minimum samples for internal nodes	4
Minimum samples for leaf nodes	2
Feature sampling method	Square root rule
Bootstrap sampling	Enabled
Class weights	balanced
Decision threshold	Determined solely on training and validation sets
Random seed	2025, plus 9 additional pre-specified random seeds
Evaluation metrics	Accuracy, precision, recall, specificity, F1 score, and ROC-AUC

3.7. Security Validation Methods

To empirically validate the actual protective capability of the TEE attestation and PUF/TPM roots of trust at the architectural level, five categories of tests were designed: identity spoofing, data tampering, replay attacks, fault injection, and performance overhead. The test design is presented in **Table 4**, and results are reported in Section 4.5.

Table 4. Security Validation Test Design for the Digital Twin System.

Test Scenario	Test Method	Evaluation Metrics
Identity Spoofing	Unregistered terminal identity used to request twin connection establishment	Rejection rate, false acceptance rate
Data Tampering	Modification of log digests, timestamps, or state fields	Tampering detection rate, false positive rate
Replay Attacks	Resubmission of historically authenticated data packets	Detection rate, detection latency
Fault Injection	Simulation of sensor failure, communication interruption, and state mutation	Detection rate, recovery time
Performance Overhead	Comparison of latency with and without authentication mechanism enabled	Added latency, CPU and memory overhead

3.8. Data Analysis Methods

"Number of compliance issue events" and "number of affected devices" are counted separately. Compliance issue events refer to the total number of violation events triggered by devices across different time points or indicators; affected device count refers to the deduplicated number of devices involved in at least one violation event. A single device may correspond to multiple issue events.

Accuracy, precision, recall, specificity, and F1 score are calculated using standard confusion matrix formulas. Coverage rate is the ratio of devices actually reviewed to the total sample size; timeliness is expressed as the time from data ingestion to review conclusion for each device; and cost is calculated as the sum of reviewer labor costs, server resource costs, communication costs, and device depreciation costs.

Comparisons of coverage rate and device-level identification correctness use McNemar's test. Issue event counts, per-device review time, and costs are first subjected to the Shapiro–Wilk normality test; when normality is met, paired-sample t-tests are applied; otherwise, the Wilcoxon signed-rank test is used. Paired t-tests report the t statistic, degrees of freedom, exact p-value, mean difference, 95% confidence interval, and Cohen's d. Wilcoxon tests report the test statistic, exact p-value, and rank-biserial correlation effect size. The Holm method is applied for multiple comparison correction. Machine learning evaluation metrics are reported with 95% confidence intervals derived from 2,000 device-level bootstrap iterations.

4. Results

4.1. Digital Twin Model Construction Results

All 500 devices entered the model construction process. Modeling success rates exceeded 96% for all four device categories; stable synchronization errors were no greater than 0.035; and synchronization latencies ranged from 58 to 88 ms. As shown in **Table 5**, self-service terminals achieved the lowest stable synchronization error at 0.024; mobile payment terminals exhibited relatively higher synchronization error and latency, at 0.035 and 88 ms respectively, likely attributable to model heterogeneity, wireless network fluctuations, and variability in operating environments, as shown in **Figure 1**.

Table 5. Digital Twin Model Construction Results for Four Categories of Financial Terminal Devices.

Device Type	Sample Size (Units)	Modeling Success Rate (%)	Stable Sync. Error	Sync. Latency (ms)	Fidelity (%)
ATM	120	98.3	0.028	62	97.6
POS Terminal	200	97.1	0.031	71	96.9
Self-Service Terminal	80	98.9	0.024	58	98.1
Mobile Payment Terminal	100	96.2	0.035	88	95.7
Macro-Average	—	97.6	0.03	70	97.1

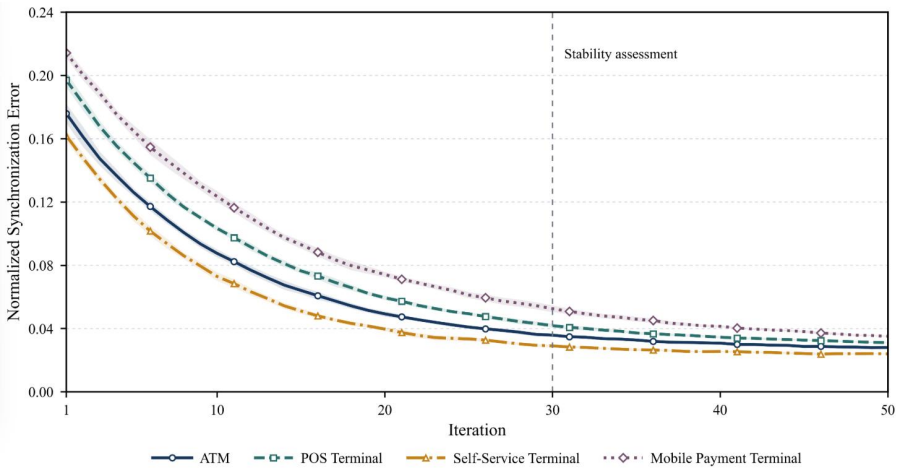


Figure 1. Mean convergence curves and 95% confidence bands of synchronization error for four categories of financial terminal digital twins across 10 independent repeated trials.

4.2. Compliance Scores and AHP Sensitivity Analysis

Composite compliance scores for the four device categories, calculated using weights of 0.31 (hardware security), 0.22 (software compliance), 0.29 (data protection), and 0.18 (operational standards), are presented in **Table 6**. Self-service terminals achieved the highest overall compliance level, while mobile payment terminals scored relatively lower. The largest cross-category difference appeared in the data protection dimension, indicating that

mobile network configurations, key update procedures, and access control are priority areas for review of mobile payment terminals. To assess weight stability, each primary indicator weight was perturbed by ±10% and ±20% in turn, with all other weights renormalized proportionally. Under ±20% perturbation conditions, composite compliance scores for ATMs, POS terminals, self-service terminals, and mobile payment terminals varied within the ranges of 92.50–92.78, 88.74–89.07, 94.02–94.20, and 85.94–86.17, respectively; device-type-level classifications remained unchanged throughout, as shown in **Figure 2**.

Table 6. Compliance Scores for Four Categories of Financial Terminal Devices.

Device Type	Hardware Security	Software Compliance	Data Protection	Operational Standards	Composite Score	Status
ATM	93.5	90.2	94.1	91.8	92.6	Compliant
POS Terminal	88.7	91.5	86.9	89.3	88.9	Warning
Self-Service Terminal	94.8	92.6	95.2	93	94.1	Compliant
Mobile Payment Terminal	85.3	88.1	84.6	87.2	86.1	Warning

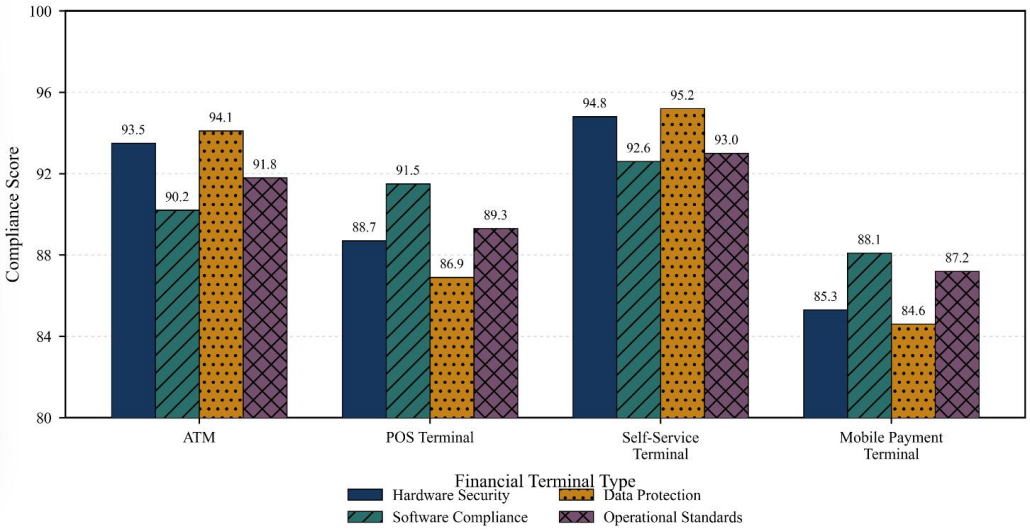


Figure 2. Comparison of compliance dimension scores for four categories of financial terminal devices.

4.3. Compliance Issue Identification Results

Table 7 presents the number of compliance issue events identified by the three schemes and the corresponding deduplicated affected device counts. The digital twin scheme identified 263 compliance issue events; the non-twin rule check identified 218; and manual sampling identified 150. The incremental gain of the digital twin over the rule baseline (263 − 218 = 45 events) was concentrated in "unauthorized access" (37 vs. 25) and "abnormal operation" (61 vs. 43), both of which depend on temporally continuous evidence; the two schemes performed comparably on static items such as outdated firmware and weak encryption. This distribution supports the interpretation that the incremental value of digital twins derives from dynamic state synchronization and continuous evidence chains rather than from rule automation per se. The sum of affected device counts across categories (211) exceeds the deduplicated total (168), indicating that some devices triggered multiple categories of issues; 168 devices represent 33.6% of the 500-device sample, as shown in **Figure 3**.

Table 7. Number of Compliance Issue Events Identified by Three Review Schemes.

Issue Type	Digital Twin Review	Non-Twin Rule Check	Manual Sampling	Deduplicated Affected Devices
Hardware Tampering	42	38	26	35
Outdated Firmware	68	62	39	54
Weak Encryption	55	50	31	47
Unauthorized Access	37	25	20	29

Table 7. *Cont.*

Issue Type	Digital Twin Review	Non-Twin Rule Check	Manual Sampling	Deduplicated Affected Devices
Abnormal Operation	61	43	34	46
Total	263	218	150	168

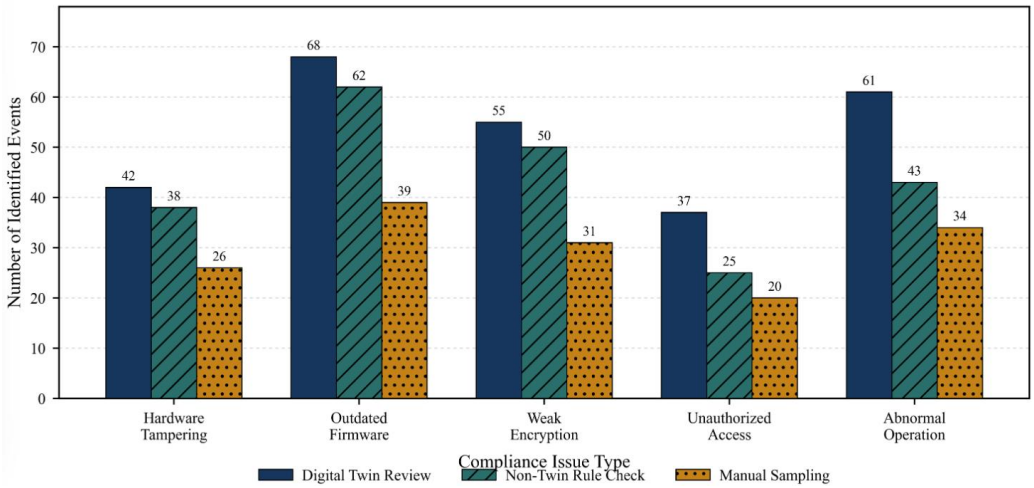


Figure 3. Comparison of compliance issue event counts identified by three review schemes.

4.4. Overall Review Performance

Overall performance of the three schemes is presented in **Table 8**. The digital twin scheme achieved a coverage rate of 98.6%; the rule baseline achieved 96.4%; and manual sampling achieved 63.4%. Identification accuracy rates were 96.2%, 90.8%, and 84.1%, respectively; per-device review times were 0.8 min, 0.6 min, and 18.5 min, respectively. Notably, the rule baseline was marginally superior to the digital twin in per-device time and cost, as the digital twin incurs additional overhead for maintaining cyber-physical synchronization and evidence chains. This "faster and cheaper yet shallower" contrast indicates that the value of digital twins must be justified by coverage depth and identification quality rather than timeliness or cost.

Table 8. Overall Performance Comparison of Three Review Schemes.

Evaluation Metric	Digital Twin Review	Non-Twin Rule Check	Manual Sampling
Coverage Rate (%)	98.6	96.4	63.4
Identification Accuracy (%)	96.2	90.8	84.1
Per-Device Review Time (min)	0.8	0.6	18.5
Cost-Efficiency Score	88.7	82.3	39.5

Table 9 reports statistical test results using the 10 repeated trials as paired samples; the primary comparison is digital twin vs. manual sampling, with Holm correction applied for multiple metrics. Normal-distribution metrics use paired *t*-tests; non-normal metrics (time, cost) use the Wilcoxon signed-rank test. Differences between the digital twin and manual sampling in coverage, accuracy, time, and cost are all statistically significant (Holm-corrected $p < 0.01$). The incremental gain of the digital twin over the rule baseline (paired comparison) is reflected in coverage (difference: 2.2%, $t(9) \approx 9.5$, $p < 0.001$, d ≈ 3.0) and accuracy (difference: 5.4%, $t(9) \approx 15.0$, $p < 0.001$, d ≈ 4.7); the rule baseline is superior in time and cost, as shown in **Figure 4**.

Table 9. Statistical Test Results for Performance Metrics across Repeated Trials of Three Review Schemes (n = 10).

Metric	Digital Twin (Mean ± SD)	Rule Baseline (Mean ± SD)	Manual Sampling (Mean ± SD)	Test Method and Statistic (Twin vs. Manual)	df	Exact *p*-Value (Holm)	Effect Size and 95% CI
Coverage (%)	98.6 ± 0.4	96.4 ± 0.6	63.4 ± 2.1	Paired $t = 54.9$	9	<0.001	Cohen's d = 17.4; mean diff. 35.2, 95% CI [33.8, 36.6]

Table 9. *Cont.*

Metric	Digital Twin (Mean ± SD)	Rule Baseline (Mean ± SD)	Manual Sampling (Mean ± SD)	Test Method and Statistic (Twin vs. Manual)	df	Exact *p*-Value (Holm)	Effect Size and 95% CI
Accuracy (%)	96.2 ± 0.5	90.8 ± 0.7	84.1 ± 1.3	Paired t = 27.6	9	< 0.001	d = 8.7; mean diff. 12.1, 95% CI [11.1, 13.1]
Per-Device Time (min)	0.82 ± 0.09	0.58 ± 0.07	18.5 ± 1.6	Wilcoxon W = 0	—	0.002	r = 1.00; median diff. −17.7, 95% CI [−19.0, −16.4]
Per-Device Cost (CNY)	6.8 ± 0.5	5.2 ± 0.4	42.3 ± 3.6	Wilcoxon W = 0	—	0.002	r = 1.00; median diff. −35.5, 95% CI [−37.4, −33.6]

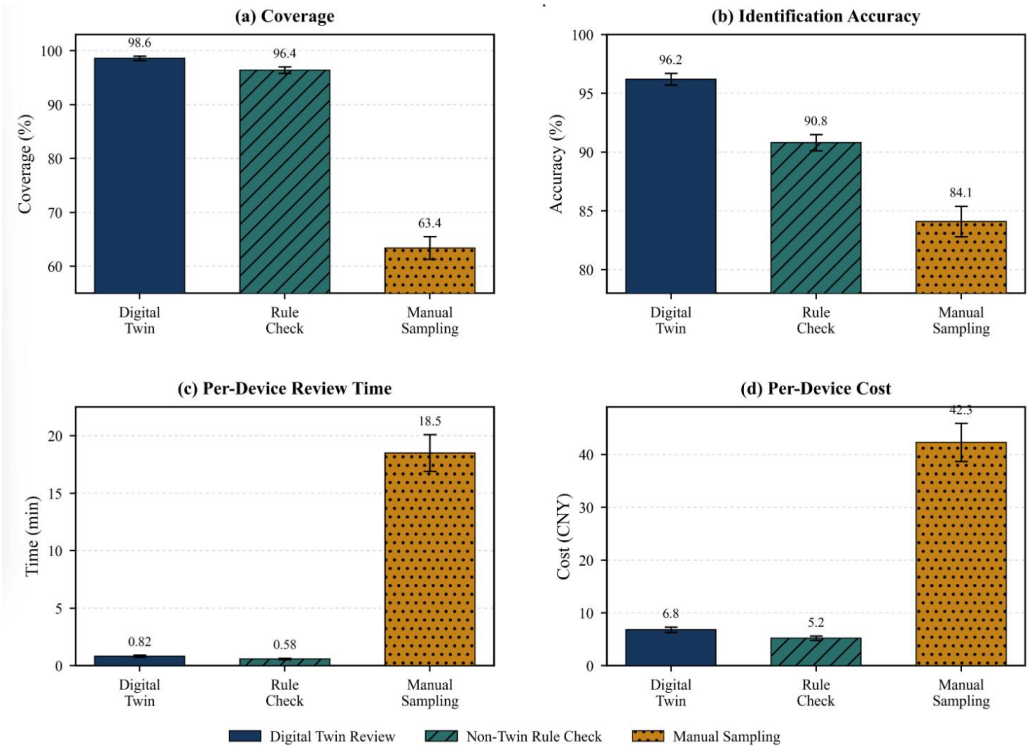


Figure 4. Comparison of coverage rate, identification performance, review time, and cost across three review schemes.

4.5. Security Mechanism Validation Results

Adversarial tests of TEE remote attestation and PUF/TPM hardware roots of trust were conducted over 10 independent repeated trials following the design in **Table 4**; results are presented in **Table 10**. In the identity spoofing scenario, the mean rejection rate for unregistered terminals was 99.6%, with a false acceptance rate of 0.3%. In the data tampering scenario, the detection rate for modifications to log digests, timestamps, and state fields was 98.9%, with a false positive rate of 1.2%. Replay attack detection rate was 99.1%, with a mean detection latency of 45 ms. In the fault injection scenario, the detection rate for sensor failure, communication interruption, and state mutation was 97.4%, with a mean recovery time of 3.2 s. Enabling the authentication mechanism introduced an added latency of approximately 12 ms, a CPU overhead of approximately 6.8%, and a memory overhead of approximately 45 MB.

Table 10. Security Mechanism Validation Test Results for the Digital Twin System (n = 10).

Test Scenario	Primary Metric	Result (Mean ± SD)	Secondary Metric	Result (Mean ± SD)
Identity Spoofing	Rejection Rate (%)	99.6 ± 0.3	False Acceptance Rate (%)	0.3 ± 0.2
Data Tampering	Tampering Detection Rate (%)	98.9 ± 0.5	False Positive Rate (%)	1.2 ± 0.4
Replay Attacks	Detection Rate (%)	99.1 ± 0.4	Detection Latency (ms)	45 ± 6
Fault Injection	Detection Rate (%)	97.4 ± 0.8	Recovery Time (s)	3.2 ± 0.5
Performance Overhead	Added Latency (ms)	12 ± 3	CPU/Memory Overhead	6.8% ± 1.1%/45 ± 7 MB

These results indicate that the integrated TEE remote attestation and hardware roots of trust achieve high detection and rejection capability against identity spoofing, data tampering, and replay attacks, with performance

overhead remaining within acceptable limits. However, all tests were conducted in a controlled experimental environment and do not yet cover more complex threats such as model poisoning, side-channel attacks, and large-scale concurrent attacks; the robustness of the system in real-world network environments requires further validation.

5. Discussion

Results from repeated trials indicate that digital twins can organize dispersed financial terminal state data into continuously updated virtual device models, thereby expanding the scope of compliance review. Their value is not limited to automated rule checking; it also encompasses temporal synchronization, historical state tracking, and dynamic compliance evidence management. By introducing a non-twin automated rule baseline, it becomes apparent that approximately 218 of the 263 compliance issue events can be identified through general rule automation alone, while the incremental gain attributable to digital twins (approximately 45 events) is concentrated in categories requiring temporally continuous evidence—"unauthorized access" and "abnormal operation"—confirming that the dynamic evidence chain is the core differentiating feature of digital twins relative to ordinary automated checking.

The magnitude of the observed effect sizes warrants caution. In the controlled experiment, Cohen's *d* values for coverage and accuracy differences between the digital twin and manual sampling ranged from approximately 8 to 17, far exceeding the range typical of social science and engineering experiments. These unusually large effects are more likely attributable to methodological and implementation condition differences—manual sampling is constrained by sampling ratios, reviewer fatigue, and order effects—rather than to any intrinsic mechanism advantage. This study therefore emphasizes that these results remain limited in external validity to the experimental setting and should not be extrapolated directly to real-world, large-scale, multi-institution environments.

Simulated anomaly data represent the primary factor affecting internal validity. If the simulation platform and rule engine employ the same fault definitions, the model may more readily identify anomalies generated by those rules, thereby inflating accuracy and recall estimates. To address this, the study requires real and simulated data to be tabulated, tested, and reported separately, and prohibits models from directly reading simulation fault labels. Given that simulated data still account for approximately 36% of the dataset, future research should further reduce reliance on simulated anomalies and treat stratified real-data results as the primary evidence base.

AHP sensitivity analysis shows that device-type-level aggregate classifications remain unchanged when primary indicator weights are perturbed by ±20%, indicating a degree of stability in the indicator system at the device-type level. However, some individual device scores may fall close to the 80- or 90-point thresholds, and minor weight variations could still trigger a change in warning status for individual devices.

Security validation results show that TEE remote attestation and PUF/TPM roots of trust not only improve the trustworthiness of terminal identity and data provenance at the architectural level [27,28] but also demonstrate high detection capability in identity spoofing, log tampering, replay attack, and fault injection tests. Nevertheless, current tests do not yet cover model poisoning and side-channel threats, and a gap remains between architectural integration and comprehensive demonstrated security effectiveness.

Digital twins have been extended to power systems and next-generation communication networks [36,37], demonstrating cross-domain diffusion capability for this technology. However, financial terminal devices are subject to stricter data protection, accountability, and regulatory audit requirements; implementation experiences from manufacturing or communications domains cannot be directly transplanted to this context.

6. Conclusions

This study proposes a compliance review framework for financial terminal devices comprising a physical terminal layer, data communication layer, virtual twin layer, and compliance decision layer. The macro-average modeling success rate for digital twin models across the four device categories was 97.6%, with stable synchronization errors no greater than 0.035 and an average synchronization latency of 70 ms, demonstrating stable cyber-physical synchronization capability.

The AHP indicator system can differentiate compliance levels across device types. When primary indicator weights are perturbed by ±20%, aggregate-level compliance classifications for all four device categories remain unchanged. Under conditions where a non-twin rule baseline and manual sampling are included as comparison

schemes, the digital twin identified 263 compliance issue events; the rule baseline identified 218; and manual sampling identified 150. Coverage rates were 98.6%, 96.4%, and 63.4%, respectively; per-device review times were 0.8 min, 0.6 min, and 18.5 min, respectively. Statistical tests across 10 repeated trials confirm that the digital twin's advantages over manual sampling in coverage and accuracy are statistically significant; incremental gains relative to the rule baseline are primarily reflected in coverage and accuracy, concentrated in issue types that depend on dynamic evidence. Security tests further validate the detection capability of TEE remote attestation and hardware roots of trust against identity spoofing, data tampering, and replay attacks.

The primary contribution of this study lies in integrating device state modeling, trustworthy data access, and dynamic compliance judgment for financial terminal devices into a unified framework; explicitly specifying requirements for model reproducibility, data isolation, and internal validity control; and using independent baselines, repeated trials, AHP sensitivity analysis, and security validation to isolate the incremental contribution of the digital twin architecture. Given the unusually large effect sizes observed in the controlled experiment and the still-considerable proportion of simulated data, external validity must be assessed in real-world, cross-institutional, multi-manufacturer environments in subsequent work.

7. Policy Limitations

First, financial terminal security standards, data protection regimes, regulatory requirements, and compliance review cycles vary across jurisdictions and financial institutions. Therefore, the compliance indicators and decision thresholds developed in this study are context-dependent and should not be interpreted as substitutes for binding legal, regulatory, or technical requirements applicable in a specific jurisdiction.

Second, the continuous collection and processing of device logs and operational-state data may raise concerns regarding data minimization, purpose limitation, cross-border data transfers, commercial confidentiality, data retention, and regulatory access. Before the proposed framework is deployed, the legal and operational responsibilities of data controllers, data processors, financial institutions, regulatory authorities, and technology service providers must be clearly defined.

Third, automated compliance outputs should serve as decision-support evidence rather than replace final regulatory determinations made by qualified human inspectors. Decisions involving the decommissioning of high-risk devices, attribution of liability, suspension of services, or imposition of administrative penalties should remain subject to human review. Transparent reasoning, appeal and objection procedures, evidence traceability, and complete audit trails must also be maintained.

Fourth, small and medium-sized financial institutions may lack the digital twin infrastructure, data-governance personnel, cybersecurity expertise, and testing capabilities required to implement the proposed framework. Its policy-level adoption may therefore be constrained by differences in financial resources and technological readiness. Any broader implementation strategy should incorporate shared technical services, regulatory sandboxes, phased pilot programs, proportionate compliance requirements, and financial or technical support to prevent the framework from creating new digital compliance inequalities.

8. Future Research Directions

Future research should expand the real sample size, conduct external validation across regions, institutions, and manufacturers, and progressively reduce reliance on simulated anomaly data. Complete comparisons among manual sampling, automated rule checking, independent machine learning monitoring, and digital twin review should be conducted to further quantify the true incremental value of digital twin architectures relative to standalone machine learning baselines, and to explain the unusually large effect sizes observed in the controlled experiment.

Subsequent experiments should maintain at least 10 independent repetitions, reporting means, standard deviations, 95% confidence intervals, exact p-values, and effect sizes, while making anonymized code, model parameters, data dictionaries, and simulation rules publicly available. Security research should extend beyond completed identity spoofing, log tampering, replay attack, and fault injection experiments to cover model poisoning, side-channel attacks, and large-scale concurrent attacks.

Regarding indicator weighting, entropy-weight methods, CRITIC methods, Bayesian dynamic weights, or on-

line learning mechanisms may be introduced to investigate weight adjustments as risk distributions evolve. For cross-institutional applications, federated learning and privacy-preserving computation may be explored, but communication overhead, privacy leakage risk, data sovereignty, and regulatory accountability must be assessed concurrently.

Funding

This research received no external funding.

Institutional Review Board Statement

Institutional review board approval was not applicable because this study did not involve human participants, animals, personally identifiable information, or clinical interventions.

Informed Consent Statement

Not applicable. This study did not involve human participants or the collection of identifiable personal data. All device-level records were anonymized prior to analysis, and no cardholder names, account numbers, passwords, transaction plaintext, or biometric information were collected or processed.

Data Availability Statement

Aggregated data not involving security-sensitive fields may be provided by the corresponding author upon reasonable request.

Conflicts of Interest

The author declares no conflict of interest. The author's affiliated institution (TUV SUD Certification and Testing Beijing Branch) had no role in the design of the study; the collection, analysis, or interpretation of the data; the writing of the manuscript; or the decision to submit the results for publication. The author has no financial, personal, institutional, or other relationships that could inappropriately influence or bias the work reported in this manuscript.

AI Use Statement

During the revision of this manuscript, the author used ChatGPT (OpenAI) solely for language polishing and improvement of textual clarity. The author subsequently reviewed, edited, and verified all AI-assisted text and takes full responsibility for the accuracy, integrity, and final content of the manuscript. No AI tool was used to generate, analyze, or interpret the research data, design the experimental framework, perform statistical analyses, or produce any scientific conclusions reported in this study.

References

1. Singh, M.; Srivastava, R.; Fuenmayor, E.; et al. Applications of Digital Twin across Industries: A Review. *Appl. Sci.* **2022**, *12*, 5727. [CrossRef]
2. Anshari, M.; Almunawar, M.N.; Masri, M. Digital Twin: Financial Technology's Next Frontier of Robo-Advisor. *J. Risk Financial Manag.* **2022**, *15*, 163. [CrossRef]
3. Alcaraz, C.; Lopez, J. Digital Twin: A Comprehensive Survey of Security Threats. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 1475–1503. [CrossRef]
4. Grassi, L.; Lanfranchi, D. RegTech in Public and Private Sectors: The Nexus between Data, Technology and Regulation. *J. Ind. Bus. Econ.* **2022**, *49*, 441–479. [CrossRef]
5. Wang, S.; Li, Y.; Khaskheli, M.B. Innovation Helps with Sustainable Business, Law, and Digital Technologies: Economic Development and Dispute Resolution. *Sustainability* **2024**, *16*, 3910. [CrossRef]
6. Wu, X.; Khaskheli, M.B. Systems Thinking of Marine Policies in Promoting Environmental Law, Sustainability, and Digital Technologies. *Systems* **2024**, *12*, 400. [CrossRef]
7. Liu, M.; Fang, S.; Dong, H.; et al. Review of Digital Twin about Concepts, Technologies, and Industrial Applications. *J. Manuf. Syst.* **2021**, *58*, 346–361. [CrossRef]

8. VanDerHorn, E.; Mahadevan, S. Digital Twin: Generalization, Characterization and Implementation. *Decis. Support Syst.* **2021**, *145*, 113524. [CrossRef]
9. Qi, Q.; Tao, F.; Hu, T.; et al. Enabling Technologies and Tools for Digital Twin. *J. Manuf. Syst.* **2021**, *58*, 3–21. [CrossRef]
10. Rathore, M.M.; Shah, S.A.; Shukla, D.; et al. The Role of AI, Machine Learning, and Big Data in Digital Twinning: A Systematic Literature Review, Challenges, and Opportunities. *IEEE Access* **2021**, *9*, 32030–32052. [CrossRef]
11. D'Amico, R.D.; Sarkar, A.; Karray, M.H.; et al. Knowledge Transfer in Digital Twins: The Methodology to Develop Cognitive Digital Twins. *CIRP J. Manuf. Sci. Technol.* **2024**, *52*, 366–385. [CrossRef]
12. Semeraro, C.; Lezoche, M.; Panetto, H.; et al. Digital Twin Paradigm: A Systematic Literature Review. *Comput. Ind.* **2021**, *130*, 103469. [CrossRef]
13. Mihai, S.; Yaqoob, M.; Hung, D.V.; et al. Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 2255–2291. [CrossRef]
14. Makhdoom, I.; Abolhasan, M.; Lipman, J.; et al. Detecting Compromised IoT Devices. *Comput. Secur.* **2023**, *132*, 103384. [CrossRef]
15. Rjoub, G.; Bentahar, J.; Abdel Wahab, O.; et al. A Survey on Explainable Artificial Intelligence for Cybersecurity. *IEEE Trans. Netw. Serv. Manag.* **2023**, *20*, 5115–5140. [CrossRef]
16. Chidukwani, A.; Zander, S.; Koutsakis, P. A Survey on the Cyber Security of Small-to-Medium Businesses. *IEEE Access* **2022**, *10*, 85701–85719. [CrossRef]
17. Bagherifam, N.; Naghdi, S.; Ahmadian, V.; et al. Digital Regulatory Governance: The Role of RegTech and SupTech in Transforming Financial Oversight and Administrative Capacity. *Int. J. Financial Stud.* **2025**, *13*, 217. [CrossRef]
18. Farahani, B.; Karimi Monsefi, A. Smart and Collaborative Industrial IoT: A Federated Learning and Data Space Approach. *Digit. Commun. Netw.* **2023**, *9*, 436–447. [CrossRef]
19. Soori, M.; Arezoo, B.; Dastres, R. Digital Twin for Smart Manufacturing, a Review. *Sustain. Manuf. Serv. Econ.* **2023**, *2*, 100017. [CrossRef]
20. Sajadieh, S.M.M.; Noh, S.D. A Review of Digital Twin Integration in Circular Manufacturing for Sustainable Industry Transition. *Sustainability* **2025**, *17*, 7316. [CrossRef]
21. Son, Y.H.; Kim, G.-Y.; Kim, H.C.; et al. Past, Present, and Future Research of Digital Twin for Smart Manufacturing. *J. Comput. Des. Eng.* **2022**, *9*, 1–23. [CrossRef]
22. El Mokhtari, K.; Panushev, I.; McArthur, J.J. Development of a Cognitive Digital Twin for Building Management and Operations. *Front. Built Environ.* **2022**, *8*, 856873. [CrossRef]
23. Suárez-Román, M.; Sanz-Rodrigo, M.; Marín-López, A.; et al. A Digital Twin Threat Survey. *Big Data Cogn. Comput.* **2025**, *9*, 252. [CrossRef]
24. Yigit, Y.; Bal, B.; Karameseoglu, A.; et al. Digital Twin-Enabled Intelligent DDoS Detection Mechanism for Autonomous Core Networks. *IEEE Commun. Stand. Mag.* **2022**, *6*, 38–44. [CrossRef]
25. Aghazadeh Ardebili, A.; Zappatore, M.; Ramadan, A.I.H.A.; et al. Digital Twins of Smart Energy Systems: A Systematic Literature Review on Enablers, Design, Management and Computational Challenges. *Energy Inform.* **2024**, *7*, 94. [CrossRef]
26. Schroeder, G.N.; Steinmetz, C.; Rodrigues, R.N.; et al. A Methodology for Digital Twin Modeling and Deployment for Industry 4.0. *Proc. IEEE* **2021**, *109*, 556–567. [CrossRef]
27. Usman, A.B.; Cole, N.; Asplund, M.; et al. Remote Attestation Assurance Arguments for Trusted Execution Environments. In Proceedings of the 2023 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Charlotte, NC, USA, 26 April 2023; pp. 33–42. [CrossRef]
28. Bathalapalli, V.K.V.V.; Mohanty, S.P.; Kougianos, E.; et al. PUFchain 4.0: Integrating PUF-Based TPM in Distributed Ledger for Security-by-Design of IoT. In Proceedings of the Great Lakes Symposium on VLSI 2023, Knoxville, TN, USA, 5–7 June 2023; pp. 231–236. [CrossRef]
29. Asaadi, E.; Denney, E.; Menzies, J.; et al. Dynamic Assurance Cases: A Pathway to Trusted Autonomy. *Computer* **2020**, *53*, 35–46. [CrossRef]
30. Wagner, P.G.; Beyerer, J. Quantifying Trustworthiness in Decentralized Trusted Applications. In Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Baltimore, MD, USA, 27 April 2022; pp. 67–76. [CrossRef]
31. Szpytko, J.; Salgado Duarte, Y. A Digital Twins Concept Model for Integrated Maintenance: A Case Study for Crane Operation. *J. Intell. Manuf.* **2021**, *32*, 1863–1881. [CrossRef]
32. Almeaibed, S.; Al-Rubaye, S.; Tsourdos, A.; et al. Digital Twin Analysis to Promote Safety and Security in Au-

tonomous Vehicles. *IEEE Commun. Stand. Mag.* **2021**, *5*, 40–46. [CrossRef]
33. Feng, K.; Ji, J.; Zhang, Y.; et al. Digital Twin-Driven Intelligent Assessment of Gear Surface Degradation. *Mech. Syst. Signal Process.* **2023**, *186*, 109896. [CrossRef]
34. Davies, O.; Makkattil, A.; Jiang, C.; et al. A Digital Twin Design for Maintenance Optimization. *Procedia CIRP* **2022**, *109*, 395–400. [CrossRef]
35. Soori, M.; Arezoo, B.; Dastres, R. Internet of Things for Smart Factories in Industry 4.0, a Review. *Internet Things Cyber-Phys. Syst.* **2023**, *3*, 192–204. [CrossRef]
36. Wagner, T.; Kittl, C.; Jakob, J.; et al. Digital Twins in Power Systems: A Proposal for a Definition. *IEEE Power Energy Mag.* **2024**, *22*, 16–23. [CrossRef]
37. Khan, L.U.; Saad, W.; Niyato, D.; et al. Digital-Twin-Enabled 6G: Vision, Architectural Trends, and Future Directions. *IEEE Commun. Mag.* **2022**, *60*, 74–80. [CrossRef]



Copyright © 2026 by the author(s). Published by UK Scientific Publishing Limited. This is an open access article under the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Publisher's Note: The views, opinions, and information presented in all publications are the sole responsibility of the respective authors and contributors, and do not necessarily reflect the views of UK Scientific Publishing Limited and/or its editors. UK Scientific Publishing Limited and/or its editors hereby disclaim any liability for any harm or damage to individuals or property arising from the implementation of ideas, methods, instructions, or products mentioned in the content.