DYNAMES
Dynamics in Engineering Systems: Innovations and Applications
DYNAMES 3(1): 20-39
ISSN 3048-2666

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

A design science research framework for continuous integrity verification of electronic data capture terminals using cryptographic tamper-evident enclosure and blockchain-based certification

Haqi Nuha Ahnafy[1],*
[1] *Bachelor's degree in veterinary medicine, Faculty of Veterinary Medicine, Universitas Airlangga, Surabaya, East Java 60115, Indonesia.*
*Correspondence: haqi.nuha.ahnafy-2024@fkh.unair.ac.id

Received Date: November 11, 2025 Revised Date: January 19, 2026 Accepted Date: February 28, 2026

ABSTRACT

Background: The expansion of digital payment infrastructure has increased the role of Electronic Data Capture (EDC) terminals as distributed transaction endpoints in merchant environments. Existing controls include device certification, encryption, secure boot, firmware signing, anti-tamper mechanisms, and transaction monitoring. However, EDC terminals may still face post-certification integrity risks, including physical tampering, firmware reflashing, device identity spoofing, runtime manipulation, and fragmented audit evidence. This study develops NEUROSHELL as a conceptual Design Science Research (DSR) artefact for continuous integrity condition monitoring of EDC terminals. In this article, physical-layer cybersecurity refers to the protection and monitoring of the terminal enclosure, tamper status, firmware state, cryptographic device identity, and certification status, rather than to generic hardware security alone. **Methods:** This study used a DSR approach based on problem identification, threat modelling, design requirement derivation, artefact construction, conceptual evaluation, and validation-pathway planning. Data sources included scholarly literature, regulatory documents, technical standards, cybersecurity reports, and conceptual design materials. The framework was evaluated conceptually through comparative analysis, mapping of security objectives and stakeholder governance, and analysis of implementation feasibility. **Findings:** The study produced NEUROSHELL as an integrated integrity assurance framework. It combines cryptographic tamper-evident enclosure, secure boot and firmware attestation, device-bound cryptographic identity, runtime integrity proof, blockchain-based certification ledger, dashboard-based monitoring, and risk-based fail-secure response. The framework is designed to support lifecycle verification across onboarding, boot-time activation, runtime operation, firmware updates, anomaly detection, and recovery. **Conclusion:** NEUROSHELL shifts EDC terminal security from static certification to lifecycle-based integrity assurance, but it remains a conceptual framework that requires prototype implementation, tamper-simulation testing, latency benchmarking, false-positive analysis, and expert validation. **Novelty/Originality of this article:** The novelty lies in unifying physical-layer protection, firmware assurance, cryptographic identity, runtime proof, privacy-preserving blockchain certification, dashboard monitoring, and fail-secure response into a continuous integrity verification framework for EDC terminals.

KEYWORDS: blockchain certification; design science research; device integrity verification; electronic data capture; physical-layer cybersecurity.

Cite This Article:
Ahnafy, H. N. (2026). A design science research framework for continuous integrity verification of electronic data capture terminals using cryptographic tamper-evident enclosure and blockchain-based certification. *Dynamics in Engineering Systems: Innovations and Applications, 3*(1), 20-39. https://doi.org/10.61511/dynames.v3i1.3765

1. Introduction

The rapid expansion of digital payment infrastructure has changed the security landscape of financial transactions. Digital payment systems increasingly operate in real time, across distributed channels, and through heterogeneous endpoint devices deployed outside the direct physical control of banks or payment system operators (Board of Governors of the Federal Reserve System, 2023). In Indonesia, this transformation is reflected in the continued growth of digital banking and electronic payments. Bank Indonesia projected that the value of digital banking transactions would reach Rp85,044 trillion in 2025, supported by a modern, secure, uninterrupted, and reliable payment system (Bank Indonesia, 2023). This growth indicates that payment security cannot be understood solely as a back-end infrastructure issue. It must also include the security of transaction endpoints that interact directly with customers, merchants, acquirers, and payment networks.

Electronic Data Capture (EDC) terminals are among the most important endpoint devices in the digital payment infrastructure. These devices operate at the point of interaction between customers and merchants, processing payment credentials, transaction commands, authentication flows, and communication with acquiring systems. The PCI PIN Transaction Security Point of Interaction standard emphasizes that point-of-interaction devices are used to protect cardholder personal identification numbers, account data, and other sensitive payment card data during payment transactions (PCI SSC, 2023). This position makes EDC terminals operationally critical but also structurally exposed. Unlike centralized banking systems, EDC terminals are physically distributed across merchant environments, handled by different operators, maintained by vendors or technicians, and exposed to diverse physical conditions (National Cybersecurity Center of Excellence, 2022).

Existing Electronic Data Capture terminal security practices commonly rely on a combination of device certification, secure boot, firmware signing, anti-tamper mechanisms, encryption, access control, transaction monitoring, and periodic compliance review (Payment Card Industry Security Standards Council, 2024). These controls remain necessary and should not be dismissed. However, they may still leave a post-certification integrity gap. A terminal that passed initial certification may later be exposed to physical tampering, unauthorized maintenance, component replacement, firmware reflashing, device identity misuse, or supply-chain compromise. This problem aligns with broader concerns in cybersecurity supply-chain risk management, where products and services may contain malicious functionality, counterfeit components, or vulnerabilities introduced during manufacturing, integration, delivery, or maintenance (NIST, 2024a). In distributed merchant environments, the challenge is not only whether a terminal was secure at the beginning of its lifecycle, but whether it remains verifiably secure during operation.

Firmware integrity is particularly important in this context. Platform firmware forms a foundational layer required to boot and operate a system. A successful attack on firmware may disrupt device operation, require reprogramming by the manufacturer, or lead to severe operational consequences (Regenscheid, 2018). NIST firmware resiliency guidance emphasizes mechanisms for protecting firmware from unauthorized changes, detecting unauthorized changes when they occur, and recovering rapidly and securely after compromise (Regenscheid, 2018). These principles are highly relevant to EDC terminals because firmware-level manipulation may occur below application-layer monitoring and may not be immediately visible through transaction-level fraud detection. As a result, EDC security should include mechanisms for continuous firmware-state verification, rather than just secure installation and periodic inspection.

Another limitation of conventional controls is the fragmented nature of audit evidence. Certification records, firmware logs, maintenance activities, and incident reports may be distributed across vendors, acquirers, merchants, banks, and auditors. This fragmentation weakens cross-actor visibility and may delay incident response (CPMI-IOSCO, 2022). National Institute of Standards and Technology Cybersecurity Framework 2.0 treats

cybersecurity governance, identification, protection, detection, response, and recovery as connected functions that should support risk management across organizational contexts (NIST, 2024b). Bank Indonesia Regulation Number 2 of 2024 similarly strengthens requirements for information system security and cyber resilience among payment system providers, money market and foreign exchange market participants, and other regulated parties (Bank Indonesia, 2024). These regulatory and governance directions indicate the need for payment-terminal security mechanisms that can produce verifiable evidence, support incident response, and strengthen auditability across stakeholders.

For the scope of engineering systems and monitoring-oriented research, EDC terminals can be interpreted as distributed cyber-physical endpoints whose trust state changes over time. Although this article does not examine vibration signatures, structural dynamics, or signal-based fault diagnosis, it frames terminal integrity as a condition-monitoring problem (the monitored state variables include tamper status, firmware baseline consistency, certificate validity, device-bound identity, runtime integrity proof, and operational risk mode). NEUROSHELL therefore contributes to integrity dynamics and lifecycle monitoring by linking condition changes in the terminal to risk-based operational responses such as trusted, suspicious, limited-operation, and blocked modes.

This study addresses the post-certification integrity gap by proposing NEUROSHELL, a design science framework for continuous integrity verification of EDC terminals. NEUROSHELL integrates a cryptographic tamper-evident enclosure, secure boot, firmware attestation, device-bound cryptographic identity, runtime integrity proof, a blockchain-based certification ledger, dashboard-based monitoring, and risk-based fail-secure response. The framework is not intended to replace existing payment security standards, fraud monitoring, or regulatory supervision. Instead, it provides an additional assurance layer focused on the physical-layer and firmware-layer integrity of EDC terminals after deployment.

A design science research approach is used because the problem is artefactual and socio-technical (the study does not merely describe an existing architecture, but derives and organizes a purposeful framework that connects technical controls, lifecycle evidence, certification logic, and stakeholder governance). DSR is therefore more appropriate than a purely technical architecture study for producing design knowledge, explicating design requirements, and positioning the framework as a conceptual artefact that can later be instantiated and empirically evaluated. The use of blockchain in NEUROSHELL is deliberately limited. Blockchain is not positioned as a payment processing system or as a repository for customer transaction data. Its function is restricted to certification and auditability by anchoring integrity-related hashes, certificate lifecycle metadata, firmware baseline references, renewal events, revocation status, and risk-state transitions. This limited use is important because blockchain can support tamper-evident shared records, but its implementation must avoid unnecessary privacy exposure, scalability burden, and operational complexity (Yaga et al., 2018). In NEUROSHELL, blockchain-based certification supports cross-actor verification while preserving the principle that sensitive payment and customer data should not be written to the ledger.

1.1 Literature synthesis and novelty gap

Existing integrity assurance approaches can be synthesized into several partially overlapping streams. Firmware resiliency and secure boot mechanisms focus on protecting, detecting, and recovering trusted firmware states, but they do not by themselves provide cross-actor certification visibility after deployment. Remote attestation and TPM/TEE-based device identity mechanisms support evidence-based verification of device state, yet they often remain component-level controls unless integrated with lifecycle governance and operational response. PCI PTS and related point-of-interaction security standards establish essential certification and protection requirements, but certification may become outdated when terminals are exposed to unauthorized maintenance, physical manipulation, or heterogeneous merchant practices after deployment. Blockchain-based auditability can

improve tamper-evident record sharing, but it does not directly solve firmware, enclosure, or runtime integrity verification unless constrained to certification metadata and integrity evidence.

The novelty gap addressed by NEUROSHELL is therefore integrative rather than component-inventive. Prior approaches tend to be component-based, pre-certification oriented, periodic rather than continuous, or insufficiently linked to distributed merchant environments. NEUROSHELL is positioned as a lifecycle assurance model that combines physical tamper evidence, firmware attestation, device-bound cryptographic identity, runtime proof, privacy-preserving blockchain certification, dashboard monitoring, and fail-secure response. This synthesis strengthens the scholarly positioning of the framework as a continuous integrity condition-monitoring approach for payment terminals rather than as a standalone hardware product, isolated attestation protocol, or generic blockchain application.

The research gap addressed in this study is therefore as follows- existing EDC security approaches remain insufficient in providing continuous, auditable, and cross-actor integrity verification after initial certification. Current controls may protect the device at installation, validate firmware at boot, or monitor transactions at the fraud-detection layer, but they do not necessarily integrate physical tamper evidence, firmware attestation, cryptographic device identity, runtime proof, certification auditability, and risk-based response into one lifecycle assurance framework. This gap is critical because EDC terminals operate in distributed environments where physical inspection is difficult to scale, vendor heterogeneity complicates standardization, and post-deployment compromise may remain unnoticed until fraud or operational disruption occurs.

Accordingly, this study aims to develop NEUROSHELL as a conceptual cybersecurity artifact for continuous integrity verification of EDC terminals. The study is guided by four research questions (1) What physical-layer and firmware-layer threats create post-certification integrity risks for EDC terminals in digital payment infrastructure? (2) What design requirements are needed to support continuous, auditable, and cross-actor integrity verification of EDC terminals? (3) How can NEUROSHELL integrate cryptographic tamper-evident enclosure, device-bound identity, runtime integrity proof, and blockchain-based certification into a unified framework? (4) What are the expected security improvements, governance implications, implementation challenges, and future validation needs of the proposed framework?

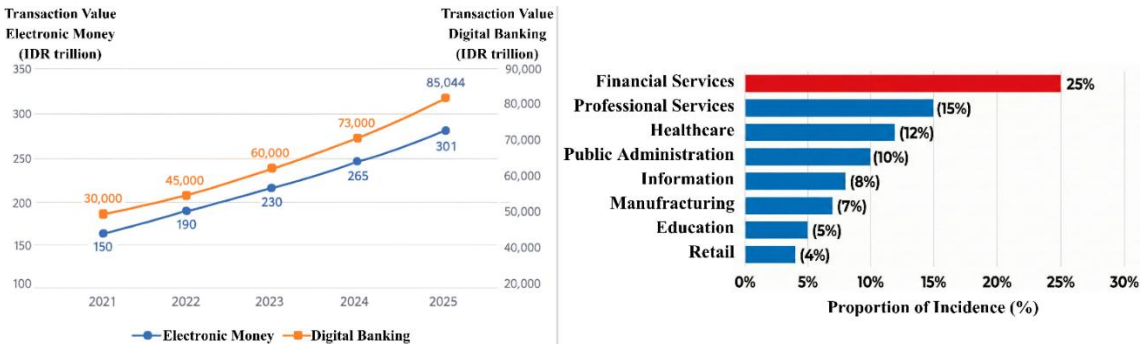

Fig. 1. Indonesia's digital transaction growth trends and composition of global cyber incidents in the financial sector, 2021-2025.
(Bank Indonesia, 2025; Verizon, 2025).

This study contributes to cybersecurity in digital payments in four ways. First, it shifts the discussion of payment terminal security from static certification to lifecycle-based integrity assurance. Second, it develops NEUROSHELL as an original design science artefact that integrates physical-layer protection, firmware assurance, device identity, runtime proof, and certification auditability. Third, it proposes a privacy-preserving blockchain certification model that records integrity evidence without storing customer transaction data. Fourth, it provides a governance-oriented implementation perspective involving

acquirers, merchants, vendors, banks, auditors, and regulators. Through these contributions, the article positions NEUROSHELL as a conceptual foundation for future prototype testing, expert validation, tamper simulation, and pilot implementation in selected merchant environments

2. Methods

2.1 Research design

This study employed a design science research approach to develop NEUROSHELL as a conceptual cybersecurity artefact for continuous integrity verification and condition-based monitoring of Electronic Data Capture (EDC) terminals in the digital payment infrastructure. DSR was selected because the research problem requires the construction of a purposeful artefact that links engineering-system monitoring logic, cybersecurity controls, certification evidence, and stakeholder governance. Unlike a technical architecture study that primarily specifies components, this study derives design requirements from the problem context and evaluates the conceptual coverage of the proposed artefact. Design science research is appropriate for studies that aim to construct, evaluate, and communicate artefacts as research contributions for addressing technological and organizational problems (Baskerville et al., 2018; Delport et al., 2024; vom Brocke et al., 2020). In this study, the artefact refers to the proposed NEUROSHELL framework, which integrates a cryptographic tamper-evident enclosure, device-bound identity, runtime integrity proofs, blockchain-based certification, dashboard-based monitoring, and risk-based fail-secure responses.

The research process consisted of six main stages (problem identification, threat modelling, design requirement derivation, artefact construction, conceptual evaluation, and validation-pathway planning). This structure was adapted from contemporary design science research and action design research perspectives, which emphasize the movement from problem formulation to artefact creation, evaluation, reflection, learning, and communication of design knowledge (Delport et al., 2024; Mullarkey et al., 2019; vom Brocke et al., 2020). Problem identification identified the post-certification security gap affecting EDC terminals as distributed physical endpoints in merchant environments. Threat modelling identified protected assets, threat actors, attack vectors, potential impacts, and corresponding control needs. Design requirement derivation translated these threats into technical and governance-oriented requirements. Artefact construction produced the conceptual architecture and operational workflow of NEUROSHELL. Conceptual evaluation assessed the framework through comparative analysis, security objective mapping, stakeholder governance analysis, and implementation feasibility indicators. Validation-pathway planning explicitly defined the empirical work still required before the framework can be claimed as operationally effective.

2.2 Research object

The research object of this study is the integrity assurance of EDC terminals as physical transaction endpoints within the digital payment infrastructure. These terminals are treated as critical point-of-interaction devices because they operate at the interface among merchants, customers, acquirers, banks, and payment system operators. As such, point-of-interaction devices are expected to protect cardholder PINs, account data, and other sensitive payment card data during transactions (PCI SSC, 2023). Moreover, the increasing exposure of financial institutions to cyber risk underscores that endpoint integrity is not merely a technical issue, but also one of financial-sector resilience and trust (IMF, 2024).

Despite such focus, EDC terminals are commonly protected through certification, encryption, secure boot, firmware signing, anti-tamper mechanisms, and operational monitoring, but they may still face post-deployment risks such as physical tampering, firmware reflashing, hardware modification, device identity spoofing, and persistent

manipulation. Firmware and platform-level compromise are particularly relevant because platform firmware forms part of the fundamental hardware-firmware layer required to boot and operate a system, and unauthorized modification at this level may create serious operational disruption (Regenscheid, 2018). Secure software and firmware lifecycle practices are also relevant because secure development, update validation, and vulnerability reduction are necessary to reduce exploitable weaknesses in deployed systems (Souppaya et al., 2022).

The design object of this study is NEUROSHELL, a proposed cybersecurity framework intended to strengthen the physical-layer and firmware-layer integrity of EDC terminals. Rather than replacing existing payment security controls, NEUROSHELL is positioned as an additional assurance layer. Specifically, its primary functions are to support continuous device integrity verification from boot-time activation to transaction runtime; manage the certification lifecycle; notify of anomalies; generate audit trails; and apply risk-based operational restrictions when the terminal shows signs of compromise.

2.3 Data sources and collection procedure

This study used secondary data sources, including scholarly literature, regulatory documents, technical standards, cybersecurity reports, and the author's conceptual design materials. This diverse use of secondary sources aligns with design science research, as artefact development requires problem-domain, solution-domain, and design knowledge to justify design decisions and evaluate relevance (Baskerville et al., 2018; Delport et al., 2024; vom Brocke et al., 2020). Furthermore, literature review methodology supports structured synthesis, which consolidates fragmented knowledge and derives conceptual insight for a specific problem area (Page et al., 2021; Snyder, 2019).

Documents were identified through five thematic domains (digital payment infrastructure, EDC or point-of-sale terminal security, physical-layer and hardware-based cybersecurity, cryptographic device identity and firmware integrity, and blockchain-based certification or audit-trail mechanisms). Sources were included when they addressed payment terminal security, device integrity, cyber resilience in financial infrastructure, hardware tamper protection, secure boot, firmware assurance, device attestation, blockchain-based certification, auditability, or governance of digital payment security. Regulatory documents, industry standards, and institutional cybersecurity reports were included when they provided relevant context for payment system governance, certification, cyber resilience, payment security, or financial-sector threat exposure (Bank Indonesia, 2024; European Payments Council, 2024; IMF, 2024; NIST, 2024a; NIST, 2024b; PCI SSC, 2023). The document identification process was thematic and purposive rather than a PRISMA-based systematic review; this limitation is acknowledged because the objective was conceptual artefact development rather than exhaustive evidence synthesis.

The author's conceptual design materials were also used as internal design inputs for the construction of the NEUROSHELL artefact. These materials included the initial NEUROSHELL mechanism, conceptual layer architecture, dashboard design, end-to-end workflow, input-output diagram, use-case mapping, comparative analysis, stakeholder mapping, SMART indicators, PESTEL analysis, and PDCA-based implementation considerations. These materials were not treated as empirical validation data, but as preliminary artefact components that were reorganized and refined through the design science process.

2.4 Analytical procedure

The analysis was conducted in five sequential stages. The first stage was problem analysis, which examined how EDC terminals may become vulnerable after initial certification due to physical exposure, heterogeneous merchant environments, vendor fragmentation, firmware lifecycle risks, and limited continuous visibility into device integrity. This stage was supported by cybersecurity risk and cyber-resilience perspectives,

which emphasize the need to understand, assess, prioritize, communicate, and manage cybersecurity risks across technical and organizational contexts (NIST, 2024b; Ross et al., 2021). The second stage was threat modelling. This stage mapped protected assets, threat actors, attack vectors, potential impacts, and required controls associated with EDC terminal integrity. Protected assets included terminal hardware, enclosures, firmware, boot sequences, cryptographic keys, device identity, transaction interfaces, integrity logs, and certification records. Threat actors included advanced persistent threat actors, malicious technicians, compromised vendors, rogue merchant insiders, counterfeit device operators, and attackers with temporary physical access to the device. The selection of these categories was informed by the literature on cyber-resilience engineering, supply-chain risk management, firmware resiliency, and hardware security (NIST, 2024a; Regenscheid, 2018; Ross et al., 2021; Vidaković & Vinko, 2023).

The third stage was the derivation of design requirements. Each identified threat was translated into one or more design requirements. The requirements emphasized continuous verification, tamper-evident protection, cryptographic binding between device identity and firmware state, runtime integrity proof, blockchain-based certification, privacy-preserving auditability, risk-based fail-secure response, vendor-neutral interoperability, and governance accountability across payment actors. These requirements were derived by connecting threat analysis with design science principles and cybersecurity outcome frameworks (Baskerville et al., 2018; NIST, 2024b; vom Brocke et al., 2020). The fourth stage was artefact construction. This stage developed NEUROSHELL as a conceptual framework comprising a cryptographic tamper-evident enclosure, an anti-tamper sensing layer, a device-bound identity, secure boot and firmware attestation, a session-based integrity proof, a blockchain-based certification ledger, dashboard-based monitoring and orchestration, and a risk-based operational response. In design science research, artefact construction is central because the research contribution is expressed through a designed solution to a relevant problem (Baskerville et al., 2018; Delport et al., 2024; vom Brocke et al., 2020).

The fifth stage was conceptual evaluation. NEUROSHELL was evaluated through four lenses (comparative evaluation, security objective mapping, stakeholder governance mapping, and implementation feasibility analysis). Comparative evaluation compared NEUROSHELL with conventional EDC security controls, including static certification, periodic inspection, secure boot, firmware signing, anti-tamper mechanisms, transaction-level fraud monitoring, and fragmented audit documentation. Security objective mapping assessed how the framework supports integrity, authenticity, traceability, auditability, privacy preservation, and operational resilience. Stakeholder governance mapping examined the distribution of responsibility among acquirers, merchants, vendors, banks, payment system operators, auditors, and regulators. The implementation feasibility analysis considered vendor heterogeneity, costs, merchant readiness, metadata privacy, key management complexity, false-positive risk, transaction continuity, dashboard governance, and regulatory coordination. This conceptual evaluation does not establish measured detection accuracy, false-positive rates, transaction latency overhead, or operational effectiveness.

2.5 Threat modelling and design requirement derivation

The threat modelling procedure served as an analytical bridge between problem identification and the derivation of design requirements. In design science research, requirements should be grounded in a clear understanding of the problem environment, ensuring the resulting artefact addresses relevant and well-defined risks (Baskerville et al., 2018; Delport et al., 2024). The procedure also followed cybersecurity risk management logic, in which assets, threats, vulnerabilities, impacts, and controls are linked to support risk-informed design decisions (NIST, 2024b; Ross et al., 2021).

The identified threats were translated into design requirements for continuous integrity verification, cryptographic tamper-evident enclosure, device-bound identity,

secure boot and firmware attestation, runtime integrity proof, privacy-preserving blockchain certification, risk-based fail-secure response, dashboard-based monitoring, key lifecycle governance, interoperability, and cross-actor governance mapping. The blockchain component was deliberately limited to certification and auditability functions, especially anchoring integrity-related proofs and certification metadata rather than storing customer transaction data. This decision reflects blockchain security literature that recognizes blockchain's relevance for integrity, auditability, identity management, and verifiable records while also acknowledging challenges related to scalability, privacy, and operational overhead (Regueiro & Urquizu, 2025; Shujaa et al., 2025; Wang et al., 2025).

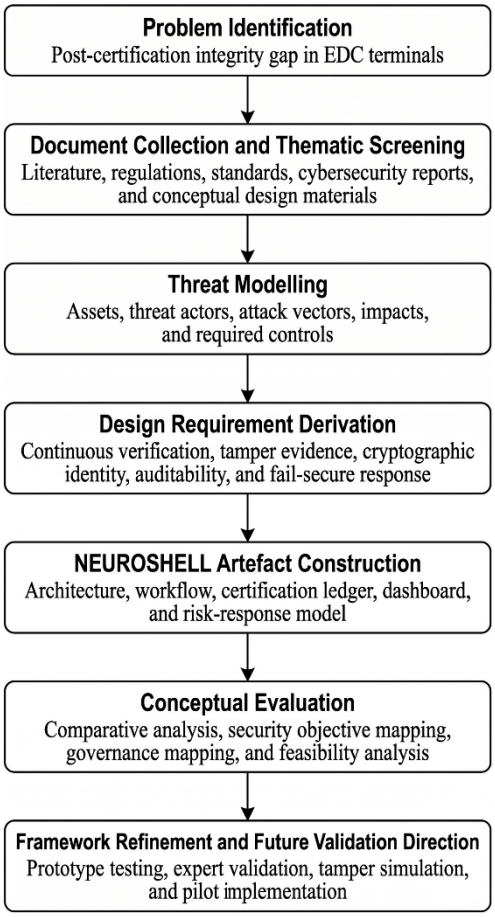

Fig. 2. Research design and analytical procedure for developing NEUROSHELL as a conceptual design science artefact and future validation pathway.

2.6 Methodological limitations

This study is limited to conceptual artefact development and does not include laboratory implementation, prototype testing, sensor-level validation, expert-panel review, empirical measurement of detection accuracy, false-positive or false-negative estimation, or transaction latency benchmarking. Therefore, the proposed NEUROSHELL framework should be interpreted as a design science contribution that provides a structured conceptual basis for future technical validation rather than as a fully implemented and empirically verified system. This limitation is consistent with design science research, where conceptual artefacts may be developed and evaluated at an early stage before being extended into prototype implementation, stakeholder validation, simulation, or field deployment (Delport et al., 2024; Mullarkey et al., 2019; vom Brocke et al., 2020).

The study also relies on secondary sources and author-generated conceptual analysis. It did not apply a PRISMA-based systematic literature review, Delphi validation, structured expert review, controlled tamper-simulation testing, or performance benchmarking. As a result, the effectiveness of NEUROSHELL in detecting physical tampering, preventing

firmware compromise, reducing fraud, improving operational resilience, or limiting transaction latency cannot be claimed as empirically proven within the scope of this article. Future research should develop a prototype, conduct controlled tamper-simulation tests, evaluate false-positive and false-negative rates, measure transaction latency and blockchain certification overhead, assess key lifecycle security controls, conduct expert validation, and test implementation feasibility through pilot deployment in selected merchant environments.

3. Results and Discussion

3.1 Threat model of EDC terminals in digital payment infrastructure

Electronic Data Capture (EDC) terminals operate as point-of-interaction devices within the digital payment infrastructure. Their security relevance extends beyond transaction execution, as they also serve as distributed physical endpoints exposed to merchant environments, maintenance activities, firmware updates, and potential post-deployment manipulation. The PCI PIN Transaction Security Point of Interaction standard emphasizes the need to protect cardholder PINs, account data, and sensitive payment card data at the point of interaction (PCI SSC, 2023). Therefore, EDC terminal security should include not only transaction-level protection but also device integrity assurance across the terminal lifecycle.

The threat model in this study focuses on post-certification compromise. A terminal may pass initial certification but later become exposed to physical tampering, firmware reflashing, key extraction, identity spoofing, runtime manipulation, or audit-record alteration. This focus is consistent with firmware resiliency guidance, which emphasizes protection against unauthorized firmware changes, detection of compromise, and recovery to a trusted state (Regenscheid, 2018). It is also aligned with the hardware security literature, which shows that electronic devices may be exposed to invasive and non-invasive attacks, including physical probing, tampering, side-channel observation, and fault injection (Vidaković & Vinko, 2023).

Table 1 indicates that the integrity problem with EDC terminals is not confined to a single technical layer. Physical compromise may enable component manipulation; firmware compromise may persist below application-level monitoring; identity compromise may allow cloned or modified devices to appear legitimate; runtime compromise may affect transaction sessions; and weak audit evidence may delay forensic response. Therefore, NEUROSHELL is designed to address EDC terminal security as a continuous lifecycle integrity problem rather than a one-time certification problem.

Based on this threat model, the study derives six core design requirements. These requirements connect the identified threats with the expected security properties of the proposed NEUROSHELL framework. The remote attestation literature supports the principle that a verifier can assess the state of a device based on evidence generated by the device being verified, which is relevant to session-based integrity proofs in distributed terminal environments (Kuang et al., 2022).

The NIST Cybersecurity Framework 2.0 also emphasizes governance, identification, protection, detection, response, and recovery as core cybersecurity functions, supporting the need for a framework that connects technical verification with operational response (NIST, 2024b). The six requirements in Table 2 can be grouped into four design clusters (terminal-level integrity assurance, cryptographic trust and device identity, privacy-preserving certification auditability, and governance-oriented operational control). These requirements form the foundation of NEUROSHELL as an integrated framework for continuous EDC terminal integrity verification.

Table 1. Threat model of EDC terminal integrity

Protected asset	Potential threat actor	Attack vector	Potential security impact	Required security control
EDC physical enclosure and internal components	Physical attacker, malicious technician, rogue merchant insider	Unauthorized casing opening, component replacement, hardware implant, or probe insertion	Loss of physical integrity, insertion of skimming or surveillance components, and persistent compromise at the transaction endpoint	Tamper-evident enclosure, anti-tamper sensor, automatic risk-status update, and fail-secure device response
Firmware and boot sequence	APT actor, compromised vendor, malicious maintenance operator	Unauthorized firmware reflashing, boot image manipulation, malicious firmware update, or persistent backdoor insertion	Compromised transaction logic, unauthorized terminal behavior, and persistence below the application layer	Secure boot verification, firmware signing validation, baseline comparison, and post-update re-attestation
Cryptographic keys and device credentials	Advanced attacker, malicious technician, hardware-level adversary	Key extraction, side-channel probing, insecure key storage, or credential cloning	Device impersonation, unauthorized transaction authorization, and weakening of cryptographic trust	Secure key storage, device-bound identity, periodic key rotation, and challenge-response verification
Runtime device integrity	APT actor, physical attacker, insider threat	Runtime tampering, abnormal sensor signals, fault injection, glitch manipulation, or sensor bypass attempt	Undetected compromise during transaction processing and delayed incident response	Continuous runtime monitoring, anomaly-triggered integrity proof, risk-based restriction, and dashboard alerting
Certification and compliance lifecycle	Compromised vendor, negligent acquirer, fragmented merchant network	Static certification, outdated compliance status, inconsistent inspection, or delayed revocation	Post-certification blind spot and inability to detect devices that become unsafe after deployment	Continuous certification-status update, automated certificate renewal or revocation, and risk-based compliance monitoring

Note: Unit of analysis: post-certification EDC terminal integrity across physical, firmware, cryptographic identity, runtime, and certification states.

(PCI SSC, 2023; Regenscheid, 2018; Kuang et al., 2022; Vidaković & Vinko, 2023; NIST, 2024b)

3.2 Proposed NEUROSHELL framework

NEUROSHELL is proposed as an integrated framework for continuous integrity verification of Electronic Data Capture (EDC) terminals. The framework is designed to address the post-certification integrity gap identified in Section 3.1 by integrating physical

tamper-evidence, firmware assurance, device-bound cryptographic identity, runtime integrity proofs, blockchain-based certification, dashboard monitoring, and risk-based response. NEUROSHELL does not replace existing payment security standards, fraud monitoring systems, or regulatory supervision. Instead, it functions as an additional assurance layer focused on the physical-layer and firmware-layer integrity of EDC terminals after deployment.

Table 2. Design requirements for the NEUROSHELL framework

Code	Core design requirement	Rationale	Expected design output
DR1	Continuous lifecycle integrity verification	EDC terminals should not be trusted only because they passed initial certification, since compromise may occur after deployment.	Verification mechanism across onboarding, booting, runtime operation, firmware update, and recovery
DR2	Tamper-evident physical and firmware assurance	Physical tampering and firmware compromise may alter terminal behavior below conventional monitoring layers.	Tamper-evident enclosure, anti-tamper sensing, secure boot, firmware attestation, and trusted baseline comparison
DR3	Device-bound cryptographic identity and session proof	Each terminal must be distinguishable from cloned, modified, counterfeit, or uncertified devices during operational sessions.	Cryptographic identity binding device ID, firmware state, certificate status, nonce-based proof, and signed integrity evidence
DR4	Privacy-preserving blockchain certification ledger	Certification records must be auditable and tamper-evident without exposing customer or transaction data.	Ledger storing integrity hashes, certification metadata, baseline references, renewal events, and revocation status
DR5	Risk-based fail-secure response	A terminal showing integrity degradation should not continue normal operation without restriction.	Safe, suspicious, limited-operation, and blocked modes with session locking, key suspension, and inspection workflow
DR6	Dashboard-based governance and interoperability	Continuous verification requires visibility and coordination across acquirer, merchant, vendor, bank, auditor, and regulator.	Monitoring dashboard, standardized device-status taxonomy, role-based access, escalation workflow, and interoperable certification protocol

Note. Unit of analysis: design requirements derived from the post-certification EDC terminal threat model and lifecycle assurance objectives.
(PCI SSC, 2023; Regenscheid, 2018; Kuang et al., 2022; Vidaković and Vinko, 2023; and NIST, 2024b)

The main assumption underlying NEUROSHELL is that an EDC terminal should not be considered trustworthy merely because it has passed initial certification. In distributed merchant environments, a terminal may later be exposed to unauthorized maintenance, casing manipulation, component replacement, firmware modification, device cloning, or other forms of post-deployment compromise. This assumption is consistent with the role of point-of-interaction devices in protecting cardholder PINs, account data, and sensitive payment data during payment transactions (PCI SSC, 2023). It is also aligned with firmware resiliency guidance, which emphasizes the need to protect firmware from unauthorized modification, detect compromise, and recover to a trusted state (Regenscheid, 2018).

Fig. 3 illustrates NEUROSHELL as a layered integrity assurance architecture. The first layer is the cryptographic tamper-evident enclosure, which treats the EDC terminal's physical body as part of the security boundary. This layer is intended to detect or indicate unauthorized casing opening, component manipulation, physical probing, or attempts to implant hardware. The hardware security literature shows that electronic devices may be

exposed to both invasive and non-invasive attacks, including probing, side-channel analysis, fault injection, and physical tampering; therefore, protection should begin at the device level (Vidaković & Vinko, 2023).

Fig. 3. Conceptual architecture of the NEUROSHELL framework, showing physical, firmware, identity, certification, monitoring, and response layers.

Building upon the initial layer, the second layer is firmware assurance through secure boot and firmware attestation. This layer verifies whether the terminal starts from an authorized boot sequence and whether its firmware state remains consistent with the registered baseline. Firmware assurance is critical because firmware compromise may persist below application-layer monitoring and alter terminal behavior before transaction-level controls identify an anomaly. In NEUROSHELL, firmware state is linked to certificate status, and any firmware update must be followed by re-attestation and baseline renewal.

The third layer is device-bound cryptographic identity and runtime integrity proof. Specifically, each terminal must produce verifiable evidence that it is the same certified device and that its operational state remains acceptable during transaction sessions. This logic relates to remote attestation, in which a verifier assesses the state of a device based on evidence generated by the device itself (Kuang et al., 2022). In NEUROSHELL, such evidence may include certificate validity, a firmware baseline reference, a tamper-status summary, a nonce-based session proof, and a signed integrity status. Overall, NEUROSHELL should be understood as an integrity assurance framework rather than as a standalone hardware product or a generic blockchain application. Its contribution lies in integrating physical tamper-evidence, firmware attestation, device-bound identity, runtime proof, blockchain certification, dashboard monitoring, and risk-based response into a single continuous verification model for EDC terminals.

3.3 NEUROSHELL operational workflow and fail-secure response

The operational workflow of NEUROSHELL translates the proposed framework into a lifecycle-based verification process for Electronic Data Capture (EDC) terminals. First, the workflow begins with device onboarding, during which an acquirer or authorized vendor registers the terminal's identity, firmware version, hardware profile, certificate status, and deployment context. This onboarding establishes the initial trust relationship between the physical terminal, its cryptographic identity, and its certification record. As point-of-interaction devices are expected to protect sensitive payment data during payment transactions, terminal onboarding represents a critical part of the payment security boundary rather than a purely administrative process (PCI SSC, 2023).

After onboarding, NEUROSHELL creates a hardware-firmware baseline. This baseline includes the expected firmware state, boot configuration, device identity reference, certificate status, and tamper-indicator profile. During boot-time verification, the terminal is checked against this baseline before it enters normal transaction mode. This stage is important because platform firmware is part of the foundational layer required to boot and operate a system, and unauthorized firmware modification may compromise device trust

before application-level controls detect abnormal behavior (Regenscheid, 2018). If a firmware update occurs, NEUROSHELL requires source validation, signature checking, post-update attestation, and baseline renewal before the terminal is restored to trusted operation.

During runtime operation, the terminal continuously monitors tamper indicators and generates a session-based integrity proof. The proof may include certificate validity, a firmware baseline reference, a tamper-status summary, a nonce-based challenge-response, and signed integrity evidence. This mechanism is conceptually related to remote attestation, in which a verifier assesses the state of a device based on evidence generated by the device itself (Kuang et al., 2022). If the integrity proof is valid, the terminal may continue normal operation. If the proof is incomplete, inconsistent, or suspicious, the terminal enters a risk-based response mode.

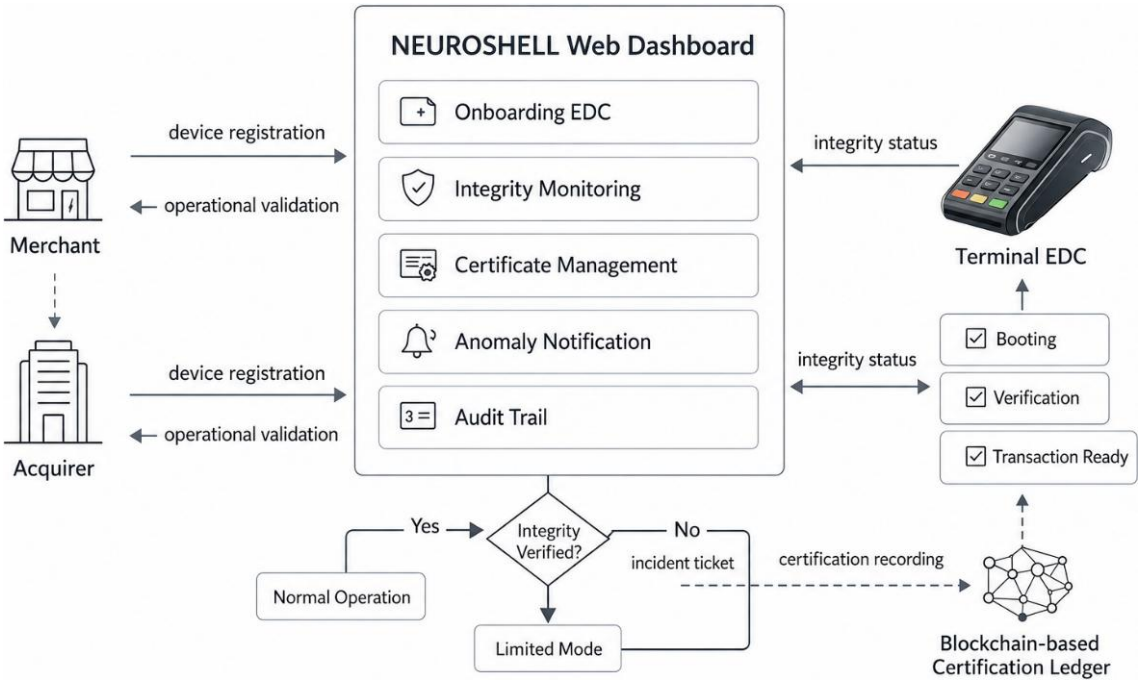

Fig. 4. End-to-end integrity verification workflow of NEUROSHELL from onboarding and runtime proof to certification recording and risk-based response.

The fail-secure response ensures that a terminal with degraded integrity does not continue operating as if it were trusted. Instead of applying a simple trusted-or-untrusted decision, NEUROSHELL uses four operational modes (trusted, suspicious, limited-operation, and blocked). This structure allows the system to distinguish between minor anomalies, medium-risk inconsistencies, and confirmed compromise. It also supports the cybersecurity functions of detection, response, recovery, and governance emphasized in the NIST Cybersecurity Framework 2.0 (NIST, 2024b). The workflow shows that NEUROSHELL is not only a detection mechanism. It connects onboarding, baseline registration, boot-time verification, runtime proof, certification recording, risk-based restriction, and recovery into one operational chain. This allows EDC terminal security to move from static certification toward continuous, auditable, and response-oriented integrity assurance.

3.4 Comparative evaluation against existing EDC security controls

Existing EDC security controls generally rely on device certification, secure boot, firmware signing, anti-tamper protection, transaction monitoring, and periodic compliance review. These controls remain important because point-of-interaction devices are expected to protect cardholder PINs, account data, and sensitive payment card data during payment transactions (PCI SSC, 2023). However, the main limitation identified in this study is that

many controls are still oriented toward initial approval, vendor-side protection, or transaction-level monitoring rather than continuous post-deployment integrity verification.

Table 3. Risk-based operational modes in NEUROSHELL

Operational mode	Trigger condition	System response	Required follow-up
Trusted mode	Valid device identity, trusted firmware baseline, active certificate, and normal tamper status	Allow normal transaction operation and record integrity status	Routine monitoring and certificate renewal
Suspicious mode	Minor inconsistency, unusual sensor signal, delayed attestation, or incomplete verification evidence	Require additional verification, increase logging, and notify the dashboard	Acquirer or vendor reviews the anomaly
Limited-operation mode	Repeated anomaly, firmware baseline warning, certificate-status uncertainty, or medium-risk integrity issue	Restrict selected operations, suspend sensitive functions, and require re-attestation	Technical inspection, re-baselining, or certificate update
Blocked mode	Strong tamper evidence, firmware mismatch, revoked certificate, identity spoofing, or confirmed compromise	Lock session, suspend cryptographic operation, block transaction capability, and isolate the device	Mandatory inspection, recovery, recertification, or device withdrawal

Note. Unit of analysis: operational integrity state transitions of an EDC terminal under NEUROSHELL governance.

(PCI SSC, 2023; Regenscheid, 2018; Kuang et al.,2022; and NIST, 2024b)

NEUROSHELL does not replace existing EDC controls. Instead, it extends them by integrating physical tamper evidence, firmware attestation, device-bound identity, runtime integrity proof, blockchain-based certification, and risk-based response into a single continuous assurance model. This is relevant because firmware compromise may require mechanisms for protection, detection, and recovery (Regenscheid, 2018), whereas remote attestation enables a verifier to assess a device's state based on evidence generated by the device itself (Kuang et al., 2022). Blockchain is used only as a certification ledger because distributed ledgers can support tamper-evident shared records when applied to appropriate trust problems (Yaga et al., 2018).

The comparison indicates that NEUROSHELL's contribution is not a single new control, but the conceptual integration of existing security logic into a continuous integrity assurance chain. Conventional controls remain necessary, but they may leave a post-certification gap when physical tampering, firmware modification, or identity misuse occurs after deployment. NEUROSHELL addresses this gap by specifying how critical terminal states, physical condition, firmware baseline, device identity, certificate validity, runtime proof, and risk mode can be made verifiable and auditable. This comparison should be read as an assessment of conceptual coverage rather than empirical superiority, since the framework has not yet been benchmarked for detection accuracy, false-positive rates, transaction latency, or scalability. The model supports the NIST Cybersecurity Framework 2.0 emphasis on governance, detection, response, and recovery as connected cybersecurity functions (NIST, 2024b).

3.5 Governance, implementation feasibility, and future validation

Implementing NEUROSHELL requires governance coordination because EDC terminal integrity is not under the control of a single actor. Acquirers are responsible for device onboarding, baseline registration, certificate management, monitoring, and incident

escalation. Vendors are responsible for ensuring firmware compatibility, secure update mechanisms, and device-level integration. Merchants are responsible for physical supervision, anomaly reporting, and compliance with inspection procedures. Banks, auditors, and regulators require visibility into certification status, audit records, and recovery actions. This governance logic aligns with cybersecurity frameworks that treat governance, identification, protection, detection, response, and recovery as interconnected functions rather than isolated technical controls (NIST, 2024).

Table 4. Comparative evaluation of conventional EDC controls and NEUROSHELL

Security dimension	Conventional EDC controls	Main limitation	NEUROSHELL contribution
Device certification	Initial device approval and periodic compliance review	Certification may become outdated after deployment	Converts certification into lifecycle-based integrity status
Firmware protection	Secure boot and firmware signing	Often focused on boot or update validation, not continuous operational proof	Links firmware baseline, attestation, certificate status, and runtime verification
Physical tamper control	Anti-tamper mechanism and manual inspection	Response may depend on delayed inspection or fragmented reporting	Connects tamper evidence to risk-status update and fail-secure operation
Audit trail	Logs and compliance documentation	Records may be fragmented across actors and difficult to verify	Anchors integrity hashes and certificate events in a blockchain-based certification ledger
Operational response	Fraud monitoring and incident handling after anomaly detection	Focus may remain transaction-level, not device-integrity-level	Applies trusted, suspicious, limited-operation, and blocked modes based on terminal integrity

Note. The comparison indicates conceptual coverage and design integration; it does not represent empirical superiority, measured detection accuracy, or verified latency performance.

(PCI SSC, 2023; Regenscheid, 2018; Kuang et al., 2022; Yaga et al., 2018; and NIST, 2024b)

In the Indonesian payment system context, NEUROSHELL is also relevant to the regulatory direction of cyber resilience. Bank Indonesia Regulation Number 2 of 2024 requires regulated payment-system actors to strengthen information system security and cyber resilience, including governance, risk management, incident handling, and supervision (Bank Indonesia, 2024). Building on these requirements, NEUROSHELL can be positioned as a technical-operational framework that supports evidence-based compliance by producing device integrity records, certificate status, anomaly chronology, and recovery evidence. From an implementation perspective, the main feasibility issues include vendor heterogeneity, integration cost, key management complexity, metadata privacy, merchant readiness, false-positive handling, and transaction continuity. These constraints indicate that NEUROSHELL should not be deployed immediately across all merchants. A more feasible strategy is a risk-based rollout, starting with high-volume merchants, critical payment locations, or terminals with greater physical access exposure. This gradual implementation can reduce operational disruption while allowing acquirers and vendors to test baseline formats, attestation procedures, dashboard workflows, and certificate lifecycle management.

Several engineering and governance trade-offs must be considered before implementation. Stronger integrity assurance may increase device-side computation, certificate checking, dashboard orchestration, and network communication. Similarly, blockchain-based auditability can strengthen tamper-evident certification records but may introduce operational overhead, ledger governance complexity, and latency if not restricted to lightweight integrity metadata. For this reason, NEUROSHELL should avoid writing

customer data or high-frequency transaction details to the ledger and should instead anchor compact integrity hashes, baseline references, certificate events, and risk-state transitions.

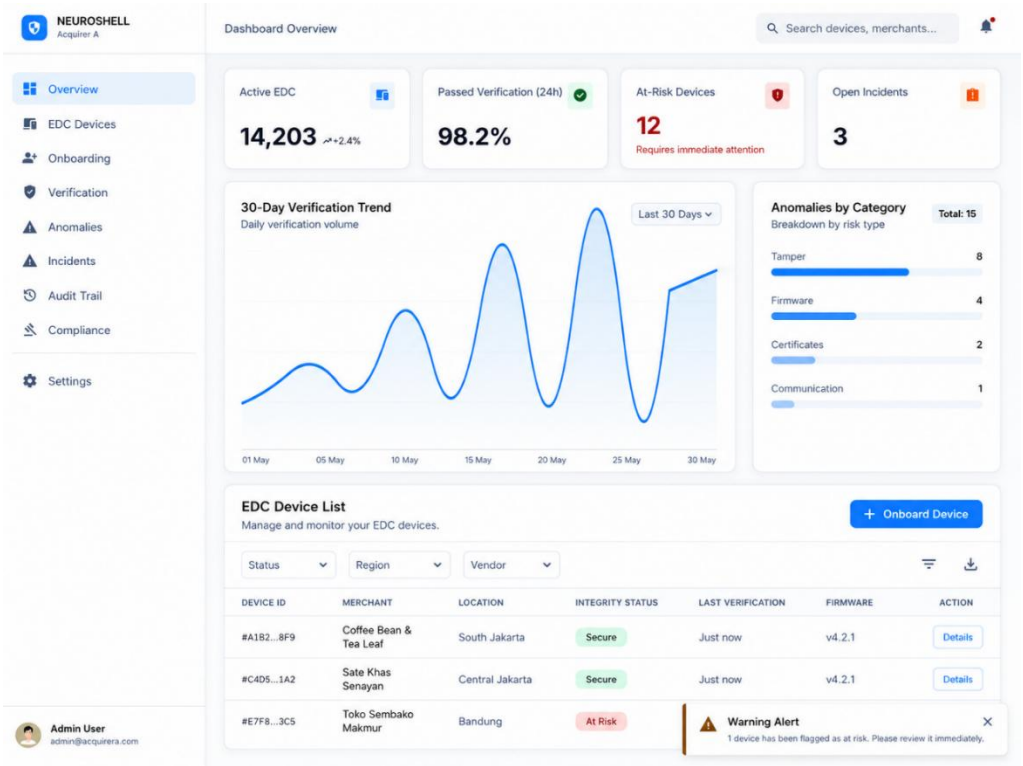

Fig. 5. NEUROSHELL web dashboard mock-up for device integrity monitoring, anomaly notification, audit trail visibility, and stakeholder coordination.

Scalability also depends on vendor interoperability, key lifecycle management, merchant readiness, and false-positive handling. A false tamper alert can unnecessarily restrict a legitimate terminal, while an overly permissive threshold can allow compromised devices to remain active. The framework therefore requires calibrated risk thresholds, role-based dashboard access, certificate revocation procedures, recovery workflows, and clear responsibility boundaries among acquirers, merchants, vendors, payment networks, auditors, and regulators. These issues reinforce the need for staged validation before full-scale deployment.

Future validation is necessary because this study develops NEUROSHELL as a conceptual design science artefact rather than an empirically tested system. A future validation pathway should include at least six stages, (1) prototype implementation of the tamper-evident enclosure, firmware attestation, device-bound identity, and dashboard modules; (2) controlled tamper-simulation testing to examine physical-opening, sensor-bypass, component-modification, and firmware-reflashing scenarios; (3) firmware attestation testbed evaluation to measure baseline consistency and recovery behavior; (4) transaction latency and blockchain certification overhead benchmarking under realistic merchant workloads; (5) false-positive and false-negative assessment under normal maintenance and abnormal tamper conditions; and (6) structured expert validation, such as Delphi review or a cybersecurity-engineering expert panel, followed by pilot deployment across heterogeneous EDC vendors. Accordingly, NEUROSHELL should be understood as a structured conceptual basis for future technical testing and policy-aligned implementation, not as a fully proven operational product.

4. Conclusions

This study developed NEUROSHELL as a design science framework for continuous integrity verification of Electronic Data Capture (EDC) terminals in the digital payment

infrastructure. The study shows that EDC terminal security should not be treated only as a matter of initial certification, transaction encryption, or periodic inspection. Since EDC terminals operate as distributed physical endpoints in merchant environments, they remain exposed to post-deployment risks, including casing tampering, firmware reflashing, device identity spoofing, runtime manipulation, and fragmented audit evidence. To address this post-certification integrity gap, NEUROSHELL integrates cryptographic tamper-evident enclosure, secure boot and firmware attestation, device-bound cryptographic identity, runtime integrity proof, blockchain-based certification ledger, dashboard-based monitoring, and risk-based fail-secure response.

The theoretical contribution of NEUROSHELL lies in its integrated lifecycle assurance model, design requirements, operational modes, conceptual architecture, and comparative framework coverage. It provides a way to conceptualize EDC terminals as cyber-physical engineering endpoints whose integrity condition changes over time and can be monitored through physical, firmware, cryptographic, certification, and runtime state variables. In this sense, the framework extends condition-monitoring logic toward cyber-physical system integrity assurance without claiming to address vibration-based or structural-health monitoring.

However, the claims of this article remain conceptual. The study does not demonstrate empirical effectiveness, detection accuracy, transaction latency, scalability, false-positive control, or prototype feasibility. Future research should instantiate NEUROSHELL in a laboratory prototype, perform tamper-simulation and firmware-attestation testing, benchmark certification and transaction latency, validate the framework through expert review, and evaluate pilot implementation across heterogeneous merchant and vendor environments. These steps are necessary before NEUROSHELL can be positioned as an operationally validated integrity assurance system.

Acknowledgement

The author would like to acknowledge the academic and institutional support received during the preparation of this manuscript. The author also appreciates the opportunity provided through the journal submission voucher awarded as part of the essay competition prize, which encouraged the development of the initial essay into a journal article.

Author Contribution

The sole author contributed to the conceptualization, methodology, formal analysis, investigation, resources, writing original draft preparation, writing review and editing, visualization, and project administration of this study. The author has read and approved the final version of the manuscript.

Funding

This research received no external research funding. If applicable, the article submission process was supported by a journal submission voucher awarded as part of the essay competition prize. The voucher provider had no role in the conceptualization, methodology, analysis, or writing of the manuscript, or in the decision to submit the article for publication.

Ethical Review Board Statement

Not available.

Informed Consent Statement

Not available.

Data Availability Statement

Not available.

Conflicts of Interest

The author declares no conflict of interest.

Declaration of Generative AI Use

During manuscript preparation and revision, ChatGPT (GPT-5.5 Thinking, OpenAI) was used to support language refinement, structural editing, clarity improvement, and reviewer-response organization. The author reviewed, verified, revised, and approved all AI-assisted outputs and remains fully responsible for the scholarly content, analysis, interpretations, citations, and conclusions of the manuscript.

Open Access

References

Ankergård, S. F. J. J., Dushku, E., & Dragoni, N. (2021). State-of-the-art software-based remote attestation: Opportunities and open issues for Internet of Things. *Sensors, 21*(5), Article 1598. https://doi.org/10.3390/s21051598

Bank Indonesia. (2023). *Bank Indonesia Annual Meeting 2023: Synergy strengthening national economic resilience and revival*. https://www.bi.go.id/en/iru/highlight-news/Pages/Bank-Indonesia-Annual-Meeting-2023-Synergy-Strengthening-National-Economic-Resilience-and-Revival.aspx

Bank Indonesia. (2024). *Bank Indonesia Regulation Number 2 of 2024 on information system security and cyber resilience for payment system providers, money market and foreign exchange market participants, as well as other parties regulated and supervised by Bank Indonesia.* https://www.bi.go.id/en/publikasi/peraturan/Pages/PBI_022024.aspx

Bank Indonesia. (2025). *Laporan Kelembagaan Bank Indonesia Triwulan III - 2025*. https://www.bi.go.id/id/publikasi/laporan/Pages/LKBI-Tw.III-2025.aspx

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: Finding a balance between artifact and theory. *Journal of the Association for Information Systems, 19*(5), 358–376. https://doi.org/10.17705/1jais.00495

Board of Governors of the Federal Reserve System. (2023). *Cybersecurity and financial system resilience report*. https://www.federalreserve.gov/publications/files/cybersecurity-report-202308.pdf

CPMI-IOSCO. (2022). *Implementation monitoring of the PFMI: Level 3 assessment on financial market infrastructures' cyber resilience*. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD723.pdf

Delport, P. M. J., Von Solms, R., & Gerber, M. (2024). Methodological guidelines for design science research. *Procedia Computer Science, 237,* 195–203. https://doi.org/10.1016/j.procs.2024.05.096

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

European Payments Council. (2024). *2024 payments threats and fraud trends report* (EPC162-24, Version 1.0). https://www.europeanpaymentscouncil.eu/

IMF. (2024). *Global financial stability report, April 2024: Cyber risk: A growing concern for macrofinancial stability.* https://www.imf.org/

Kuang, B., Fu, A., Susilo, W., Yu, S., & Gao, Y. (2022). A survey of remote attestation in Internet of Things: Attacks, countermeasures, and prospects. *Computers & Security, 112*, 102498. https://doi.org/10.1016/j.cose.2021.102498

Mullarkey, M. T., Hevner, A. R., & Ågerfalk, P. J. (2019). An elaborated action design research process model. *European Journal of Information Systems, 28*(1), 6–20. https://doi.org/10.1080/0960085X.2018.1451811

National Cybersecurity Center of Excellence. (2022). Validating the integrity of computing devices (NIST Special Publication 1800-34). *National Institute of Standards and Technology*. https://doi.org/10.6028/NIST.SP.1800-34

NIST. (2024a). *Cybersecurity supply chain risk management practices for systems and organizations* (NIST Special Publication 800-161 Revision 1, Update 1). https://doi.org/10.6028/NIST.SP.800-161r1-upd1

NIST. (2024b). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29).* https://doi.org/10.6028/NIST.CSWP.29

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., & Moher, D. (2021). *The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372*, Article n71. https://doi.org/10.1136/bmj.n71

PCI SSC. (2024). *Payment Card Industry Data Security Standard: Requirements and testing procedures, version 4.0.1*. https://www.pcisecuritystandards.org/

PCI SSC. (2023). *PTS Point of Interaction (POI).* https://www.pcisecuritystandards.org/standards/pts-point-of-interaction-poi/

Regenscheid, A. R. (2018). Platform firmware resiliency guidelines (NIST Special Publication 800-193). *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.SP.800-193

Regueiro, C., & Urquizu, B. (2025). Blockchain-based evidence trustworthiness system in certification. *Journal of Cybersecurity and Privacy, 5*(1), Article 1. https://doi.org/10.3390/jcp5010001

Ross, R., Pillitteri, V. Y., Graubart, R., Bodeau, D., & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach (NIST Special Publication 800-160, Volume 2, Revision 1). *National Institute of Standards and Technology.* https://doi.org/10.6028/NIST.SP.800-160v2r1

Shujaa, W., Alanzi, M., & Sankaranarayanan, S. (2025). Enhancing IoT security through blockchain integration. *Frontiers in Computer Science, 7*, 1670473. https://doi.org/10.3389/fcomp.2025.1670473

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104,* 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Souppaya, M., Scarfone, K., & Dodson, D. (2022). *Secure Software Development Framework (SSDF) version 1.1: Recommendations for mitigating the risk of software vulnerabilities (NIST Special Publication 800-218).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-218

Verizon. (2025). *Verizon 2025 Data Breach Investigations Report.* https://www.verizon.com/business/resources/reports/dbir/

Vidaković, M., & Vinko, D. (2023). Hardware-based methods for electronic device protection against invasive and non-invasive attacks. *Electronics, 12*(21), Article 4507. https://doi.org/10.3390/electronics12214507

vom Brocke, J., Hevner, A., & Maedche, A. (2020). Introduction to design science research. In J. vom Brocke, A. Hevner, & A. Maedche (Eds.), Design Science Research. *Cases* (pp. 1–13). Springer. https://doi.org/10.1007/978-3-030-46781-4_1

Wang, W., Yan, B., Chai, B., Shen, R., Dong, A., & Yu, J. (2025). EBIAS: ECC-enabled blockchain-based identity authentication scheme for IoT device. *High-Confidence Computing, 5*(1), Article 100240. https://doi.org/10.1016/j.hcc.2024.100240

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview (NIST Interagency/Internal Report 8202).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Biographies of Author

Haqi Nuha Ahnafy, is a veterinary medicine undergraduate student at Universitas Airlangga, Surabaya, Indonesia. His academic interests include digital payment security, cybersecurity governance, financial technology, blockchain-based certification, and cyber resilience in digital financial infrastructure. His current research focuses on developing NEUROSHELL as a conceptual framework for continuous integrity verification of Electronic Data Capture terminals.

- Email: haqi.nuha.ahnafy-2024@fkh.unair.ac.id
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A