Evolution of Remote Attestation: A Systematic Literature Review of Post-2020 Approaches

Florian Wegscheider[1,*,†], Tobias Hilbig[1,†] and Thomas Schreck[1,†]

[1]Munich University of Applied Sciences HM, Munich, Germany

Abstract

Device attestation is a critical component of Zero Trust Architecture (ZTA), where access decisions depend on the integrity of device health signals. While hardware-anchored Remote Attestation (RA) offers stronger cryptographic assurances than self-reported telemetry, its adoption in ZTA remains limited. To assess the current state of the field, we conducted a Systematic Literature Review (SLR) of RA research published between 2020 and 2025. We consider 110 peer-reviewed publications from five major digital libraries, and relevant standardization documents. Our analysis categorizes RA schemes along five dimensions: root of trust, evidence type, evidence gathering, verification, and scalability. Our results indicate a clear shift toward hybrid root of trust architectures leveraging commodity hardware features, a proliferation of scalable swarm attestation protocols driven by Internet of Things (IoT) growth, and the emergence of machine learning as a verification technique for dynamic evidence. Privacy preservation has also emerged as a prominent new design requirement not addressed in prior reviews. On the standardization front, RFC 9334 (Remote ATtestation procedureS, RATS) has matured into a foundational framework. However, significant gaps remain in enterprise Bring Your Own Device (BYOD) environments, heterogeneous infrastructure, and the integration of RA claims into identity and access management frameworks.

Keywords

Systematic Literature Review, Zero Trust Architecture, Device Attestation, Remote Attestation

1. Introduction

The adoption of Zero Trust (ZT) principles has redefined information security by enforcing a strict "Never trust, always verify" paradigm [1]. In this model, every access request is evaluated based on a computed trust score that is derived from multiple context signals. The strength of user authentication and the health status of the requesting device are considered to be of primary importance. The robustness of a ZTA is, therefore, directly proportional to the reliability of these signals.

While the industry has successfully implemented high-assurance methods for user verification, e.g., FIDO2-based passkeys [2], the methods for verifying device health often lack comparable maturity. Device attestation approaches for office IT environments typically rely on support by the operating system, while Mobile Device Management solutions are employed for portable devices. Information collected through these systems usually covers static data such as hardware and firmware details and dynamically collected, runtime-dependent context data. However, software-based reporting mechanisms are inherently susceptible to manipulation. In the presence of a compromised operating system, monitoring software may be forced to report an apparently healthy state. As a result, access control decisions may be based on falsified telemetry, thereby undermining one of the core ZTA tenets [1].

To elevate the integrity of device health telemetry, the source of evidence must shift to a hardware-anchored Root of Trust (RoT). RA facilitates this shift through secure hardware elements such as Trusted Platform Modules (TPMs) [3] that generate verifiable reports on the internal state of the device. Through such procedures, access decisions can be based on verifiable measurements rather than self-reported data. Implementing RA therefore allows organizations to align device verification with the high-assurance principles commonly applied to user identity.

4th International Workshop on Trends in Digital Identity (TDI 2026), April 20–21, 2026, Verona, Italy

*Corresponding author.

†These authors contributed equally.

florian.wegscheider@hm.edu (F. Wegscheider); tobias.hilbig@hm.edu (T. Hilbig); thomas.schreck@hm.edu (T. Schreck)

0009-0000-5609-2862 (F. Wegscheider); 0000-0002-2904-4758 (T. Hilbig); 0000-0002-8960-6986 (T. Schreck)

© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

This study aims to investigate how research on device attestation approaches, including RA procedures, has developed in the past five years. To ensure a comprehensive coverage of the topic, we also include works by standardization bodies in addition to academic literature in our review. To that end, we consider the following research questions:

- **RQ1:** How did research of remote attestation approaches develop between 2020 and 2025?
- **RQ2:** How did standardization efforts for remote attestation progress between 2020 and 2025?
- **RQ3:** Which remote attestation approaches fulfill the requirements of zero trust environments?

To the best of our knowledge, the latest SLR on remote attestation was published by Johnson et al. in 2021 [4], with a focus on attestation in embedded systems. Their study covers approaches published between 2003 and 2020 and proposes a novel taxonomy that decomposes the attestation process into five fundamental dimensions. In addition, the authors provide a cost-benefit analysis for each dimension and introduce an enhanced threat model that allows assessing the level of compromise a RA solution is able to protect against. Building directly upon this foundation, we extend their work by considering RA schemes published from 2020 onwards, and also adopt and extend their taxonomic framework for analysis and classification. More targeted SLRs have also been conducted in recent years, for instance on RA solutions for IoT devices [5], on software-based RA [6], and on wireless networks [7]. While our third research question targets the applicability of RA approaches in ZTAs, this SLR is not confined to a specific domain or application. However, we employed specific exclusion criteria to only consider academic works that provide novel insights into RA approaches as detailed in Section 3. An updated review of the literature is therefore necessary due to: (1) the rapid proliferation of IoT devices, prime candidates for RA; (2) the vast number of academic works on the topic published in recent years; and (3) advancements in standardization [3].

The main contribution of our work is a comprehensive review of recent research on remote device attestation. Our results show a clear shift toward hybrid root of trust architectures, a proliferation of scalable swarm attestation protocols, and the emergence of verification techniques based on Machine Learning (ML). On the standardization front, the Internet Engineering Task Force (IETF) Remote ATtestation ProcedureS (RATS) architecture [3] has reached Request for Comment (RFC) status. This paper is organized as follows: We provide background information on ZTA and RA in Section 2 and detail our methodology in Section 3. Structured along our taxonomy, we present the results of our SLR in Section 4. We answer and discuss our research questions in Section 5 and conclude with Section 6.

2. Background

To contextualize our research, we provide background information on ZTA and RA in the following.

2.1. Zero Trust Architecture

The widespread adoption of BYOD policies, remote work arrangements, and cloud-based services has effectively dissolved the traditional network perimeter, rendering classic perimeter-based security approaches increasingly inadequate. Where such approaches rely on separating assets into distinct trust zones, the boundaries of modern enterprise networks are no longer well-defined. Conceived over 20 years ago, ZTA has emerged as a new enterprise network security paradigm and can be summarized by the principle “Never trust, always verify” [1]. Rather than trusting entities based on their network location, ZTA enforces access control decisions at each individual asset: no entity is granted access to a resource without explicit authentication and authorization. To this end, access decisions are governed by a comprehensive access policy, evaluated by Policy Decision Points (PDPs) that incorporate contextual data, e.g., user identity, authentication strength, and device integrity status.

Research on ZTA is well established and has progressed considerably in recent years. Buck et al. conducted a comprehensive literature review on the topic, also covering grey literature in the process [8]. The concept has been also successfully implemented by major organizations in the past, with Google [9]

and Microsoft [10] offering mature solutions. Specialized frameworks for specific use-cases have also emerged, e.g., in healthcare [11] and for federated learning [12]. Finally, the concept was formalized by the National Institute of Standards and Technology (NIST) in Special Publication 800-207 [1].

2.2. Device Attestation

Device attestation is the process by which trust in devices is established and verified [3]. Beyond mere identification, attestation enables the collection of evidence about a device's current state. For instance, this can include the software being executed, firmware integrity, and group policy compliance, all of which can be incorporated into access policy decisions by a PDP. When this process is initiated by a remote party that also receives and evaluates the collected evidence, it is referred to as RA. A central challenge in RA is preventing attestation statements from being tampered with by a compromised device. Hardware-based solutions such as TPMs and Trusted Execution Environments (TEEs) can serve this purpose. A TEE is an isolated processing environment that provides confidentiality and integrity guarantees for code and data. By anchoring the attestation process within such an environment, the integrity of the collected evidence can be cryptographically assured.

3. Methodology

This research utilizes a SLR design to consolidate current knowledge on RA with a focus on the applicability of RA within ZTAs. To ensure a comprehensive, reproducible, and unbiased review, the systematic components of this review adhere to the guidelines proposed by Kitchenham and Charters [13]. We executed our search in October 2025 and considered five primary digital libraries: IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Scopus. Additionally, the dataset was complemented with relevant technical standards and working drafts identified through the IETF Datatracker to capture the most recent state of practice. For technical standards, we conducted a specialized quality assessment to evaluate the authority of the producing body and the objectivity of the technical contribution as suggested by Garousi et al. [14]. Our approach aligns with the rapid evolution of standards, where technical specifications often emerge in parallel with academic publications.

3.1. Search Strategy

The initial search strategy utilized the specific term remote attestation. However, preliminary analysis indicated that many publications, particularly those predating the 2023 RATS standard, utilized broader terminology. Consequently, the search string was refined to include attestation in combination with keywords such as trust or integrity to capture mechanisms described using older nomenclature. This refinement necessitated a manual filtering process to exclude results from domains other than information technology, such as those pertaining to notary services or legal attestations. Furthermore, approaches primarily relying on distributed ledger technology or blockchain were excluded at this stage, as terminology in this field frequently overlaps with RA without offering specific architectural contributions to the attestation mechanisms. The complete list of search strings and their library-specific variations is provided in Appendix A.

3.2. Inclusion and Exclusion Criteria

Candidate publications were evaluated against specific quality and relevance criteria to filter the search results. Inclusion was limited to peer-reviewed publications and recognized technical papers written in English that are applicable for implementation within ZTAs. As our study is built upon an existing review from 2021 [4], we only included works published between 2020 and 2025. Exclusions were applied to purely formal proofs lacking system implementation details, proposals focusing solely on hardware design, and applications of RA unrelated to ZT, such as isolated supply chain security or software bill of materials generation. Finally, works proposing the generic integration of ML models into

attestation flows without specific architectural novelty were removed. The selection process followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) [15] flow and involved four distinct phases consisting of identification, screening, eligibility, and inclusion. The full selection process is visualized in Figure 1 in Appendix B.

This review is subject to several methodological limitations: First, the screening and selection of publications was conducted by a single reviewer, which introduces the risk of subjective bias. Second, the restriction to English-language may have excluded publications in other languages. While representing the most authoritative standardization body in this domain, the inclusion of grey literature was limited to the IETF, which could exclude potentially relevant reports from other organizations.

3.3. Classification Taxonomy

To ensure a systematic and rigorous analysis of the selected literature, this study adopts the taxonomy established by Johnson et al. [4]. While the original work focuses on embedded systems, the structural decomposition of the attestation process offers a generalized logical framework. The authors consider five distinct, interconnected problems of attestation for their taxonomy.

The first dimension is the RoT, which serves as the security foundation of any attestation scheme. Within this dimension, RoTs are classified as software-based when they rely on techniques such as hypervisor isolation, memory integrity monitoring, or timing-based verification to protect the evidence collection process without dedicated hardware. They are classified as hardware-based if they employ dedicated security components that physically isolate attestation functionality from the main processor, ensuring immutable and attack-resistant evidence generation even in the presence of a compromised operating system. A hybrid classification applies when schemes leverage commodity hardware features like TEEs or TPMs to combine hardware-level isolation with the flexibility and upgradability of software-based approaches. The second and third dimensions address the nature of evidence and its collection method. The taxonomy distinguishes between static evidence, which comprises immutable data such as binaries and configuration files, and dynamic evidence, which captures volatile system states such as the contents of memory. These are paired with the collection frequency, categorized as either discrete for capturing a system snapshot at a specific point in time, or continuous for providing ongoing monitoring over a defined duration. The final dimensions concern verification methods and network scalability. While the foundational taxonomy categorizes verification into whitelist, control-flow graph, and data-flow graph methods, recent literature necessitates the expansion of these categories to include probabilistic and behavioral verification techniques driven by ML. Scalability is assessed based on the network topology, categorizing schemes into one-to-one, many-to-one, or many-to-many architectures.

3.4. Applicability to Zero Trust Architectures

Although the taxonomy was derived from a review of embedded systems, its application to non-embedded devices typically found in ZTAs, such as laptops, servers, and cloud instances, is justified by the following three reasons: First, the classification of RoTs is directly transferable to enterprise hardware. The taxonomy's definition of a hybrid RoT encompasses standard commodity hardware features like Intel SGX and TPMs. These components are ubiquitous in modern non-embedded devices, meaning the classification criteria regarding trust anchors apply equally to IoT sensors and enterprise workstations. Second, the distinction between discrete and continuous evidence gathering aligns with the core principles of a ZTA. The taxonomy highlights that discrete collection methods are vulnerable to Time-of-Check-to-Time-of-Use (TOCTOU) attacks, where malware evades detection by modifying the system state between checks. By categorizing approaches that utilize continuous monitoring, the framework supports the ZT requirement for real-time health verification of endpoints. Finally, the taxonomy addresses heterogeneity and scalability in a manner consistent with diverse network environments. This is a prerequisite for a ZTA, which must secure a mix of legacy systems, modern servers, and employee devices.

4. Results

This section presents the results from our SLR. We consider each of the five dimensions and the characteristics proposed in previous work separately [4]. Furthermore, our evaluation and categorization of the entire synthesized corpus is provided in Table 1 in Appendix C.

4.1. Root of Trust

Our investigation indicates that research in RA has shifted toward architectures utilizing a hybrid RoT. While purely software-based and hardware-based approaches remain actively researched, their applicability is increasingly bound to specific operational environments. Current literature suggests that the prevalence of hybrid models stems from their ability to balance the flexibility of software with the security guarantees of hardware [16, 17, 18, 19]. For instance, schemes like SAPEM [18] utilize ARM TrustZone to secure the attestation process without requiring custom, purpose-built co-processors, thereby maintaining compatibility with widely deployed IoT microcontrollers. Similarly, MATEE [20] proposes an approach that establishes two distinct chains of trust, one via Intel SGX and another via a TPM, mitigating the risk of a single point of compromise. The prevalence of this architecture suggests a shift away from a binary choice between expensive hardware and insecure software, settling on a middle ground where trusted firmware leverages privilege levels to isolate the attestation logic [21, 17, 18].

Despite the dominance of hybrid models, purely software-based attestation remains relevant for two use cases: legacy devices [22, 23, 19] and ultra-low-end microcontrollers [24, 19]. SIMPLE [19] demonstrates that software-based RA is necessary for resource-constrained devices that lack Memory Protection Units (MPUs), using a formally verified software RoT to bridge the gap for very low-resource embedded devices. Furthermore, RealSWATT [22] justifies the use of software-based attestation in real-time systems by arguing that traditional attestation routines interrupt normal operations, which violates critical timing constraints. To avoid this interference, RealSWATT leverages a dedicated processor core on the embedded device to run the software-based prover continuously in the background.

Conversely, advancements in purely hardware-based RoTs have evolved structurally beyond traditional secure co-processors to increasingly focus on Physical Unclonable Functions (PUFs). Protocols like PAMA [25] and PISA [26] utilize PUFs not only for device identification but to anchor the entire attestation protocol, aggregating responses over multi-hop networks without storing sensitive secrets on the device. Overall, this trend indicates a transition toward hardware RoT that are tied to the silicon itself, exemplified by PUFs, as opposed to add-on security components such as TPMs [26, 27].

4.2. Evidence

Evidence is classified into two primary categories: static and dynamic. Static evidence consists of immutable information about the object under attestation, such as executable binaries and software configurations, which typically do not change over the device's lifetime. Dynamic evidence captures the current operational state and runtime behavior of the attestation target.

4.2.1. Static Evidence

Static attestation evidence is predominantly derived from cryptographic measurements of firmware or memory regions, forming the basis of trusted boot and integrity verification mechanisms [28, 18, 29, 30]. Alladi et al. propose a lightweight authentication scheme in which the evidence consists of a hash of the checksums over selected memory blocks, which are validated by edge servers [27].

In architectures incorporating TPMs, Khurshid and Raza present AutoCert, which extends the rudimentary generation of signed Platform Configuration Registers (PCRs) by introducing a software-bound Integrity Key [30]. While standard schemes simply transmit measurements via a TPM Quote structure to prove boot integrity, AutoCert cryptographically seals the private portion of the Integrity Key to these PCR values. This binding ensures that the key becomes inaccessible if the device's state changes after the initial check, thereby mitigating TOCTOU attacks. Similarly, Jäger et al. rely on TPMs

to anchor the Linux Integrity Measurement Architecture (IMA), with evidence consisting of a boot log and an IMA log protected by hardware-signed quotes [31].

To address scalability challenges in large-scale and swarm-based IoT deployments, several approaches replace raw cryptographic digests with compressed or probabilistic data structures. Frontera and Lazzeretti employ Bloom filters as static evidence, where devices encode their integrity status into a bit array, enabling a verifier to estimate the proportion of compromised devices while minimizing communication overhead [32]. For decentralized environments that require proofs of code possession, Gamboni-Diehl et al. utilize Merkle trees, generating it over the set of deployed code files, which allows devices to prove the presence of correct software components without transmitting binaries [33].

Another line of work focuses on privacy preservation by decoupling integrity evidence from device identity. Bai et al. introduce ZKSA [34], which leverages zero-knowledge proofs to produce evidence in the form of a proof that confirms consistency between the device's software state and a Merkle root without disclosing the underlying software contents or enabling unauthorized identification [34].

4.2.2. Dynamic Evidence

Dynamic attestation mechanisms primarily focus on verifying the runtime behavior of software by observing its execution characteristics [18, 35]. A common approach is control-flow attestation, which reconstructs or validates the execution path of a program [36]. Neto and Nunes present ISC-FLAT [37], in which the attestation evidence consists of an authenticated control-flow log that accumulates the destination addresses of branch instructions, enabling the verifier to reconstruct the executed control-flow path. To address the combinatorial growth of valid execution paths in complex software, Chilese et al. propose transforming execution traces into graph embeddings that are analyzed using graph neural networks, allowing the verifier to classify executions without relying on exact hash matching [36].

To reduce the overhead associated with instrumenting control-flow instructions, several works leverage hardware performance counters as a proxy for execution integrity. Gonzalez-Gomez et al. introduce LightFAt [38], where the attestation evidence consists of performance monitor unit traces, such as instructions per cycle and cache access counts, which collectively form a characteristic fingerprint of program execution and are analyzed through ML. Similarly, Li Calsi and Zaccaria employ a vector of hardware event counters as attestation evidence to support interruptible attestation while ensuring that no unauthorized code executes during interrupt handling [39].

An alternative class of dynamic attestation approaches relies on fingerprinting the data state of volatile memory rather than tracking instruction-level behavior. Iqbal et al. propose using raw snapshots of RAM as attestation evidence, which are analyzed by ML techniques to detect anomalies caused by firmware modifications or runtime compromises [21]. Extending this concept to distributed environments, Kohli et al. analyze SRAM traces across device swarms using graph neural networks, allowing the detection of compromise propagation effects between communicating nodes [40].

Finally, several approaches treat the device as a black box and derive evidence from physical or behavioral side channels. Delgado-Lozano et al. utilize power consumption traces captured via analog-to-digital converters, which serve as execution signatures that can be compared against reference profiles [41]. Chen et al. apply a similar principle to programmable logic controllers by using neural networks to model the expected behavior of the software. Instead of modeling the physical process, they train a model to predict the actuator commands based on observed sensor inputs, utilizing discrepancies between the predicted and actual commands as evidence to detect unauthorized modifications [42].

4.3. Gathering

Evidence gathering refers to the methodology employed to acquire attestation evidence from the target device, distinct from the subsequent packaging and transmission of those results. We categorize these mechanisms into discrete and continuous gathering.

4.3.1. Discrete Gathering

Discrete gathering mechanisms capture the state of an attester at a specific instance, typically triggered by a request from a verifier, establishing a challenge-response interaction where the verifier initiates the process to examine the device's internal state [43, 18]. This model usually involves measuring static memory contents or configuration snapshots at the moment of the request. However, recent advancements have introduced privacy-preserving techniques to this gathering process. To address privacy concerns, Kassem et al. propose PRIVÉ [44], a scheme based on Direct Anonymous Attestation (DAA) that facilitates the gathering of evidence to prove the integrity of a swarm while concealing the identities of individual devices. By leveraging DAA credentials and zero-knowledge proofs, PRIVÉ ensures that the identity of honest devices remains anonymous to the verifier, providing traceability and linkability only when a compromise is detected or a specific device causes an attestation failure. Additionally, Bai et al. introduce ZKSA [34], which utilizes zero-knowledge proofs for mutual gathering, allowing devices to verify each other without revealing their configuration. ZKSA enables decentralized verification where devices generate proofs based on non-interactive zero-knowledge protocols, ensuring that the software state remains confidential and is not disclosed during the gathering process.

Furthermore, innovations have been proposed to handle interrupts and intermittent availability during the discrete gathering process. Sponziello et al. introduce ITERATOR [45], a protocol that transforms the traditional memory hash calculation into a series of set membership queries using a Cuckoo filter. By dividing the memory into blocks and associating them with a pre-built Cuckoo filter, ITERATOR allows the gathering process to be performed in multiple independent rounds, enabling the device to handle interrupts between rounds without compromising security. Similarly, Rabbani et al. propose RESERVE [46], a protocol specifically designed for intermittent IoT devices that rely on energy harvesting. RESERVE abandons the execution assumption by organizing the device software into modules and performing discrete checks on as many modules as the current energy budget permits. It utilizes checkpoints to bridge the gap between active and sleep modes, ensuring that the gathering process can span across power cycles while maintaining a probability of detecting modifications.

4.3.2. Continuous Gathering

Continuous gathering mechanisms are designed to provide a persistent or high-frequency view of the device's state, addressing the limitations of discrete snapshots. A primary focus in this domain is the efficient collection of runtime behavior. Li Calsi and Zaccaria propose an interruptible gathering mechanism that utilizes hardware performance counters. This approach allows the device to pause the heavy cryptographic checksumming of memory to handle interrupts, while the performance counters continuously gather execution metrics to ensure no malicious code runs during the interruption [39]. Similarly, Zhan et al. introduce a granularity-adaptive mechanism that balances security benefits and performance overheads. To resolve the specific scope of measurement, they utilize the Non-dominated Sorting Genetic Algorithm-II to generate a division strategy, assigning fine-grained, basic-block-level monitoring to security-critical core functions, while restricting noncore functions [47].

In the realm of asynchronous and event-driven architectures, gathering mechanisms have evolved to decouple evidence generation from verification. Dushku et al. propose SARA [48], which gathers evidence of service interactions in a distributed manner. Devices continuously attach attestation tokens to their asynchronous messages, allowing a verifier to trace the propagation of potential compromises through the service chain. Building on this, Dushku et al. introduce PROVE [49], which leverages a publish-subscribe model where publishers act as attesters. Evidence is continuously published to a log storage and protected by a one-way key chain, enabling subscribers to retrospectively gather and verify the integrity of the data source without direct interaction [49].

For virtualized and cloud-edge environments, Wang et al. propose a bottom-up active gathering scheme. Instead of waiting for a verifier's challenge, the virtual machine monitor actively collects trusted chain information from virtual machines and pushes the encrypted evidence to a verification service, ensuring timely detection of anomalies [50].

4.4. Verification

The verification phase constitutes the appraisal process where the verifier evaluates the trustworthiness of the attester based on the gathered evidence.

4.4.1. Whitelist

Whitelist verification remains the predominant mechanism for static attestation. In this model, the received evidence, which typically consists of a cryptographic hash representing the binary state, is compared against a database of known good values. Recent research has evolved to address the inherent limitations of this approach, specifically in the areas of privacy and administrative overhead. To mitigate data exposure, Eckel et al. utilize non-interactive zero-knowledge proofs to verify software authenticity. This approach allows a verifier to confirm that a system is running authorized software without revealing specific versions or configurations, effectively preserving the privacy of the attester [51].

Beyond privacy concerns, the requirement for verifiers to maintain exhaustive databases of reference values presents a significant scalability challenge. To address this, Ott et al. propose a framework that shifts the management of allowlists from the verifier to the attester through the use of signed manifests. By including vendor signed metadata and reference values within the attestation exchange, the verification logic moves from a static database lookup to a dynamic check of cryptographic signatures. This decentralized approach allows the verifier to assess the trustworthiness of diverse software stacks without the burden of maintaining a massive central repository [52].

4.4.2. Control-Flow Graph

Control-Flow Attestation (CFA) mechanisms verify that the execution path of a program adheres to a valid Control-Flow Graph (CFG). Recent advancements focus on reducing the performance overhead of graph analysis. Zhang et al. introduce ReCFA [53], a resilient control-flow attestation scheme that improves efficiency by compressing the record of execution events. Rather than mapping every possible path beforehand, ReCFA reconstructs the actual path taken and validates it against the program's expected behavior [53]. Furthermore, hardware-assisted techniques have emerged to enhance the precision of control-flow attestation. Ammar et al. present CFA+ [54], a framework that capitalizes on processor capabilities designed to enforce valid execution paths. Instead of transmitting execution logs, the verification process employs formal constraint solving to analyze the device's reported hardware state against the allowable CFG. This approach enables the mathematical deduction of control-flow violations, allowing the verifier to confirm execution integrity while reducing the communication overhead typically associated with trace-based attestation. In the domain of TEEs, Morbitzer et al. propose GuaranTEE [55], which employs a mechanism to forward control-flow data from a target microservice to a verifier enclave, allowing for the verification of workloads against a pre-learned CFG.

4.4.3. Data-Flow Graph

Data-flow verification extends control-flow techniques to ensure the integrity of non-control data, thereby detecting data-oriented programming attacks. De Oliveira Nunes et al. introduce DIALED [56], a hybrid architecture that logs not only the control flow but also all data inputs received by the software. This log enables the verifier to perform an abstract execution or local emulation of the program. By knowing the code, the exact control flow, and all external inputs, the verifier can reproduce the execution steps to ensure that intermediate data states are consistent with the expected logic.

4.4.4. Behavioral and Machine Learning-Based

An evolution in the field is the shift towards behavioral verification, where the verifier analyzes the effects or side-channels of execution rather than the code itself. This approach is particularly relevant for legacy systems or black-box devices. Li Calsi and Zaccaria propose CHARM [39], which utilizes

machine learning to analyze hardware performance counters. The verifier checks if the vector of micro-architectural events corresponds to a benign execution profile, enabling the detection of malware. Similarly, recent advancements have introduced unsupervised learning techniques to analyze the integrity of device memory [21]. Rather than relying on pre-defined signatures, this approach processes raw snapshots of the device's RAM to construct a dynamic behavioral model. The verifier evaluates whether the extracted characteristics of a memory dump align with the patterns of known good states, creating a fingerprint of the firmware's operational status without requiring manual feature engineering.

In the domain of Industrial Control Systems, recent behavioral attestation methodologies evaluate the Programmable Logic Controller (PLC) software based on its observable external interactions rather than internal execution states [42]. Rather than inspecting the software code directly or relying on complex physical process models, this paradigm utilizes neural networks to systematically learn the deterministic mapping between the sensory inputs of the PLC and its expected actuator commands. Verification is subsequently executed by cross-referencing the actual commands issued by the physical device against these computational predictions, an approach that systematically facilitates the detection of localized code modification attacks even in deployment scenarios where the internal operational state of the controller is deliberately obfuscated or architecturally inaccessible to the verifier.

Furthermore, this concept has been expanded to encompass device swarms through the application of relational analysis techniques [40]. By correlating the volatile memory states of interacting nodes, this approach moves beyond isolated device verification to model the collective behavior of the network. This holistic perspective enables the detection of anomalies that transcend individual units, allowing the verifier to identify the propagation of malicious patterns and uncover sophisticated, coordinated attacks by leveraging the structural dependencies inherent in the swarm.

4.5. Scalability

Scalability in remote attestation defines the capacity of an attestation scheme to efficiently verify a potentially large group of systems. This characteristic is crucial for large-scale deployments where networks may contain thousands of nodes. The taxonomy of scalability is generally divided into three distinct interaction models which are one-to-one, many-to-one, and many-to-many.

4.5.1. One-to-One

The one-to-one scalability model characterizes the traditional attestation paradigm where a single verifier directly validates a single attester. While providing robust security guarantees, this direct relationship introduces significant bottlenecks, e.g., in cloud and virtualized environments. Recent research has proposed scalable architectures such as CloudTA [29]. By aggregating active verification requests with periodic reporting, this approach consolidates multiple Virtual Machines (VMs) into a single TPM Quote operation. This strategy bypasses the throughput limitations of hardware trust anchors, achieving high concurrency and substantially reducing verification latency compared to traditional serialized methods. Addressing scalability at the network edge, the RA as a service model restructures the one-to-one paradigm into a hierarchical three-layer architecture comprising cloud services, edge gateways, and low-end IoT nodes [57]. This design delegates the immediate verification burden to edge devices, effectively decoupling the central cloud verifier from the direct management of end nodes and minimizing the latency associated with direct communication over wide-area networks. Furthermore, advancements have been made to address temporal scalability in intermittent computing environments, as demonstrated by the RESERVE framework [46]. By enabling energy-harvesting devices to execute attestation routines in modular steps across multiple power cycles, this scheme eliminates the requirement for continuous, synchronous sessions. This allows the attestation process to scale in environments characterized by sporadic and unpredictable device availability.

4.5.2. Many-to-One

In the domain of many-to-one scalability, recent contributions have focused on optimizing the logic used to aggregate attestation reports from large device populations. Addressing the challenge of accountability in aggregated reports, the CoRA [58] framework employs aggregate authentication techniques to secure evidence propagation. Unlike traditional schemes where a single invalid contribution rejects the entire group proof, this method introduces a sequential detection mechanism capable of tracing the specific origin of erroneous reports. Further enhancements target the structural management of dynamic, heterogeneous environments. The SAFEHIVE [59] framework leverages dynamic clustering protocols to coordinate the aggregation process. A key innovation is its automated isolation mechanism, which issues cryptographic authorization tokens based on verification outcomes. This ensures that compromised nodes are seamlessly quarantined from the swarm, preserving the operational integrity of the remaining network. Finally, adapting collective attestation to complex cloud-edge architectures, the SLCSA [60] scheme utilizes signature aggregation primitives to facilitate scalable verification. This enables users to perform simultaneous validation of multiple cooperative services, addressing the latency and throughput limitations of traditional methods in dynamic topologies.

4.5.3. Many-to-Many

Many-to-many scalability architectures are characterized by decentralized or distributed verification models, a paradigm particularly vital for highly dynamic or disruptive networks where continuous connectivity to a central authority cannot be guaranteed. Recent research has focused on optimizing these distributed interactions to reduce computational complexity and enhance resilience.

To address the inefficiencies inherent in peer-to-peer aggregation within disruptive networks, the Delica framework introduces a role-based architectural optimization [61]. Prior decentralized approaches often incurred prohibitive computational overheads due to redundant aggregation tasks performed indiscriminately by every node in the network. Delica mitigates this by architecturally differentiating network nodes into distinct roles of attesters and aggregators. By restricting the resource-intensive task of evidence aggregation to specific aggregator nodes while limiting standard attesters to evidence propagation, the protocol lowers the overall computational complexity of the verification process.

Addressing the specific challenge of detecting physical attacks in mobile swarms, the LICAPA [62] protocol proposes a lightweight collective attestation mechanism. In highly dynamic networks, traditional absence detection methods often generate false positives due to benign connectivity interruptions. LICAPA mitigates this through a mechanism, which requires devices to propagate timestamps cryptographically endorsed by their recently attested neighbors. Since a physical attack typically necessitates taking a device offline for a non-negligible duration, a compromised node will fail to acquire and present these fresh, neighbor-validated proofs. This approach allows the network to distinguish between benign disconnections and actual physical compromises with significantly higher accuracy than previous methods, while simultaneously reducing the overall overhead of swarm attestation.

5. Discussion

In the following, we generalize and discuss the results along our research questions in detail. Finally, we consider directions for future research.

5.1. RQ1: Evolution of the Field

In their foundational work, Johnson et al. identified several research gaps and future directions for the field of RA. This discussion builds upon their framework by specifically addressing three of these identified gaps, while also highlighting a newly emerging paradigm. The need for dynamic evidence to accurately capture runtime behavior is emphasized in their work. However, our results reveal that the majority of recent literature continues to predominantly rely on static evidence. For most of

these studies, the primary research focus lies in optimizing other dimensions of the RA architecture. Nevertheless, there is a distinct and growing subset of research dedicated to advancing dynamic evidence collection that has led to the development of novel architectural constructs.

Closely related to this is the second gap, the lack of contextual analysis during the verification phase. Our findings indicate that the overarching majority of current RA schemes still fail to incorporate meaningful execution context into the verification process. Even in scenarios where complex dynamic evidence is gathered, the verification logic frequently reverts to a rigid, whitelist-based comparison. Given the inherent complexity and high dimensionality involved in evaluating dynamic execution traces, recent research has increasingly explored ML techniques to facilitate context-aware verification and anomaly detection without relying on static reference values.

The third critical gap was the urgent need to prioritize scalability, a directive that the research community has pursued. Arguably, the most significant advancement in RA over recent years has been the proliferation of novel architectures designed to efficiently attest massive device networks. This trend is linked to the rapid growth of IoT deployments, which has propelled swarm attestation from a theoretical concept to a practical necessity. Consequently, the literature now offers a diverse array of scalability models, ranging from many-to-one aggregation topologies to fully decentralized, many-to-many architectures that enable autonomous mutual attestation among peer devices.

Finally, our analysis identifies privacy preservation as a paramount, newly emerging requirement in modern RA. Across various dimensions of the attestation taxonomy, researchers are actively investigating mechanisms to enhance data confidentiality and device anonymity. This paradigm shift is evident from the evidence-gathering and packaging phases, where protocols are evolving away from simply hashing and exposing specific software binaries. Instead, property-based attestation or advanced cryptographic primitives such as Zero-Knowledge Proofs are employed. The strategic implementation of these mechanisms guarantees that valid proofs of integrity can be securely verified without unequivocally disclosing the explicit configuration, intellectual property, or identity of the underlying device.

5.2. RQ2: Standardization Efforts

Since 2023, the standardization landscape for remote attestation has experienced continuous maturation, evidenced by the publication of multiple new drafts and RFCs. The foundational milestone in this domain was the formalization of the IETF RATS architecture within RFC 9334 [3]. While some parallel initiatives attempt to establish decoupled frameworks, the newly published RFCs predominantly function as direct extensions and concrete implementations of the RATS architecture. Notable examples include the specification of the Entity Attestation Token (EAT) in RFC 9711 [63], which standardizes the format and encoding of attestation claims. Concurrently, the formalization of the Challenge/Response Interaction Model is instantiated via the CHAllenge-Response based Remote Attestation protocol, as delineated in RFC 9684 [64]. The academic research community rapidly acknowledged the importance of these standardization efforts. Early RATS Internet-Drafts were referenced by the literature as early as 2021, a trend that has demonstrably accelerated as the standards matured. The RATS architecture provides a robust structural foundation that accommodates traditional attestation paradigms. For instance, when mapped to our taxonomy, RATS supports the extraction of static evidence, discrete gathering mechanisms, and whitelist-based verification logic. Furthermore, the most significant practical contribution of the RATS standard lies in its establishment of semantic interoperability through the unification of terminology. The framework explicitly defines standardized roles including the Attester, Verifier, Relying Party, Endorser, and Reference Value Provider. These discrete classifications systematically resolve prior conceptual ambiguities. Consequently, these standardization efforts streamline the design, implementation, and deployment of interoperable RA frameworks.

5.3. RQ3: Compatibility with Zero Trust Architecture

Although explicit references to the integration of RA within the broader context of ZTAs remain limited in the examined literature, progress in aligning RA with ZTA principles is distinctly observable across

primary operational domains. The first domain encompasses the expansive ecosystem of IoT devices, which presents a suitable environment for the systematic application of ZT principles. In this context, recent advancements in swarm attestation enable decentralized networks of devices to continuously transmit and verify their operational states. The corresponding research thoroughly explores various dimensions of evidence gathering, demonstrating that both static memory measurements and dynamic execution traces can be reliably captured through discrete challenge-response mechanisms or continuous monitoring paradigms. However, it is crucial to recognize that the majority of these protocols explicitly target highly resource-constrained, lightweight devices.

The second domain encompasses the established realm of cloud computing and web services, where ZT principles are strictly enforced over public networks. A promising research direction in this area involves the cryptographic integration of RA directly into the TLS handshake. By embedding attestation reports within standard TLS messages, systems can cryptographically bind the establishment of a secure communication channel directly to the verified hardware and software integrity of the corresponding endpoint. Furthermore, recent methodological efforts have elevated this verification capability to the application layer through the structural augmentation of standard HTTP protocols. Such integrations facilitate trusted end-to-end communication, enabling clients to cryptographically verify that a remote web service operates securely before any sensitive data is transmitted.

5.4. Future Work

Future research should focus on several limitations to facilitate the broader adoption of RA within enterprise ZTAs. Primarily, the integration of RA mechanisms within multi-tenant and BYOD environments necessitates the development of performant, privacy-preserving constrained disclosure protocols. By leveraging advanced cryptographic primitives such as non-interactive zero-knowledge proofs, attesters can selectively disclose requisite state information while cryptographically obfuscating personal or proprietary configurations. This selective disclosure systematically mitigates the inherent privacy violations associated with traditional, full-disclosure measurement architectures. Furthermore, achieving ZT operationalization requires the integration of RA claims directly into established enterprise identity and access management frameworks. Subsequent investigations should therefore focus on binding cryptographic access tokens directly to the verified underlying system state. The inherent heterogeneity of modern corporate cloud infrastructures presents a fundamental interoperability barrier. Consequently, the formulation of universal, hardware-agnostic RA abstraction layers is essential for enabling centralized verifiers to systematically evaluate heterogeneous software stacks.

6. Conclusion

This SLR documents the progression of remote attestation research between 2020 and 2025. Our multi-dimensional analysis of 110 peer-reviewed publications and standardization documents reveals a shift toward hybrid RoT paradigms that balance the cryptographic assurances of dedicated hardware with the operational flexibility of software-based approaches. Concurrently, the proliferation of decentralized IoT deployments has accelerated the advancement of scalable swarm attestation protocols. Furthermore, our synthesis identifies privacy preservation as a design requisite, compelling the integration of advanced cryptographic primitives such as zero-knowledge proofs to facilitate constrained evidence disclosure without exposing sensitive operational data. On the macroscopic level, the standardization landscape has matured, predominantly guided by the formalization of the RATS architecture, which has successfully established the semantic interoperability requisite for heterogeneous network integration. To ensure integration across enterprise environments, future research must consequently focus on formulating universal, hardware-agnostic abstraction layers to foster interoperability, while simultaneously engineering the integration of attestation evidence directly into established identity and access management frameworks. By systematically addressing these architectural gaps, the academic and standardization communities can fully operationalize RA as an indispensable, high-fidelity health telemetry signal bridging the physical and logical boundaries of the ZT paradigm.

Acknowledgments

This research was funded by the German Federal Ministry of Research, Technology and Space (BMFTR) under the Nice Device project.

Declaration on Generative AI

During the preparation of this work, the authors used Claude [65], ChatGPT [66], Gemini [67], and Deepl [68] in order to: Grammar and spelling check, paraphrase and reword. After using these services, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] S. Rose, O. Borchert, S. Mitchell, S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, National Institute of Standards and Technology, 2020. doi:10.6028/NIST.SP.800-207.

[2] FIDO Alliance, FIDO2: FIDO Alliance, 2026. URL: https://fidoalliance.org/fido2/, accessed: 2026-02-23.

[3] H. Birkholz, D. Thaler, M. Richardson, N. Smith, W. Pan, Remote ATtestation procedureS (RATS) Architecture, Request for Comments RFC 9334, Internet Engineering Task Force, 2023. doi:10.17487/RFC9334.

[4] W. A. Johnson, S. Ghafoor, S. Prowell, A taxonomy and review of remote attestation schemes in embedded systems, IEEE access : practical innovations, open solutions 9 (2021) 142390–142410. doi:10.1109/ACCESS.2021.3119220.

[5] B. Kuang, A. Fu, W. Susilo, S. Yu, Y. Gao, A survey of remote attestation in internet of things: Attacks, countermeasures, and prospects, Computers and Security 112 (2022) 102498. doi:10.1016/j.cose.2021.102498.

[6] S. Kumar, P. Eugster, S. Santini, Software-based remote network attestation, IEEE Transactions on Dependable and Secure Computing 19 (2022) 2920–2933. doi:10.1109/TDSC.2021.3077993.

[7] R. V. Steiner, E. Lupu, Attestation in wireless sensor networks: A survey, ACM Comput. Surv. 49 (2016). doi:10.1145/2988546.

[8] C. Buck, C. Olenberger, A. Schweizer, F. Völter, T. Eymann, Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust, Computers & Security 110 (2021) 102436. doi:10.1016/j.cose.2021.102436.

[9] R. Ward, B. Beyer, Beyondcorp: A new approach to enterprise security, ;login: 39 (2014) 6–11.

[10] Microsoft Corporation, Zero Trust Strategy & Architecture, 2026. URL: https://www.microsoft.com/en-us/security/business/zero-trust, accessed: 2026-02-23.

[11] G. Vukotich, Healthcare and cybersecurity: Taking a zero trust approach, Health Services Insights 16 (2023) 5. doi:10.1177/11786329231187826.

[12] M. Asad, S. Otoum, Integrative federated learning and zero-trust approach for secure wireless communications, IEEE Wireless Communications 31 (2024) 14–20. doi:10.1109/MWC.001.2300355.

[13] B. Kitchenham, S. Charters, Guidelines for Performing Systematic Literature Reviews in Software Engineering, Technical Report EBSE 2007-001, Keele University and Durham University, Keele, UK and Durham, UK, 2007.

[14] V. Garousi, M. Felderer, M. V. Mäntylä, Guidelines for including grey literature and conducting multivocal literature reviews in software engineering, Information and Software Technology 106 (2019) 101–121. doi:10.1016/j.infsof.2018.09.006.

[15] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, et al., The prisma 2020 statement: an updated guideline for reporting systematic reviews, bmj 372 (2021). doi:10.1136/bmj.n71.

[16] M. Younis, M. Ebrahimabadi, S. S. Mehjabin, E. Pozniak, T. Sookoor, N. Karimi, LiSB: Lightweight secure boot and attestation scheme for IoT and edge devices, IEEE Transactions on Information Forensics and Security 20 (2025) 9009–9024. doi:10.1109/TIFS.2025.3592573.

[17] J. Julku, J. Suomalainen, M. Kylänpää, Delegated device attestation for IoT, 2021 8th International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (2021) 1–8. doi:10.1109/IOTSMS53705.2021.9704959.

[18] N. Ahmed, M. A. Talib, Q. Nasir, SAPEM: Secure attestation of program execution and program memory for IoT applications, Computers, Materials and Continua 67 (2020) 23–49. doi:10.32604/cmc.2021.014523.

[19] M. Ammar, B. Crispo, G. Tsudik, Simple: A remote attestation approach for resource-constrained iot devices, in: 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS), 2020, pp. 247–258. doi:10.1109/ICCPS48487.2020.00036.

[20] A. Galanou, F. Gregor, R. Kapitza, C. Fetzer, Matee: multimodal attestation for trusted execution

environments, in: Proceedings of the 23rd ACM/IFIP International Middleware Conference, Middleware '22, Association for Computing Machinery, New York, NY, USA, 2022, p. 121–134. doi:10.1145/3528535.3565239.

[21] A. Iqbal, U. Zia, M. N. Aman, B. Sikdar, RAM-based firmware attestation for IoT security: A representation learning framework, IEEE Internet of Things Journal 11 (2024) 35124–35140. doi:10.1109/JIOT.2024.3436057.

[22] S. Surminski, C. Niesler, F. Brasser, L. Davi, A.-R. Sadeghi, Realswatt: Remote software-based attestation for embedded devices under realtime constraints, in: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, CCS '21, Association for Computing Machinery, New York, NY, USA, 2021, pp. 2890–2905. doi:10.1145/3460120.3484788.

[23] P. Frolikov, Y. Kim, R. T. Prapty, G. Tsudik, TOCTOU resilient attestation for IoT networks, Proceedings of the 23rd ACM conference on embedded networked sensor systems (2025) 88–101. doi:10.1145/3715014.3722057.

[24] J. Cao, T. Zhu, R. Ma, Z. Guo, Y. Zhang, H. Li, A software-based remote attestation scheme for internet of things devices, IEEE Transactions on Dependable and Secure Computing 20 (2023) 1422–1434. doi:10.1109/TDSC.2022.3154887.

[25] S. S. Mehjabin, M. Younis, PAMA: PUF-based aggregated multi-hop attestation protocol for IoT, ICC 2025 - IEEE International Conference on Communications (2025) 722–727. doi:10.1109/ICC52391.2025.11161539.

[26] S. Mehjabin, M. Younis, PISA: PUF-based IoT swarm attestation protocol, IEEE Internet of Things Journal 12 (2025) 36094–36111. doi:10.1109/JIOT.2025.3583269.

[27] T. Alladi, S. Chakravarty, V. Chamola, M. Guizani, A lightweight authentication and attestation scheme for in-transit vehicles in IoV scenario, IEEE Transactions on Vehicular Technology 69 (2020) 14188–14197. doi:10.1109/TVT.2020.3038834.

[28] A. Juhola, M. Kylänpää, Experimental implementation of remote attestation over OPC UA protocol, 2022 International Conference on Networks, Communications and Information Technology (CNCIT) (2022) 83–88. doi:10.1109/CNCIT56797.2022.00021.

[29] J. Cheng, K. Zhang, B. Tu, Remote attestation of large-scale virtual machines in the cloud data center, 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (2021) 180–187. doi:10.1109/TrustCom53373.2021.00041.

[30] A. Khurshid, S. Raza, AutoCert: Automated TOCTOU-secure digital certification for IoT with combined authentication and assurance, Computers and Security 124 (2023). doi:10.1016/j.cose.2022.102952.

[31] L. Jäger, D. Lorych, M. Eckel, A resilient network node for the industrial internet of things, in: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 1–10. doi:10.1145/3538969.3538989.

[32] S. Frontera, R. Lazzeretti, Bloom filter based collective remote attestation for dynamic networks, in: Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES '21, Association for Computing Machinery, New York, NY, USA, 2021, pp. 1–10. doi:10.1145/3465481.3470054.

[33] T. Gamboni-Diehl, S. Wuthier, J. Kim, J. Kim, S.-Y. Chang, Lightweight code assurance proof for wireless software, in: Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '22, Association for Computing Machinery, New York, NY, USA, 2022, p. 285–287. doi:10.1145/3507657.3529653.

[34] F. Bai, Z. Wang, K. Zeng, C. Zhang, T. Shen, X. Zhang, B. Gong, ZKSA: Secure mutual attestation against TOCTOU zero-knowledge proof based for IoT devices, Computers & Security 148 (2025) 104136. doi:10.1016/j.cose.2024.104136.

[35] A. Caulfield, L. Tyler, I. D. O. Nunes, SpecCFA: Enhancing control flow attestation/auditing via application-aware sub-path speculation, 2024 Annual Computer Security Applications Conference (ACSAC) (2024) 563–578. doi:10.1109/ACSAC63791.2024.00055.

[36] M. Chilese, R. Mitev, M. Orenbach, R. Thorburn, A. Atamli-Reineh, A.-R. Sadeghi, One for all

and all for one: GNN-based control-flow attestation for embedded devices, Proceedings - IEEE Symposium on Security and Privacy (2024) 3346–3364. doi:10.1109/SP54263.2024.00251.

[37] A. J. Neto, I. D. O. Nunes, ISC-FLAT: On the conflict between control flow attestation and real-time operations, 2023 IEEE 29th Real-Time and Embedded Technology and Applications Symposium (RTAS) (2023) 133–146. doi:10.1109/RTAS58335.2023.00018.

[38] J. Gonzalez-Gomez, H. Nassar, L. Bauer, J. Henkel, LightFAt: Mitigating control-flow explosion via lightweight PMU-based control-flow attestation, 2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (2024) 222–226. doi:10.1109/HOST55342.2024.10545348.

[39] D. Li Calsi, V. Zaccaria, Interruptible remote attestation of low-end IoT microcontrollers via performance counters, ACM Trans. Embed. Comput. Syst. 22 (2023). doi:10.1145/3611674.

[40] V. Kohli, B. Kohli, M. N. Aman, B. Sikdar, Swarm-net: Firmware attestation in IoT swarms using graph neural networks and volatile memory, IEEE Internet of Things Journal 12 (2025) 8338–8352. doi:10.1109/JIOT.2024.3501854.

[41] I. M. Delgado-Lozano, M. C. Martínez-Rodríguez, A. Bakas, B. B. Brumley, A. Michalas, Attestation waves: Platform trust via remote power analysis, in: M. Conti, M. Stevens, S. Krenn (Eds.), Cryptology and Network Security, Springer International Publishing, Cham, 2021, pp. 460–482. doi:10.1007/978-3-030-92548-2_24.

[42] Y. Chen, C. M. Poskitt, J. Sun, Code integrity attestation for plcs using black box neural network predictions, in: Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, ESEC/FSE 2021, Association for Computing Machinery, New York, NY, USA, 2021, pp. 32–44. doi:10.1145/3468264.3468617.

[43] A. Mondal, S. Gangopadhyay, D. Chatterjee, H. Boyapally, D. Mukhopadhyay, PReFeR : Physically related function based remote attestation protocol, ACM Trans. Embed. Comput. Syst. 22 (2023). doi:10.1145/3609104.

[44] N. Kassem, W. Hellemans, I. Siachos, E. Dushku, S. Vasileiadis, D. Karas, L. Chen, C. Patsakis, T. Giannetsos, PRIVE: Towards privacy-preserving swarm attestation, Proceedings of the International Conference on Security and Cryptography 1 (2025) 247–262. doi:10.5220/0013629000003979.

[45] N. Sponziello, A. Sateesan, M. M. Rabbani, N. Mentens, N. Dragoni, E. Dushku, ITERATOR: Interruptible remote attestation through cuckoo filters, IEEE Internet of Things Journal (2025) 1–1. doi:10.1109/JIOT.2025.3621016.

[46] M. M. Rabbani, E. Dushku, J. Vliegen, A. Braeken, N. Dragoni, N. Mentens, Reserve: Remote attestation of intermittent iot devices, in: Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems, SenSys '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 578–580. doi:10.1145/3485730.3493364.

[47] J. Zhan, Y. Li, Y. Liu, H. Li, S. Zhang, L. Lin, NSGA-II-based granularity-adaptive control-flow attestation, Security and Communication Networks 2021 (2021). doi:10.1155/2021/2914192.

[48] E. Dushku, M. M. Rabbani, M. Conti, L. V. Mancini, S. Ranise, SARA: Secure asynchronous remote attestation for IoT systems, IEEE Transactions on Information Forensics and Security 15 (2020) 3123–3136. doi:10.1109/TIFS.2020.2983282.

[49] E. Dushku, M. M. Rabbani, J. Vliegen, A. Braeken, N. Mentens, PROVE: Provable remote attestation for public verifiability, Journal of Information Security and Applications 75 (2023) 103448. doi:10.1016/j.jisa.2023.103448.

[50] Q. Wang, X. Chen, X. Jin, X. Li, D. Chen, X. Qin, Enhancing trustworthiness of internet of vehicles in space–air–ground-integrated networks: Attestation approach, IEEE Internet of Things Journal 9 (2022) 5992–6002. doi:10.1109/JIOT.2021.3084449.

[51] M. Eckel, D. R. George, B. Grohmann, C. Krauß, Remote attestation with constrained disclosure, in: Proceedings of the 39th Annual Computer Security Applications Conference, ACSAC '23, Association for Computing Machinery, New York, NY, USA, 2023, p. 718–731. doi:10.1145/3627106.3627118.

[52] S. Ott, M. Kamhuber, J. Pecholt, S. Wessel, Universal remote attestation for cloud and edge

platforms, in: Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES '23, Association for Computing Machinery, New York, NY, USA, 2023, pp. 1–11. doi:10.1145/3600160.3600171.

[53] Y. Zhang, X. Liu, C. Sun, D. Zeng, G. Tan, X. Kan, S. Ma, ReCFA: Resilient control-flow attestation, ACM International Conference Proceeding Series (2021) 311–322. doi:10.1145/3485832.3485900.

[54] M. Ammar, A. Abdelraoof, S. Vlasceanu, On bridging the gap between control flow integrity and attestation schemes, in: 33rd USENIX Security Symposium (USENIX Security 24), USENIX Association, Philadelphia, PA, 2024, pp. 6633–6650. URL: https://www.usenix.org/conference/usenixsecurity24/presentation/ammar.

[55] M. Morbitzer, B. Kopf, P. Zieris, GuaranTEE: Introducing control-flow attestation for trusted execution environments, 2023 IEEE 16th International Conference on Cloud Computing (CLOUD) (2023) 547–553. doi:10.1109/CLOUD60044.2023.00073.

[56] I. De Oliveira Nunes, S. Jakkamsetti, G. Tsudik, Dialed: Data integrity attestation for low-end embedded devices, in: 2021 58th ACM/IEEE Design Automation Conference (DAC), 2021, pp. 313–318. doi:10.1109/DAC18074.2021.9586180.

[57] M. Calvo, M. Beltrán, Remote attestation as a service for edge-enabled IoT, 2021 IEEE International Conference on Services Computing (SCC) (2021) 329–339. doi:10.1109/SCC53864.2021.00046.

[58] A. Diop, M. Laurent, J. Leneutre, J. Traoré, CoRA: A scalable collective remote attestation protocol for sensor networks, International Conference on Information Systems Security and Privacy (2020) 84–95. doi:10.5220/0008962700840095.

[59] L. Ferro, E. Bravi, S. Sisinni, A. Lioy, Safehive: Secure attestation framework for embedded and heterogeneous iot devices in variable environments, in: Proceedings of the 2024 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, SaT-CPS '24, Association for Computing Machinery, New York, NY, USA, 2024, p. 41–50. doi:10.1145/3643650.3658609.

[60] J. Cui, Q. Chen, L. Han, Y. Li, Q. Zhang, L. Liu, H. Zhong, SLCSA: Scalable layered cooperative service attestation scheme in cloud-edge-end cooperation environments, 2023 IEEE 29th International Conference on Parallel and Distributed Systems (ICPADS) (2023) 1741–1750. doi:10.1109/ICPADS60453.2023.00242.

[61] Z. Wang, C. Sun, Q. Yao, D. Ding, J. Ma, Delica: Decentralized lightweight collective attestation for disruptive IoT networks, 2021 IEEE 27th International Conference on Parallel and Distributed Systems (ICPADS) (2021) 364–371. doi:10.1109/ICPADS53394.2021.00051.

[62] Z. Wang, C. Sun, LICAPA: Lightweight collective attestation for physical attacks detection in highly dynamic networks, Pervasive and Mobile Computing 99 (2024) 101903. doi:10.1016/j.pmcj.2024.101903.

[63] L. Lundblade, G. Mandyam, J. O'Donoghue, C. Wallace, The Entity Attestation Token (EAT), RFC 9711, 2025. URL: https://www.rfc-editor.org/info/rfc9711. doi:10.17487/RFC9711.

[64] H. Birkholz, M. Eckel, S. Bhandari, E. Voit, B. Sulzen, L. Xia, T. Laffey, G. Fedorkow, A YANG Data Model for Challenge-Response-Based Remote Attestation (CHARRA) Procedures Using Trusted Platform Modules (TPMs), RFC 9684, 2024. URL: https://www.rfc-editor.org/info/rfc9684. doi:10.17487/RFC9684.

[65] Anthropic, Claude, Large language model, 2025. URL: https://claude.ai, accessed: 2026-02-23.

[66] OpenAI, ChatGPT, Large language model, 2025. URL: https://chatgpt.com, accessed: 2026-02-23.

[67] Google DeepMind, Gemini, Large language model, 2025. URL: https://gemini.google.com, accessed: 2026-02-23.

[68] DeepL SE, DeepL translator, Neural machine translation service, 2025. URL: https://www.deepl.com, accessed: 2026-02-23.

[69] I. E. Akkus, I. Rimac, Duet: Combining a trustworthy controller with a confidential computing environment, 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (2024) 436–442. doi:10.1109/EuroSPW61312.2024.00028.

[70] A. Alsayed, M. Binsawad, J. Ali, A. Khalid, W. Ahmed, Realizing macro based technique for

behavioral attestation on remote platform, Advances in Intelligent Systems and Computing 1250 (2021) 132–144. doi:10.1007/978-3-030-55180-3_10.

[71] M. Ammar, B. Crispo, VerifyandRevive: Secure detection and recovery of compromised low-end embedded devices, ACM International Conference Proceeding Series (2020) 717–732. doi:10.1145/3427228.3427253.

[72] M. Ammar, B. Crispo, WISE: A lightweight intelligent swarm attestation scheme for the internet of things, ACM Trans. Internet Things 1 (2020). doi:10.1145/3386688.

[73] M. Ammar, B. Crispo, I. De Oliveira Nunes, G. Tsudik, Delegated attestation: scalable remote attestation of commodity cps by blending proofs of execution with software attestation, in: Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 37–47. doi:10.1145/3448300.3467818.

[74] P. Antonino, A. Derek, W. A. Wołoszyn, Flexible remote attestation of pre-SNP SEV vms using SGX enclaves, IEEE access : practical innovations, open solutions 11 (2023) 90839–90856. doi:10.1109/ACCESS.2023.3308850.

[75] G. Arfaoui, T. Jacques, M. Lacoste, C. Onete, L. Robert, Towards a privacy-preserving attestation for virtualized networks, Lecture Notes in Computer Science 14347 (2024) 351–370. doi:10.1007/978-3-031-51482-1_18.

[76] G. Bansal, B. Sikdar, Secure and trusted attestation protocol for UAV fleets, IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (2022) 1–6. doi:10.1109/INFOCOMWKSHPS54753.2022.9798087.

[77] G. Bansal, Naren, V. Chamola, B. Sikdar, SHOTS: Scalable secure authentication-attestation protocol using optimal trajectory in UAV swarms, IEEE Transactions on Vehicular Technology 71 (2022) 5827–5836. doi:10.1109/TVT.2022.3162226.

[78] D. L. Calsi, J. Nötzel, Quantum static remote attestation, 2023 IEEE 9th World Forum on Internet of Things (WF-IoT) (2023) 01–06. doi:10.1109/WF-IoT58464.2023.10539576.

[79] Y. Chen, Y. Ding, J. Zhang, L. Song, MRA-IMA: Enhanced mutual remote attestation based on ARM TrustZone, 2024 9th International Conference on Computer and Communication Systems (ICCCS) (2024) 1278–1284. doi:10.1109/ICCCS61882.2024.10603080.

[80] T. Cloosters, S. Surminski, G. Sangel, L. Davi, Salsa: SGX attestation for live streaming applications, 2022 IEEE Secure Development Conference (SecDev) (2022) 45–51. doi:10.1109/SecDev53368.2022.00019.

[81] C. Cremers, G. Horowitz, C. Jacomme, E. Ronen, Token weaver: Privacy preserving and post-compromise secure attestation, 2025 IEEE Symposium on Security and Privacy (SP) (2025) 4173–4191. doi:10.1109/SP61157.2025.00093.

[82] A. Dhar, I. Puddu, K. Kostiainen, S. Capkun, Proximitee: Hardened sgx attestation by proximity verification, in: Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, CODASPY '20, Association for Computing Machinery, New York, NY, USA, 2020, p. 5–16. doi:10.1145/3374664.3375726.

[83] E. Dileesh, A. Shanthi, An application specific dynamic behaviour model using function-call sequence and memory access-graph for execution integrity verification, Computers & Security 107 (2021) 102299. doi:10.1016/j.cose.2021.102299.

[84] M. Eckel, T. Riemann, Userspace software integrity measurement, in: Proceedings of the 16th International Conference on Availability, Reliability and Security, ARES '21, Association for Computing Machinery, New York, NY, USA, 2021, pp. 1–11. doi:10.1145/3465481.3470018.

[85] N. Fotos, S. Vasileiadis, T. Giannetsos, Trust or bust: Reinforcing trust-aware path establishment with implicit attestation capabilities, 2025 IEEE International Conference on Cyber Security and Resilience (CSR) (2025) 867–874. doi:10.1109/CSR64739.2025.11130147.

[86] A. Garah, N. Mbarek, S. Kirgizov, DBSCAN-based IoT object integrity self-management, 2025 International Wireless Communications and Mobile Computing (IWCMC) (2025) 637–642. doi:10.1109/IWCMC65282.2025.11059448.

[87] A. Garah, N. Mbarek, S. Kirgizov, Fuzzy logic-based IoT object integrity self-management, 2025

12th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (2025) 344–351. doi:10.1109/NTMS65597.2025.11076658.

[88] B. Gong, J. Liu, S. Guo, A trusted attestation scheme for data source of internet of things in smart city based on dynamic trust classification, IEEE Internet of Things Journal 8 (2021) 16121–16141. doi:10.1109/JIOT.2020.3006349.

[89] F. Gregor, R. Krahn, D. L. Quoc, C. Fetzer, Sinclave: Hardware-assisted singletons for tees, in: Proceedings of the 24th International Middleware Conference, Middleware '23, Association for Computing Machinery, New York, NY, USA, 2023, p. 85–97. doi:10.1145/3590140.3629107.

[90] R. M. Halldórsson, E. Dushku, N. Dragoni, ARCADIS: Asynchronous remote control-flow attestation of distributed IoT services, IEEE access : practical innovations, open solutions 9 (2021) 144880–144894. doi:10.1109/ACCESS.2021.3122391.

[91] Z. O. Imam, M. Lacoste, G. Arfaoui, Towards a modular attestation framework for flexible data protection for drone systems, 2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (2021) 96–102. doi:10.1109/WiMob52687.2021.9606269.

[92] O. Jarkas, R. Ko, N. Dong, R. Mahmud, VIMA: A privacy-preserving integrity measurement architecture for containerized environments, IACR Transactions on Cryptographic Hardware and Embedded Systems 2025 (2025) 1053–1076. doi:10.46586/tches.v2025.i4.1053-1076.

[93] K. T. Kim, J. D. Lim, J. N. Kim, An IoT device-trusted remote attestation framework, 2022 24th International Conference on Advanced Communication Technology (ICACT) (2022) 218–223. doi:10.23919/ICACT53585.2022.9728853.

[94] G. King, H. Wang, HTTPA/2: A trusted end-to-end protocol for web services, Lecture Notes in Networks and Systems 652 (2023) 824–848. doi:10.1007/978-3-031-28073-3_55.

[95] B. Kuang, A. Fu, Y. Gao, Y. Zhang, J. Zhou, R. H. Deng, FeSA: Automatic federated swarm attestation on dynamic large-scale IoT devices, IEEE Transactions on Dependable and Secure Computing 20 (2023) 2954–2969. doi:10.1109/TDSC.2022.3193106.

[96] M. Kucab, P. Boryło, P. Cholda, Remote attestation and integrity measurements with Intel SGX for virtual machines, Computers and Security 106 (2021). doi:10.1016/j.cose.2021.102300.

[97] S. Kumar, P. Eugster, S. Santini, Software-based remote network attestation, IEEE Transactions on Dependable and Secure Computing 19 (2022) 2920–2933. doi:10.1109/TDSC.2021.3077993.

[98] P. Li, X. Li, L. Fang, DMA: Mutual attestation framework for distributed enclaves, Lecture Notes in Computer Science 15056 (2025) 145–164. doi:10.1007/978-981-97-8798-2_8.

[99] J. Lin, Q. Wu, A security integrated attestation scheme for embedded devices, 2021 7th IEEE International Conference on Network Intelligence and Digital Content (IC-NIDC) (2021) 489–493. doi:10.1109/IC-NIDC54101.2021.9660438.

[100] W. Lin, H. C. Tan, B. Chen, F. Zhang, DNAttest: Digital-twin-based non-intrusive attestation under transient uncertainty, 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (2023) 376–388. doi:10.1109/DSN58367.2023.00044.

[101] Z. Ling, H. Yan, X. Shao, J. Luo, Y. Xu, B. Pearson, X. Fu, Secure boot, trusted boot and remote attestation for ARM TrustZone-based IoT Nodes, Journal of Systems Architecture 119 (2021) 102240. doi:10.1016/j.sysarc.2021.102240.

[102] W. Liu, J. Yu, L. Qi, K. Yang, K. Li, Z. Xu, K. Shang, Q. Wu, Multi-node trusted remote attestation and recovery scheme for power industrial control terminal, 2023 3rd International Conference on Intelligent Power and Systems (ICIPS) (2023) 10–16. doi:10.1109/ICIPS59254.2023.10404365.

[103] Y. Liu, H. Xiao, J. Li, F. Yu, Y. Huang, ADATA: Asymmetric device identifier composition engine compliant aggregate trust attestation, IEEE access : practical innovations, open solutions (2025) 1–1. doi:10.1109/ACCESS.2025.3625217.

[104] M. Mansouri, W. B. Jaballah, M. Önen, M. M. Rabbani, M. Conti, Fadia: fairness-driven collaborative remote attestation, in: Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '21, Association for Computing Machinery, New York, NY, USA, 2021, p. 60–71. doi:10.1145/3448300.3468284.

[105] N. Matsumoto, T. Kawanishi, K. Ohira, M. Kozuka, Yak: WebAssembly-based data analysis plat-

form with data providers driven analysis control, 2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC) (2025) 1116–1125. doi:10.1109/COMPSAC65507.2025.00144.

[106] J. Ménétrey, M. Pasin, P. Felber, V. Schiavoni, G. Mazzeo, A. Hollum, D. Vaydia, A comprehensive trusted runtime for WebAssembly with intel SGX, IEEE Transactions on Dependable and Secure Computing 21 (2024) 3562–3579. doi:10.1109/TDSC.2023.3334516.

[107] J. Ménétrey, P. Yuhala, P. Felber, V. Schiavoni, A. Grüter, J. Oeftiger, M. Pasin, A holistic approach for trustworthy distributed systems with WebAssembly and tees, Leibniz International Proceedings in Informatics, LIPIcs 286 (2024). doi:10.4230/LIPIcs.OPODIS.2023.23.

[108] S. Mohammad, F. Farahmandi, Dyfora: Dynamic firmware obfuscation and remote attestation using hardware signatures, in: Proceedings of the Great Lakes Symposium on VLSI 2024, GLSVLSI '24, Association for Computing Machinery, New York, NY, USA, 2024, p. 471–476. doi:10.1145/3649476.3658715.

[109] E. Moon, Y. Shin, HBRA: A history-based remote attestation approach to resolve malicious verifiers in IoT, International Conference on ICT Convergence (2024) 1562–1567. doi:10.1109/ICTC62082.2024.10827194.

[110] A. Niemi, V. Pop, J.-E. Ekberg, Trusted sockets layer: A TLS 1.3 based trusted channel protocol, Lecture Notes in Computer Science 13115 (2021) 175–191. doi:10.1007/978-3-030-91625-1_10.

[111] I. Oliver, Trust, security and privacy through remote attestation in 5G and 6G systems, 2021 IEEE 4th 5G World Forum (5GWF) (2021) 368–373. doi:10.1109/5GWF52925.2021.00071.

[112] W. Ozga, R. Faqeh, D. L. Quoc, F. Gregor, S. Dragone, C. Fetzer, Chors: hardening high-assurance security systems with trusted computing, in: Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing, SAC '22, Association for Computing Machinery, New York, NY, USA, 2022, p. 1626–1635. doi:10.1145/3477314.3506961.

[113] W. Ozga, P. Sagmeister, T. Visegrády, S. Dragone, Wawel: Architecture for scalable attestation of heterogeneous virtual execution environments, 2023 IEEE 16th International Conference on Cloud Computing (CLOUD) (2023) 96–107. doi:10.1109/CLOUD60044.2023.00020.

[114] D. Papamartzivanos, S. A. Menesidou, P. Gouvas, T. Giannetsos, Towards efficient control-flow attestation with software-assisted multi-level execution tracing, 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) (2021) 512–518. doi:10.1109/MeditCom49071.2021.9647635.

[115] D. Pontes, F. Silva, A. Melo, A. Asadujjaman, E. Falcão, A. Brito, C. Filho, Multi-platform and vault-free attestation of confidential vms, in: Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing, LADC '24, Association for Computing Machinery, New York, NY, USA, 2024, p. 241–251. doi:10.1145/3697090.3698036.

[116] L. Preibsch, M. R. von Onciul, R. Kapitza, Site attestation: Browser-based remote attestation, in: Proceedings of the 18th European Workshop on Systems Security, EuroSec'25, Association for Computing Machinery, New York, NY, USA, 2025, p. 11–17. doi:10.1145/3722041.3723095.

[117] W. Ren, J. Pan, D. Chen, AccGuard: Secure and trusted computation on remote FPGA accelerators, 2021 IEEE International Symposium on Smart Electronic Systems (iSES) (2021) 378–383. doi:10.1109/iSES52644.2021.00093.

[118] K. Shang, F. Lu, K. Huang, Y. Qin, W. Li, W. Feng, Cluster nodes integrity attestation and monitoring scheme for confidential computing platform, 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (2023) 740–749. doi:10.1109/TrustCom60117.2023.00109.

[119] C. Shepherd, K. Markantonakis, G. A. Jaloyan, LIRA-v: Lightweight remote attestation for constrained RISC-v devices, 2021 IEEE Security and Privacy Workshops (SPW) (2021) 221–227. doi:10.1109/SPW53761.2021.00036.

[120] D. Shur, G. D. Crescenzo, Q. Zhang, T. Chen, R. Krishnan, Y. J. Lin, Z. Patni, S. Alexander, G. Tsudik, SEDIMENT: An IoT-device-centric methodology for scalable 5G network security, 2022 IEEE Wireless Communications and Networking Conference (WCNC) (2022) 49–54. doi:10.1109/

WCNC51071.2022.9771654.

[121] S. Sisinni, D. G. Berbecaru, V. Donnini, A. Lioy, MATCH-in: Mutual attestation for trusted collaboration in heterogeneous IoT networks, 2024 IEEE Symposium on Computers and Communications (ISCC) (2024) 1–6. doi:10.1109/ISCC61673.2024.10733616.

[122] M. Usama, M. Aman, B. Sikdar, Runtime self-attestation of FPGA-based IoT devices, IEEE Internet of Things Journal 11 (2024) 33406–33417. doi:10.1109/JIOT.2024.3429109.

[123] R. Walther, C. Weinhold, M. Roitzsch, RATLS: Integrating transport layer security with remote attestation, Lecture Notes in Computer Science 13285 (2022) 361–379. doi:10.1007/978-3-031-16815-4_20.

[124] Z. Wang, Y. Zhuang, Q. Xia, Mutual authentication-based RA scheme for embedded systems, IET Information Security 14 (2020) 232–240. doi:10.1049/iet-ifs.2019.0027.

[125] Y. Wang, J. Li, X. Chen, H. Lin, F. Yu, J. Luo, Remote attestation for intelligent electronic devices in smart grid based on trusted level measurement, Chinese Journal of Electronics 29 (2020) 437–446. doi:10.1049/2020.02.019.

[126] C. Weinhold, M. U. Sardar, I. Mihalcea, Y. Deshpande, H. Tschofenig, Y. Sheffer, T. Fossati, M. Roitzsch, Separate but together: integrating remote attestation into tls, in: USENIX ATC '25: Proceedings of the 2025 USENIX Conference on Usenix Annual Technical Conference, Bos, 2025, pp. 1319 – 1326. doi:10.5555/3768039.3768116.

[127] X. Xiang, J. Cao, W. Fan, Scalable attestation protocol resilient to physical attacks for IoT environments, IEEE Systems Journal 15 (2021) 4566–4577. doi:10.1109/JSYST.2020.3040739.

[128] M. Yang, G. Huang, H. Chen, Y. Liao, Q. Wang, X. Chen, Enhancing the availability and security of attestation scheme for multiparty-involved DLaaS: A circular approach, IEEE Transactions on Cloud Computing 13 (2025) 227–244. doi:10.1109/TCC.2024.3522993.

[129] F. Yu, Y. Huang, SDATA: Symmetrical device identifier composition engine complied aggregate trust attestation, Symmetry 16 (2024). doi:10.3390/sym16030310.

[130] G. Vasiliadis, A. Karampelas, A. Shevtsov, P. Papadopoulos, S. Ioannidis, A. Kapravelos, WRIT: Web request integrity and attestation against malicious browser extensions, IEEE Transactions on Dependable and Secure Computing 21 (2024) 3082–3095. doi:10.1109/TDSC.2023.3322516.

[131] K. Yang, L. Chen, Z. Zhang, C. J. P. Newton, B. Yang, L. Xi, Direct anonymous attestation with optimal TPM signing efficiency, IEEE Transactions on Information Forensics and Security 16 (2021) 2260–2275. doi:10.1109/TIFS.2021.3051801.

A. Search Strings

A.1. IEEE Xplore

("attestation" NEAR/3 (security OR trust OR integrity OR verification OR evidence OR assurance)) AND NOT ("medical attestation" OR "legal attestation" OR "nursing attestation" OR blockchain OR "distributed ledger" OR "smart contract" OR cryptocurrency OR clinical) AND NOT ("agreement attraction" OR "gender agreement" OR "sentence processing" OR linguistics OR psycholinguistics OR "cognitive science" OR "language comprehension" OR "memory and language" OR grammar OR syntax OR morphology OR semantic OR linguistic)

A.2. ACM Digital Library

AllField:(("attestation" 3)) AND AllField:(NOT ("medical attestation" OR "legal attestation" OR "nursing attestation" OR blockchain OR "distributed ledger" OR "smart contract" OR cryptocurrency OR clinical)) AND AllField:(NOT ("agreement attraction" OR "gender agreement" OR "sentence processing" OR linguistics OR psycholinguistics OR "cognitive science" OR "language comprehension" OR "memory and language" OR grammar OR syntax OR morphology OR semantic OR linguistic))

A.3. SpringerLink

(attestation NEAR/3 (security OR trust OR integrity OR verification OR evidence OR assurance)) AND NOT ("medical attestation" OR "legal attestation" OR "nursing attestation" OR blockchain OR "distributed ledger" OR "smart contract" OR cryptocurrency OR clinical) AND NOT ("agreement attraction" OR "gender agreement" OR "sentence processing" OR linguistics OR psycholinguistics OR "cognitive science" OR "language comprehension" OR "memory and language" OR grammar OR syntax OR morphology OR semantic OR linguistic)

A.4. ScienceDirect

attestation W/3 (security OR trust OR integrity OR verification OR assurance)

A.5. Scopus

TITLE-ABS-KEY (attestation W/3 (security OR trust OR integrity OR verification OR evidence OR assurance)) AND NOT TITLE-ABS-KEY ("medical attestation" OR "legal attestation" OR "nursing attestation" OR blockchain OR "distributed ledger" OR "smart contract" OR cryptocurrency OR clinical) AND NOT TITLE-ABS-KEY ("agreement attraction" OR "gender agreement" OR "sentence processing" OR "linguistics" OR "psycholinguistics" OR "cognitive science" OR "language comprehension" OR "memory and language" OR "grammar" OR "syntax" OR "morphology" OR "semantic" OR "linguistic") AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "ENGI") OR EXCLUDE (SUBJAREA , "MEDI") OR EXCLUDE (SUBJAREA , "BIOC")) AND (LIMIT-TO (LANGUAGE , "English") OR LIMIT-TO (LANGUAGE , "German"))

B. PRISMA filtering process

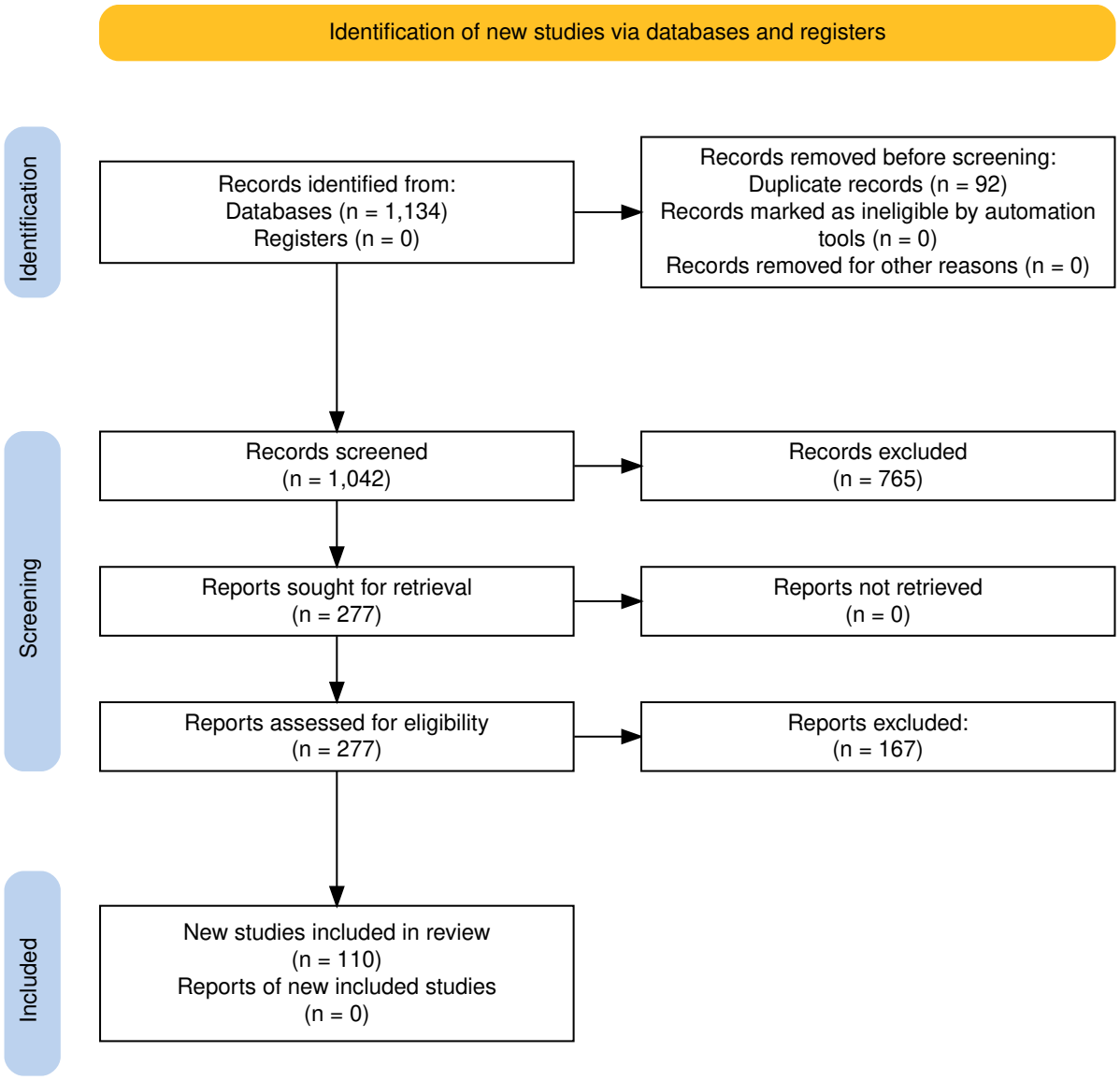

Figure 1: PRISMA filtering process

C. Literature Review Table

Table 1: Results of our systematic literature review with taxonomy by Johnson et al. [4]

ID	Author(s)	Root of Trust	Evidence Type	Evidence Gathering	Verification	Scalability
[16]	Younis et al.	Hardware	Static	Discrete	Whitelist	One-to-One
[21]	Iqbal et al.	Software	Dynamic	Discrete	Behavioral and ML	Many-to-One
[17]	Julku et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[18]	Ahmed et al.	Hybrid	Dynamic	Continuous	Control Flow Graph	One-to-One
[19]	Ammar et al.	Software	Dynamic	Discrete	Whitelist	Many-to-One
[20]	Galanou et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[22]	Surminski et al.	Software	Static	Continuous	Whitelist	Many-to-One
[23]	Frolikov et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[24]	Cao et al.	Software	Dynamic	Discrete	Whitelist	Many-to-One
[25]	Mehjabin and Younis	Hardware	Static	Discrete	Whitelist	Many-to-One
[26]	Mehjabin and Younis	Hardware	Static	Discrete	Whitelist	Many-to-One
[27]	Alladi et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[28]	Juhola and Kylänpää	Hybrid	Static	Discrete	Whitelist	One-to-One
[29]	Cheng et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[30]	Khurshid and Raza	Hybrid	Static	Discrete	Whitelist	One-to-One
[31]	Jäger et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[32]	Frontera and Lazzeretti	Hybrid	Static	Discrete	Whitelist	Many-to-Many
[33]	Gamboni-Diehl et al.	Software	Static	Discrete	Whitelist	Many-to-Many
[34]	Bai et al.	Hybrid	Dynamic	Continuous	Whitelist	Many-to-Many
[35]	Caulfield et al.	Hybrid	Dynamic	Continuous	Control Flow Graph	One-to-One
[36]	Chilese et al.	Hybrid	Dynamic	Continuous	Behavioral and ML	One-to-One
[37]	Neto and Nunes	Hybrid	Dynamic	Continuous	Control Flow Graph	One-to-One
[38]	Gonzalez-Gomez et al.	Hybrid	Dynamic	Continuous	Behavioral and ML	One-to-One
[39]	Li Calsi and Zaccaria	Hybrid	Dynamic	Discrete	Behavioral and ML	One-to-One
[40]	Kohli et al.	Software	Dynamic	Discrete	Behavioral and ML	Many-to-One

ID	Author(s)	Root of Trust	Evidence Type	Evidence Gathering	Verification	Scalability
[41]	Delgado-Lozano et al.	Hybrid	Dynamic	Continuous	Behavioral and ML	One-to-One
[42]	Chen et al.	Software	Dynamic	Continuous	Behavioral and ML	One-to-One
[43]	Mondal et al.	Hardware	Dynamic	Continuous	Behavioral and ML	Many-to-One
[44]	Kassem et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[45]	Sponziello et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[46]	Rabbani et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[47]	Zhan et al.	Hybrid	Dynamic	Continuous	Control Flow Graph	One-to-One
[48]	Dushku et al.	Hybrid	Dynamic	Continuous	Behavioral and ML	Many-to-One
[49]	Dushku et al.	Hybrid	Static	Discrete	Whitelist	Many-to-Many
[50]	Wang et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[51]	Eckel et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[52]	Ott et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[53]	Zhang et al.	Hybrid	Dynamic	Continuous	Control Flow Graph	One-to-One
[54]	Ammar et al.	Hybrid	Dynamic	Continuous	Control Flow Graph	Many-to-One
[55]	Morbitzer et al.	Hybrid	Dynamic	Continuous	Control Flow Graph	One-to-One
[56]	De Oliveira Nunes et al.	Hardware	Dynamic	Continuous	Data Flow Graph	One-to-One
[57]	Calvo and Beltrán	Hybrid	Static	Discrete	Whitelist	Many-to-One
[58]	Diop et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[59]	Ferro et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[60]	Cui et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[61]	Wang et al.	Software	Static	Discrete	Whitelist	Many-to-Many
[62]	Wang and Sun	Hybrid	Static	Discrete	Whitelist	Many-to-Many
[69]	Akkus and Rimac	Hybrid	Dynamic	Continuous	Whitelist	One-to-One
[70]	Alsayed et al.	Hybrid	Dynamic	Continuous	Behavioral and ML	One-to-One
[71]	Ammar and Crispo	Software	Static	Discrete	Whitelist	One-to-One
[72]	Ammar and Crispo	Hybrid	Dynamic	Discrete	Whitelist	Many-to-One
[73]	Ammar et al.	Software	Static	Discrete	Whitelist	Many-to-One
[74]	Antonino et al.	Hybrid	Dynamic	Discrete	Whitelist	One-to-One

ID	Author(s)	Root of Trust	Evidence Type	Evidence Gathering	Verification	Scalability
[75]	Arfaoui et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[76]	Bansal and Sikdar	Hardware	Static	Discrete	Whitelist	Many-to-One
[77]	Bansal et al.	Hardware	Static	Discrete	Whitelist	Many-to-One
[78]	Calsi and Nötzel	Hardware	Static	Discrete	Whitelist	Many-to-One
[79]	Chen et al.	Hybrid	Static	Discrete	Whitelist	Many-to-Many
[80]	Cloosters et al.	Hybrid	Dynamic	Continuous	Control Flow Graph	One-to-One
[81]	Cremers et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[82]	Dhar et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[83]	Dileesh and Shanthi	Software	Dynamic	Continuous	Data Flow Graph	One-to-One
[84]	Eckel and Riemann	Hybrid	Static	Discrete	Whitelist	One-to-One
[85]	Fotos et al.	Hybrid	Static	Discrete	Whitelist	Many-to-Many
[86]	Garah et al.	Software	Static	Discrete	Whitelist	One-to-One
[87]	Garah et al.	Software	Static	Discrete	Whitelist	One-to-One
[88]	Gong et al.	Software	Dynamic	Continuous	Behavioral and ML	Many-to-Many
[89]	Gregor et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[90]	Halldórsson et al.	Hybrid	Dynamic	Continuous	Control Flow Graph	Many-to-One
[91]	Imam et al.	Hybrid	Dynamic	Continuous	Data Flow Graph	Many-to-One
[92]	Jarkas et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[93]	Kim et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[94]	King and Wang	Hybrid	Static	Discrete	Whitelist	One-to-One
[95]	Kuang et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[96]	Kucab et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[97]	Kumar et al.	Software	Static	Discrete	Whitelist	Many-to-One
[98]	Li et al.	Hybrid	Static	Discrete	Whitelist	Many-to-Many
[99]	Lin and Wu	Hybrid	Static	Discrete	Whitelist	Many-to-One
[100]	Lin et al.	Software	Dynamic	Continuous	Whitelist	Many-to-One
[101]	Ling et al.	Hybrid	Dynamic	Discrete	Whitelist	One-to-One
[102]	Liu et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[103]	Liu et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[104]	Mansouri et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[105]	Matsumoto et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[106]	Ménétrey et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[107]	Ménétrey et al.	Hybrid	Static	Discrete	Whitelist	One-to-One

ID	Author(s)	Root of Trust	Evidence Type	Evidence Gathering	Verification	Scalability
[108]	Mohammad and Farahmandi	Hardware	Dynamic	Discrete	Whitelist	One-to-One
[109]	Moon and Shin	Software	Static	Discrete	Whitelist	Many-to-One
[110]	Niemi et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[111]	Oliver	Hybrid	Static	Discrete	Whitelist	Many-to-One
[112]	Ozga et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[113]	Ozga et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[114]	Papamartzivanos. et al.	Hybrid	Dynamic	Continuous	Control Flow Graph	One-to-One
[115]	Pontes et al.	Hybrid	Static	Discrete	Whitelist	Many-to-One
[116]	Preibsch et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[117]	Ren et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[118]	Shang et al.	Hybrid	Dynamic	Discrete	Whitelist	Many-to-One
[119]	Shepherd et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[120]	Shur et al.	Software	Dynamic	Discrete	Whitelist	One-to-One
[121]	Sisinni et al.	Hybrid	Static	Discrete	Whitelist	Many-to-Many
[122]	Usama et al.	Hybrid	Dynamic	Discrete	Whitelist	One-to-One
[123]	Walther et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[124]	Wang et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[125]	Wang et al.	Hybrid	Dynamic	Discrete	Behavioral and ML	Many-to-One
[126]	Weinhold et al.	Hybrid	Static	Discrete	Whitelist	One-to-One
[127]	Xiang et al.	Hardware	Static	Discrete	Whitelist	Many-to-One
[128]	Yang et al.	Hybrid	Static	Discrete	Whitelist	Many-to-Many
[129]	Yu and Huang	Hybrid	Static	Discrete	Whitelist	Many-to-One
[130]	Vasiliadis et al.	Software	Dynamic	Discrete	Control Flow Graph	Many-to-One
[131]	Yang et al.	Hybrid	Static	Discrete	Whitelist	One-to-One