IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 16 June 2026, accepted 7 July 2026, date of publication 13 July 2026, date of current version 17 July 2026.

*Digital Object Identifier 10.1109/ACCESS.2026.3712376*

SURVEY

# Trust Quantification on Zero Trust Architecture: A Survey

**SEUNG-WOO NAM, GYEONG-MIN YU, (Graduate Student Member, IEEE), YOON-SEONG JANG, (Graduate Student Member, IEEE), JU-SUNG KIM, JI-MIN KIM, AND MYUNG-SUP KIM**
Department of Computer and Information Science, Korea University, Sejong Campus, Sejong 30019, South Korea

Corresponding author: Myung-Sup Kim (tmskim@korea.ac.kr)

This work was supported in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by Korean Government [Ministry of Science and Information and Communications Technology (MSIT)] through the Development of Standards for Quantum Cryptography-Based Zero Trust Secure Network/Service and Control/Management Against Quantum Computer Attacks under Grant RS-2025-02219319, and in part by IITP funded by Korean Government (MSIT) through the Development of Security Monitoring Technology-Based Network Behavior Against Encrypted Cyber Threats in ICT Convergence Environment under Grant 00235509.

**ABSTRACT** Zero Trust Architecture (ZTA) has emerged as a prominent security paradigm that moves beyond traditional network perimeter–based security by continuously verifying all access requests. In this paradigm, Trust Quantification (TQ) plays a critical role by numerically evaluating the trustworthiness of users, devices, sessions, and behaviors, thereby enabling dynamic access control and policy decision-making. To date, ZTA and TQ have been surveyed in isolation from one another. Existing surveys on ZTA primarily focus on architectural structures, policy components, and system frameworks, while an in-depth analysis of TQ mechanisms has remained limited. Conversely, surveys on TQ have mainly concentrated on model analysis and performance comparison, without considering the specific characteristics and requirements of ZTA environments. Therefore, this study investigates existing studies on TQ within the context of ZTA and presents an integrated analytical framework for systematic comparison and evaluation. The proposed framework divides the TQ process into three stages: 1) Data Collection; 2) Data Pre-Processing; and 3) Trust Quantification Model. In addition, it incorporates evaluation criteria derived from the core tenets of ZTA. Based on this framework, existing TQ approaches designed for ZTA environments were systematically analyzed and evaluated. Through a stage-wise analysis, this study identifies the limitations of current TQ research and provides an academic foundation for guiding future research directions in trust quantification for ZTA systems.

**INDEX TERMS** Zero trust, trust management, network security, access control, risk assessment.

## I. INTRODUCTION

Zero Trust Architecture (ZTA) [1] is a security paradigm proposed to overcome the limitations of traditional perimeter-based security models, which assume implicit trust by distinguishing between internal and external networks. Because perimeter-based security models are vulnerable to cyber threats such as internal system compromise and lateral movement attacks, ZTA introduces key principles—such as the assumption of breach and continuous verification—to eliminate access decisions based solely on network location or pre-established trust relationships.

In a ZTA environment, all entities, including users, devices, applications, and services, are assumed to be potentially compromised. As a result, every access request to a resource requires authentication at the individual session level, enforcement of least-privileged access, and continuous verification [1]. To support this process, ZTA adopts architecture in which access decisions are made based on dynamically changing contextual information rather than static security policies. Such contextual information includes the user identity, device status, network behavior, environmental conditions, and historical activity records.

The associate editor coordinating the review of this manuscript and approving it for publication was Mueen Uddin.

At this point, the discussion naturally connects to Trust Quantification (TQ), which is a key requirement in ZTA environments. TQ refers to the process of representing the trust level of an entity or session as a numerical and measurable value when accessing a specific resource. By aggregating various contextual information, TQ converts these signals into continuous trust scores or risk-based indicators, thereby refining access decision mechanisms. In ZTA systems, TQ is typically performed during the policy decision process through trust algorithms or risk evaluation engines. These mechanisms compute trust scores by integrating multiple contextual signals, including identity attributes, device status, behavioral patterns, and environmental information, thereby supporting dynamic access control decisions. As access requests in ZTA environments are determined based on dynamically calculated trust values, research on TQ models applicable to ZTA security architectures has gradually increased.

In prior studies, numerous survey papers have addressed ZTA and TQ as separate research topics, contributing significantly to the theoretical foundation and technological development of each field. Survey studies on ZTA have mainly focused on architectural components, policy structures, access control workflows, and deployment scenarios, thereby systematizing the conceptual framework and implementation strategies of Zero Trust. In contrast, survey studies on TQ have categorized and analyzed trust models across various domains such as network systems, the Internet of Things (IoT), distributed environments, electronic commerce, and human–machine interactions. These studies typically compare different trust modeling approaches, including probabilistic models, reputation-based models, fuzzy logic–based methods, and machine learning–based techniques.

However, integrated studies that systematically analyze TQ mechanisms while reflecting the security characteristics of ZTA and its session-based dynamic access control context remain relatively limited. Although NIST SP 800-207 introduces the concept of a Trust Algorithm, its discussion remains largely conceptual. Furthermore, while TQ research within ZTA has been explored and applied across various domains, existing surveys on ZTA-related trust mechanisms have not analyzed these studies from the perspective of the conceptual definition and structural dimensions of trust within ZTA. In addition, limited research has examined the entire TQ process—from data input and processing to trust evaluation—in an integrated manner. A systematic classification framework that analyzes TQ models while explicitly considering the principles of ZTA is also lacking.

This section outlines the two core concepts that constitute the theoretical foundation of this study: ZTA and TQ. First, the concept and structural characteristics of ZTA are introduced, and the research scope addressed in this survey is clearly defined. Subsequently, the conceptual definition and general properties of TQ are briefly summarized to establish the an analytical basis for the discussions presented in the following sections.

To address this research gap, this paper presents a comprehensive survey that systematically organizes and analyzes TQ in ZTA environments. Specifically, this study makes three primary contributions. First, it redefines the conceptual definition and structural dimensions of trust based on ZTA tenets and proposes trust evaluation criteria derived from these principles. Second, it classifies the TQ process into three stages—Data Collection, Data Pre-Processing, and Trust Quantification Model—and proposes an analytical framework that enables stage-wise evaluation based on ZTA tenets. Third, this study conducts a comprehensive analysis of the evolution of ZTA research and systematically categorizes existing TQ studies within ZTA according to the proposed framework, enabling comparative analysis of their characteristics and limitations. The main contributions of this study can be summarized as follows:

- Establishing the conceptual definition and structural dimensions of trust based on ZTA tenets
- Proposing a framework for analyzing TQ by dividing the process into three stages
- Analyzing the research trends of ZTA and systematically comparing and analyzing 50 TQ studies in ZTA environments

The remainder of this paper is organized as follows. Section II introduces the fundamental concepts of ZTA and TQ and defines the scope of this survey. Section III describes the literature search strategy and reviews the relevant studies. Section IV presents the taxonomy of TQ in ZTA environments. Section V defines the evaluation criteria for each stage of the taxonomy. Section VI analyses the surveyed studies based on the proposed evaluation criteria. Finally, Section VII concludes the study and discusses future research directions.

## II. ZERO TRUST ARCHITECTURE AND TRUST QUANTIFICATION

### A. ZERO TRUST ARCHITECTURE

As discussed earlier, ZTA is a security paradigm proposed to overcome the limitations of traditional perimeter-based security models. Fig. 1 illustrates the architecture of ZTA. In general, ZTA can be divided into two main components: the Control Plane and the Data Plane.

#### 1) CONTROL PLANE

In ZTA, the Control Plane refers to the logical domain responsible for policy decisions and security evaluations regarding access requests. The Control Plane includes a Policy Decision Point (PDP), that consists of a Policy Engine (PE) and a Policy Administrator (PA). In this architecture, TQ operates within the PE, where it quantifies the trust level of the data received by the PA and applies policies based on the quantified trust values. The PDP dynamically enforces access policies by collecting and analyzing various types of information, including user identity attributes, device security status, behavioral history, and environmental context.

Access decisions in ZTA are not solely based on the success or failure of authentication. Rather, they incorporate session-level risk assessment and trust evaluation. In this process, TQ operates as a core computational mechanism

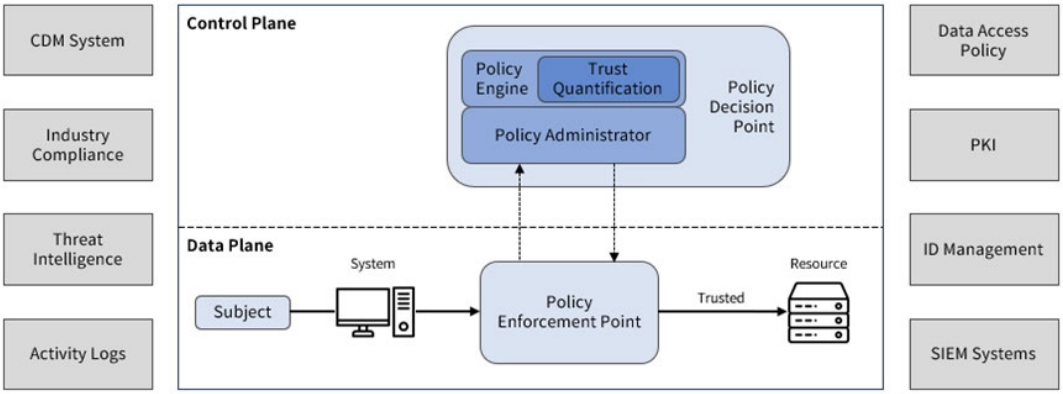


**FIGURE 1.** Zero trust architecture.

within the Control Plane to support policy decisions. Specifically, TQ aggregates heterogeneous contextual information and security indicators to compute a trust score, which is then delivered to the Policy Engine. Based on this quantified trust value, the system determines whether to grant access, require additional authentication, assign restricted privileges, or deny the request altogether.

Accordingly, the scope of TQ research considered in this survey was principally confined to trust computation mechanisms implemented within the Control Plane. More specifically, the analysis focuses on: (1) data collection structures for trust estimation, (2) feature extraction and preprocessing procedures, (3) trust score computation models, and (4) trust value representations. In summary, the Control Plane constitutes the primary operational domain in which TQ is realized in ZTA environments, and this study aims to systematically analyze the trust computation models and architectural designs proposed within this domain.

### 2) DATA PLANE

In ZTA, the Data Plane refers to the operational domain where actual user traffic and resource access requests are transmitted and processed. It includes the Policy Enforcement Point (PEP), which enforces the policies determined by the Control Plane by allowing or denying access and managing session establishment, maintenance, and termination. The Data Plane generates operational data such as network traffic flows, session states, and resource access logs. This information is subsequently transmitted back to the Control Plane, where it is utilized for continuous monitoring and trust re-evaluation.

However, the primary focus of this survey is not on traffic-handling techniques within the Data Plane itself, but rather on the TQ mechanisms executed in the Control Plane that leverage observational data produced by the Data Plane. Accordingly, technologies related to data transmission and protection—such as traffic encryption and network segmentation—are considered beyond the scope of this analysis.

In summary, ZTA performs dynamic access control based on the separation between the Control Plane and the Data Plane, and TQ is primarily implemented within the Control Plane. Accordingly, this study clearly defines the hierarchical scope in which trust quantification is positioned within the ZTA architecture and systematically classifies and analyzes TQ models centered on the Control Plane.

### 3) ZTA TENET

As described earlier, NIST SP 800-207, which forms the foundation of ZTA, defines seven core ZTA tenets [1]. Their definitions and detailed explanations are summarized as follows.

- **All data sources and computing services are considered resources (All entities as resources)**: In a ZTA environment, not only server data but also objects, services, and applications are treated as resources. This principle implies that all entities, regardless of whether they are internal or external, must be protected.
- **All communication is secured regardless of network location (Location-independent trust prohibition)**: In a ZTA environment, the same security requirements must be applied to all communications regardless of whether they originate from internal or external networks.
- **Access to individual enterprise resources is granted on a per-session basis (Least privilege principle)**: Access is granted on a per-session basis, and privileges must be limited to the minimum necessary to perform the requested task. This implies that trust evaluation mechanisms should be capable of assigning privileges appropriate to the requester's intended operation.
- **Access to resources is determined by dynamic policy (Dynamic policy decision)**: Trust evaluation should incorporate observable attributes such as the identity status of the requesting entity and the status of applications or services. This indicates that trust quantification should consider not only access request data but also behavioral and environmental attributes.
- **The enterprise monitors and measures the integrity and security posture of all owned and associated assets (Continuous monitoring and log analysis)**: When evaluating resource access requests, the ZTA system must also assess the security posture of the relevant

assets. This implies that ZTA implementations should incorporate mechanisms for continuous internal diagnostics and apply patches or corrective actions when necessary.

- **All resource authentication and authorization are dynamic and strictly enforced before access is allowed (Continuous verification)**: Trust must be continuously re-evaluated from the moment an access request is initiated until the session is terminated. This requires continuous monitoring throughout user transactions, along with re-authentication and re-authorization based on defined policies.
- **The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture (Full information-based security)**: Organizations should collect as much information as possible regarding access requests and system states in order to strengthen their security posture. ZTA systems gather data related to security status, network traffic, and access requests, and use the insights derived from these data to improve policy generation and enforcement.

The summarized ZTA tenets not only normatively present the security principles required in ZTA environments but also provide structural criteria for how trust should be handled within the architecture. These tenets can serve as conceptual evaluation criteria for assessing TQ models. For example, they can be used to examine whether a TQ model utilizes diverse and multidimensional data—such as entity information, communication environment status, and security patch status—when evaluating trust (Dynamic policy decision), whether the model is continuously improved based on collected data (Continuous monitoring and log analysis), and whether the TQ model is designed to consider not only internal communications but also external communications (All entities as resources). In other words, the ZTA tenets extend beyond simple operational security guidelines and can function as analytical criteria that define the requirements a trust quantification model should satisfy within a ZTA environment.

### B. TRUST QUANTIFICATION

TQ refers to the concept of representing trust as a quantitative value. In other words, it is the process of numerically expressing how trustworthy a particular entity (e.g., user, device, or service) or a specific session is. Unlike binary decisions such as trustworthy or untrustworthy, TQ represents trust levels using continuous values or graded scales, thereby enabling more fine-grained decision-making.

Trust quantification was performed based on observable information. This information may include the entity state information, behavioral history, environmental context, and security attributes. These factors are evaluated according to predefined criteria, and the resulting trust assessment is typically expressed in forms such as scores, probabilities, or risk values.

A key characteristic of trust quantification is that trust is treated not as a fixed attribute but as a variable that can change depending on context and time. That is, trust is calculated based on observable information at a specific point in time and can be re-evaluated when new information becomes available. Therefore, trust quantification should be understood not merely as a static classification of states, but as a dynamic decision-making mechanism that continuously updates its assessment through the accumulation and interpretation of observational data.

In the context of ZTA, TQ functions as a mechanism that supports decision-making for access requests. However, in this section, TQ is defined in a general sense as the process of representing trust in a quantitative form and utilizing it in decision-making, without assuming any specific model or technique. Based on this conceptual definition, the following sections analyze trust quantification studies implemented within ZTA environments.

## III. RELATED WORK

This section reviews prior survey studies conducted in the domains of ZTA and TQ in order to clarify the positioning and distinctiveness of the present work. Since this study aims to systematically analyze TQ within ZTA environments, the related literature is examined along two primary dimensions: (1) surveys on ZTA and (2) surveys on TQ.

### A. SEARCH STRATEGY

This section describes the search strategy and keyword selection process used to systematically identify the survey literature related to ZTA and TQ. As this study aims to analyze research trends in TQ within ZTA environments, the focus was placed not merely on collecting individual research articles, but on prioritizing publications that exhibit a survey-oriented nature in each domain.

The literature search was conducted using Google Scholar, which provides one of the most comprehensive academic indexing platforms currently available. Google Scholar was selected as the sole search source for three reasons. First, its indexing coverage broadly encompasses major academic databases, including IEEE Xplore, ACM Digital Library, and Scopus, allowing it to function as a superset rather than a competing source. Second, Google Scholar supports the ''intitle:'' operator, which enables title-based precision searching equivalent to the title-field search of dedicated databases; this capability was central to our keyword design, in which candidate papers were identified by the presence of target terms in their titles. Third, ZTA and TQ constitute a rapidly emerging research area in which a substantial portion of recent work appears as preprints, theses, and early-access articles that are not yet indexed in conventional databases. Relying on Google Scholar therefore reduced the risk of omitting the most recent studies, which is particularly important given that the majority of the surveyed works were published in 2025 or later. The search strategy was structured into three primary categories. The first keyword set was designed to identify survey studies on ZTA. The second keyword set targeted survey literature on TQ. The third keyword set was

formulated to identify studies specifically addressing TQ within ZTA environments, which constitutes the central focus of this study. The selected keywords and filtering criteria were as follows:.

- **ZTA Survey Search Keyword**: (intitle:"ZTA" OR intitle:"Zero Trust" OR intitle:"ZT") and (intitle:"survey" OR intitle:"review")
- **TQ Survey Search Keyword**: (intitle:"Trust Quantification" OR intitle:"Trust Evaluation" OR intitle:"Trust Scoring" OR intitle:"Trust Assessment" OR intitle:"Trust Modeling" OR intitle:"Trust Computation") AND (intitle:"survey" OR intitle:"review")
- **ZTA-based TQ Search Keyword**: (intitle:"Trust Quantification" OR intitle:"Trust Evaluation" OR intitle:"Trust Scoring" OR intitle:"Trust Assessment" OR intitle:"Trust Modeling" OR intitle:"Trust Computation") AND ("ZTA" OR "Zero Trust")

It should be noted that the first two keyword sets include the terms "survey" or "review" because they are intended to identify existing survey and review literature on ZTA and TQ for the Related Work analysis. In contrast, the third keyword set deliberately omits these terms, as its purpose is to retrieve primary studies that implement and evaluate trust quantification within ZTA environments—the individual works that constitute the analysis set in Section VI. Including "survey" or "review" in this third set would have excluded the primary studies that are the actual subject of this analysis.

Each search keyword was primarily selected based on the titles of research papers. If a keyword appeared in the title of a study, the paper was included as a candidate for analysis. The title-based (intitle) search was adopted to prioritize precision, ensuring that the retrieved papers address trust quantification as a central topic rather than mentioning it only peripherally. To reduce the recall loss inherent in title-only searching, a broad set of synonymous expressions—"Trust Quantification," "Trust Evaluation," "Trust Scoring," "Trust Assessment," "Trust Modeling," and "Trust Computation"—was combined disjunctively, so that studies addressing trust quantification under different terminology in their titles would still be captured. Studies that discuss trust quantification only incidentally in the body text, without reflecting it as a primary contribution in the title, generally fall outside the analytical scope of this survey, which targets studies that explicitly implement and evaluate trust quantification within ZTA environments.

The selected studies included a small number of theses (e.g., [79], [84]); consistent with the search strategy described above, which was designed to capture recent grey literature such as preprints and theses, these were included under the same criteria as peer-reviewed work. As both were published in 2025, no citation threshold was applied to them, in line with the year-specific thresholds defined above.

The publication period for the literature search was set from 2020 to the present, considering the release of the NIST SP 800-207 document in 2020. In addition, a minimum citation threshold was applied to prioritize the studies that have been referenced by a substantial number of subsequent studies. Specifically, papers published between 2020 and 2022 were required to have at least 20 citations, papers published between 2023 and 2024 were required to have at least 10 citations, and papers published from 2025 to the present were included without a citation threshold.

For the ZTA survey search strategy, only the studies specifically related to the Zero Trust domain were selected as the final analysis set. Similarly, in the TQ survey search process, only studies directly related to trust quantification were retained for analysis. For the search of TQ studies within ZTA environments, only studies that included performance evaluation results were ultimately selected.

### B. SEARCH RESULTS

Based on the search strategy defined in the previous section, survey literature on ZTA and TQ was systematically collected. The overall selection process for the three keyword sets is summarized in Fig. 2, which presents a PRISMA-style flow diagram of the records identified, screened, and finally included at each stage. For each keyword set, records were first excluded when the full text was inaccessible (citation-only entries or paywalled papers), then filtered by the year-specific citation thresholds described in Section III-A, and finally screened for relevance to the respective domain. This process yielded 53 ZTA survey studies, 7 TQ survey studies, and 50 ZTA-based TQ studies. Table 1 presents the results of the ZTA survey literature review.

A total of 53 ZTA survey studies were included. When examining the temporal distribution of these surveys, 5 studies were published between 2020 and 2022, 16 studies between 2023 and 2024, and 32 studies from 2025 to the present. This distribution indicates that ZTA research has recently gained significant attention.

The year-specific citation thresholds, while intended to prioritize substantively referenced works, introduce a temporal bias that warrants closer examination. Because the threshold has decreased in recent years and has been removed entirely from 2025 onward, recent publications are systematically more likely to pass the filter than older ones. As shown in Fig. 2, none of the records published from 2025 onward were excluded from the citation grounds, whereas a substantial share of the earlier records was removed by this criterion. This asymmetry directly influences the relative proportion of recent studies in the final set. Consequently, the apparent dominance of 2025 publications in the analyzed studies should not be read solely as evidence of a surge in research activity; part of this concentration is an artifact of the filtering criteria, as comparable studies from earlier years were disproportionately removed. Nonetheless, the thresholds were retained to ensure that older studies included in the analysis demonstrated scholarly impact, balancing recency against citation-based quality. Readers should therefore interpret year-wise distributions as reflecting both genuine growth in ZTA-based TQ research and the structural effect of the citation filter.

ZTA research has been conducted across a wide range of domains. Fig. 3 illustrates the distribution of research fields derived from the titles and keywords of existing ZTA survey studies. The identified categories include Network Security,

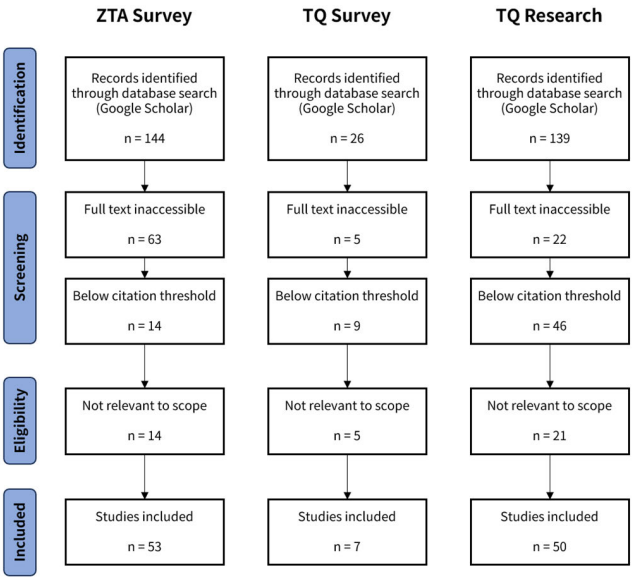


**FIGURE 2.** Selection process for the three keyword sets.

Artificial Intelligence (AI), IoT Security, Cloud Security, 5G/6G Security, Vehicle Security, and Others (including Blockchain, Web3, UAV Security, and VPN, each represented by one study). Among these categories, Network Security accounted for the largest proportion, representing approximately 40% of the surveyed studies. This is expected because ZTA primarily operates within communication network environments. AI-related research accounts for approximately 17% of the studies, while additional survey research has been conducted in areas such as IoT Security and Cloud Security. These findings indicate that ZTA is actively studied across most domains where networked systems are deployed, highlighting its significance as a promising research area.

The collected survey papers can be categorized into six analytical and descriptive structures, as summarized below.

- Taxonomy-First [2], [5], [7], [14], [16], [18], [23], [26], [35], [40], [46], [47], [48], [53], [54]: This structure organizes ZTA elements, technologies, threats, and challenges into hierarchical taxonomies. It represents a traditional survey format that classifies technologies and components into structured comparison tables.
- Component-Loop [3], [8], [11], [12], [32], [33]: This approach centers on architectural workflows, including policy decision, enforcement, signal collection, and resource management. Trust is typically introduced as one module within the architecture, and ZTA is described from a system-level or architectural circuit perspective.
- Technology-Catalog [20], [25], [31], [38], [43], [50]: This structure comparatively examines specific technologies that replace or enhance traditional security mechanisms, such as authentication, authorization, Software-Defined Perimeter (SDP), and micro-segmentation.
- Migration/Adoption [6], [19], [29], [41], [52]: This category focuses on ZTA adoption roadmaps, migration strategies, and operational considerations during implementation.
- Domain-Specific [4], [9], [10], [13], [15], [17], [21], [22], [24], [28], [30], [34], [37], [42]: These surveys specialize in applying ZTA concepts to specific domains, including cloud computing, IoT, 5G/6G networks, vehicular systems, and UAV environments.
- AI-Enhanced [27], [36], [39], [44], [45], [49], [51]: This structure emphasizes machine learning and artificial intelligence techniques for anomaly detection, risk scoring, and automated policy management within ZTA frameworks.

Fig. 4 illustrates the distribution of the analytical and descriptive structures used in existing ZTA survey studies. This classification shows that prior ZTA surveys have been organized from various perspectives, includng taxonomy-oriented approaches, component-based analyses, technology-oriented approaches, and migration strategy–focused analyses. These perspectives indicate that ZTA is not merely a single technical solution but rather an architectural paradigm that requires multi-layered analysis.

Although each survey was categorized according to its primary analytical perspective, several studies exhibited characteristics spanning multiple categories. For example, some AI-enhanced surveys also adopt taxonomy-oriented structures, while certain domain-specific surveys simultaneously analyze architectural control loops. This observation suggests that recent ZTA survey research increasingly integrates multiple analytical perspectives rather than adhering to a single classification style.

Furthermore, when examining recent research trends after 2025, it can be observed that dynamic decision-making models based on machine learning (ML) and artificial intelligence (AI) are increasingly being adopted, moving beyond the traditional static rule-based policy approaches. This trend can be interpreted as a technological evolution aimed at more accurately implementing the dynamic policy decisions and context-aware evaluations required in ZTA environments.

Nevertheless, a common limitation observed across existing ZTA survey studies is the lack of a systematic and in-depth analysis of trust quantification (TQ) within ZTA. Although some studies [5], [11], [20], [22], [26], [27], [28], [34], [36], [42], [44], [51] briefly mention TQ-related aspects, these discussions are typically limited to describing TQ as a supporting functional component of ZTA implementation or simply listing related studies. This observation suggests that the scope of ZTA research has traditionally been structured around architectural design and policy mechanisms rather than focusing on trust quantification as a core analytical subject.

Table 2 presents the literature review results for TQ survey studies. A total of seven survey papers were identified. When examining the quantitative distribution of these studies, it can be observed that the number of TQ surveys is significantly smaller compared to ZTA surveys. This outcome may partly result from the minimum citation threshold applied in the search strategy for the different publication years. Nevertheless, the results still indicate that the overall research

**TABLE 1.** Zero trust architecture survey search results.

| No. | Year | Focus Area | Key Contributions | Limitation compared to our paper |
|---|---|---|---|---|
| [2] | 2021 | Network Security | Multivocal zero-trust review proposing framework, gaps, and future research directions | No detailed analysis of trust quantification |
| [3] | 2022 | Network Security | Authentication and access control technology–based integrated and systematic ZTA survey | No detailed analysis of trust quantification |
| [4] | 2022 | Blockchain | Strengthening and Systematizing Zero Trust Architecture Systems Using Blockchain Immutability Survey | No detailed analysis of trust quantification |
| [5] | 2022 | Network Security | Systematic organization of ZTA components and core elements review | Lack of detailed analysis of trust quantification |
| [6] | 2022 | Cloud Security | Compares ZTA approaches, challenges, and migration strategies for secure cloud networks | No detailed analysis of trust quantification |
| [7] | 2023 | Network Security | Reinterprets zero trust from the perspective of trust in network security and systematically establishes the concept, characteristics, and principles of trust | No detailed analysis of trust quantification |
| [8] | 2023 | Network Security | Systematic analysis of Zero Trust adoption, architecture, benefits, and challenges | No detailed analysis of trust quantification |
| [9] | 2023 | Web3 | Analyzes Web3 ecosystem, impacts, integrations, zero-trust architectures, and adoption solutions | No detailed analysis of trust quantification |
| [10] | 2024 | 6G Network | Analyzes ZTA applicability, principles, cases, challenges, and future directions for 6G security | No detailed analysis of trust quantification |
| [11] | 2024 | Cloud Security | Analyzes Zero Trust research, compares approaches, identifies limitations, and suggests future directions | Lack of detailed analysis of trust quantification |
| [12] | 2024 | Network Security | Endogenous architecture and SPA to extend and operationalize zero trust beyond single-policy models | No detailed analysis of trust quantification |
| [13] | 2024 | IoT Security | Proposes IoT-tailored ZTA framework with analysis and practical deployment guidelines | No detailed analysis of trust quantification |
| [14] | 2024 | AI | Comprehensive analysis of Zero Trust transition, integrating AI, quantum computing, and XDR with implementation guidelines | No detailed analysis of trust quantification |
| [15] | 2024 | UAV Security | Systematic analysis of Zero Trust and ML for secure military UAV threat detection | No detailed analysis of trust quantification |
| [16] | 2024 | Network Security | Proposes unified adaptive framework addressing zero trust implementation gaps and challenges | No detailed analysis of trust quantification |
| [17] | 2024 | IoT Security | Analyzes behavioral factors improving authentication and authorization in Zero Trust IoT frameworks | No detailed analysis of trust quantification |
| [18] | 2024 | Network Security | Comprehensive ZTA analysis with implementation guidance and future integration insights | No detailed analysis of trust quantification |
| [19] | 2024 | Cloud Security | Analyzes AI's role in zero trust cloud security for risk reduction and trust enhancement | No detailed analysis of trust quantification |
| [20] | 2024 | VPN | Proposes validated Zero Trust VPN framework addressing security, scalability, and performance limitations | Lack of detailed analysis of trust quantification |
| [21] | 2024 | IoT Security | ZTA components and integration across practical domains survey, with security and privacy analysis | No detailed analysis of trust quantification |
| [22] | 2024 | Vehicle Security | Comprehensive survey of Zero Trust for connected vehicle security and research gaps | Lack of detailed analysis of trust quantification |
| [23] | 2025 | Network Security | Systematic cross-domain ZTA review highlighting trends, challenges, and IoT-specific gaps | No detailed analysis of trust quantification |
| [24] | 2025 | IoT Security | Systematic mapping study structuring implementation challenges, technologies, and human factors of Zero Trust Management in IoT environments. | No detailed analysis of trust quantification |
| [25] | 2025 | Network Security | Comprehensive multidimensional ZT analysis linking architecture, deployment, practice, challenges, and future directions | No detailed analysis of trust quantification |

**TABLE 1.** *(Continued.)* **Zero trust architecture survey search results.**

| | | | | |
|---|---|---|---|---|
| [26] | 2025 | Network Security | Review of ZTA authentication and authorization evolution, performance, trends, limitations, and future directions. | Lack of detailed analysis of trust quantification |
| [27] | 2025 | AI | Systematic analysis of ZTA from AI-driven threat response perspective identifying real-world gaps and key limitations | Lack of detailed analysis of trust quantification |
| [28] | 2025 | Vehicle Security | Surveys ZTA for vehicular CPS and proposes deep learning–based replay attack detection for HEV BMS | Lack of detailed analysis of trust quantification |
| [29] | 2025 | Network Security | Analysis of ZTNA principles, technologies, challenges, and future directions | No detailed analysis of trust quantification |
| [30] | 2025 | 6G Network | Study proposing a ZTA integration framework for O-RAN | No detailed analysis of trust quantification |
| [31] | 2025 | Cloud Security | Systematic analysis of ZTA micro-segmentation techniques, benefits, challenges, and trends | No detailed analysis of trust quantification |
| [32] | 2025 | Network Security | Systematic comparative analysis review between ZTA and SDP | No detailed analysis of trust quantification |
| [33] | 2025 | Network Security | Systematically analyzes zero trust models, principles, maturity, architectures, benefits, and limitations | No detailed analysis of trust quantification |
| [34] | 2025 | 5G/6G Network | Demonstrates AI's essential role in Zero Trust for 5G/6G and analyzes key challenges | Lack of detailed analysis of trust quantification |
| [35] | 2025 | Network Security | Review of ZTA evolution, core technical components, and use case analysis | No detailed analysis of trust quantification |
| [36] | 2025 | AI | Critically analyzes ZTA gaps under generative AI and proposes CFKC and adaptive defense directions | Lack of detailed analysis of trust quantification |
| [37] | 2025 | IoT Security | Analyzes ZTA for IoT, exposing limits of traditional security and future research directions | No detailed analysis of trust quantification |
| [38] | 2025 | Network Security | Comprehensively analyzes ZTNA and proposes a general deployment framework for modern network security | No detailed analysis of trust quantification |
| [39] | 2025 | AI | AI-driven taxonomy, layered architecture, and practical roadmap for multi-cloud ZTA | No detailed analysis of trust quantification |
| [40] | 2025 | IoT Security | Systematic analysis of five-step Zero Trust for smart homes and IoT, identifying gaps | No detailed analysis of trust quantification |
| [41] | 2025 | AI | Analysis of existing literature considering both ZTA and machine learning techniques | No detailed analysis of trust quantification |
| [42] | 2025 | IoT Security | Systematic review of integrated AI, blockchain, edge, and zero-trust IoT security frameworks | Lack of detailed analysis of trust quantification |
| [43] | 2025 | Cloud Security | Presents a comprehensive review and architectural framework for Zero Trust Security in multi-cloud microservices | No detailed analysis of trust quantification |
| [44] | 2025 | AI | Comparative framework for ML-based anomaly detection, integrating data, features, and metrics in ZTNA | No analysis of trust modeling |
| [45] | 2025 | AI | Systematic zero-trust framework and research directions for multi-LLM systems in EGI. | No detailed analysis of trust quantification |
| [46] | 2025 | Network Security | Comparative analysis survey of perimeter-based security models and zero trust models | No detailed analysis of trust quantification |
| [47] | 2025 | Network Security | Survey based on application cases of zero trust security | No detailed analysis of trust quantification |
| [48] | 2025 | Network Security | Systematic literature review on ZTA in educational institutions | No detailed analysis of trust quantification |
| [49] | 2025 | AI | Proposes secure multi-party AI training via zero-trust federated data warehousing | No detailed analysis of trust quantification |
| [50] | 2025 | Cloud Security | Practical taxonomy, real benchmarks, deployment patterns, and decision frameworks for micro-segmentation | No detailed analysis of trust quantification |
| [51] | 2025 | AI | AI-driven observability framework and architectural guidance enhancing Zero Trust security resilience | Lack of detailed analysis of trust quantification |
| [52] | 2025 | Cloud Security | Systematically analyzes strategies and key mechanisms for modernizing IT audit for Zero Trust cloud security. | No detailed analysis of trust quantification |
| [53] | 2025 | Network Security | Systematic taxonomy and analysis of ZTA applications, technologies, and adoption challenges | No detailed analysis of trust quantification |
| [54] | 2025 | Network Security | Proposes SUT matrix and unified framework integrating human factors for adaptive Zero Trust | No detailed analysis of trust quantification |

interest in TQ surveys is relatively lower than that in ZTA surveys.

An analysis of the collected TQ survey studies shows that many surveys categorize and compare trust models based on specific modeling approaches, such as machine learning (ML) [55] and Bayesian methods [56]. In addition, several studies have focused on domain-specific surveys, including IoT environments [57], distributed networks [58], and 6G systems [59].

However, most of these studies primarily focus on the general structure of trust models, their mathematical foundations, or their application domains, and do not provide systematic analyses that consider the structural characteristics of ZTA. A recent study [61] surveyed TQ-related papers within ZTA environments; however, its analysis mainly focused on the performance evaluation.

This observation indicates that there is still a lack of survey research that systematically analyzes TQ from the perspective of ZTA's structural principles and operational mechanisms while providing an integrated comparison of the entire pipeline—from data design and preprocessing to model construction. This suggests that TQ in ZTA should not be treated merely as a performance optimization problem but rather analyzed in conjunction with the structural principles of ZTA.

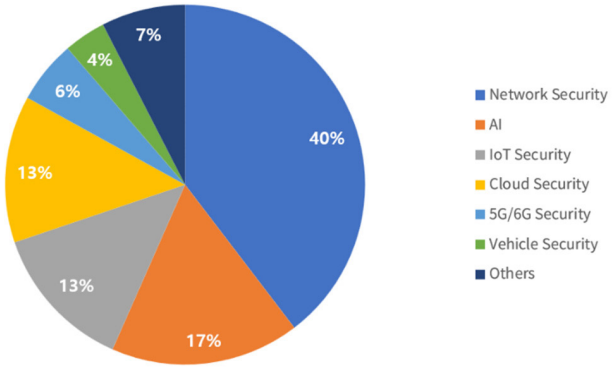


**FIGURE 3.** Distribution of ZTA survey papers by research area.

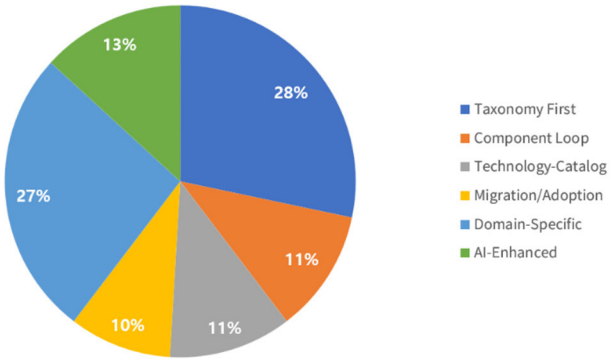


**FIGURE 4.** Distribution of ZTA Survey papers by analysis and description method.

## IV. TAXONOMY

As discussed in the previous sections, the two fields have matured along separate trajectories, leaving the connection between trust computation and ZTA's structural principles underexplored. Consequently, a comprehensive analytical framework that systematically structures TQ research within the context of ZTA has not been sufficiently presented. Therefore, this section proposes a taxonomy for analyzing TQ studies in ZTA environments. The proposed taxonomy is designed as an analytical framework that systematically categorizes TQ research by reflecting both the structural characteristics of TQ and the security principles defined by the ZTA tenets. Through this framework, it becomes possible to structurally compare how existing studies satisfy the requirements of ZTA and what limitations they exhibit.

As defined earlier, TQ refers to the process of representing the trust level of a specific entity or session as a quantitative value. This trust value is dynamically computed and updated based on observable information. Rather than representing a binary state, trust is typically expressed as a continuous value or graded level and is used as an input to decision-making processes such as access control.

From this perspective, the trust value quantified in TQ is derived through a sequential process that includes the collection of observable information, the transformation of the collected data, and the computation of trust based on the processed information. In other words, the structural process through which the trust value is generated is more important than the resulting value itself. In particular, within ZTA environments, trust must be recalculated according to the contextual conditions of a session at a given time. Therefore, the selection of data, the method of data processing, and the design of the computation model must be closely interconnected.

Based on this understanding, this study conceptualizes TQ in ZTA as a process composed of three interrelated stages. This staged structure enables trust quantification studies to be compared under a consistent analytical framework. The three stages of TQ are defined as follows:

- **Data Collection**: The stage in which observable information used as the basis for trust evaluation is collected.
- **Data Pre-Processing**: The stage in which the collected information is transformed into a computable and comparable format.
- **Trust Quantification Model**: The stage in which trust values are computed based on the processed information.

Structurally, these three stages parallel the standard machine learning pipeline of data collection, preprocessing, and modeling, and we adopt this familiar decomposition deliberately because trust quantification likewise proceeds from observation to representation to computation. The novelty of the proposed taxonomy lies not in the staged structure itself but in how each stage is interpreted and evaluated through the lens of ZTA. Whereas a conventional pipeline evaluates each stage by predictive performance, the proposed framework evaluates each stage against criteria derived from the ZTA tenets—for example, whether data collection preserves temporal context for continuous verification, whether preprocessing retains session structure for least-privilege

**TABLE 2.** Trust quantification survey search results.

| No | Year | Focus Area | Key Contributions | Limitation compared to our paper |
|---|---|---|---|---|
| [55] | 2020 | Network Security | Systematic literature survey on machine learning-based trust evaluation research | ZTA characteristics not considered |
| [56] | 2020 | Network Security | Survey of Bayesian trust models and analysis of generalized Bayesian trust modeling | ZTA characteristics not considered |
| [57] | 2023 | IoT | Comprehensively surveys IoT trust evaluation models, systematizing features, classifications, challenges, and research directions | Limited to the IoT environment |
| [58] | 2023 | Network Security | Systematic review proposing a framework evaluating TMM models' validation, security, and structure | ZTA characteristics not considered |
| [59] | 2024 | 6G Network | Systematic comparison of trust models using fuzzy algorithms with an evaluation framework | ZTA characteristics not considered |
| [60] | 2025 | Network Security | Classification and characteristic comparison of trust modeling strategies | ZTA characteristics not considered |
| [61] | 2026 | Network Security | Systematic TSA analysis and adaptive orchestration framework for scalable, resilient zero-trust security | Performance-focused comparison conducted |

evaluation, and whether the model avoids using network location as a trust label. In this way, the taxonomy reframes a generic processing pipeline as a structured means of assessing how faithfully each stage of trust quantification reflects the security principles of Zero Trust, which to our knowledge has not been systematically formulated in prior TQ or ZTA surveys.

### A. DATA COLLECTION

The Data Collection stage refers to the process of defining and gathering observable information that serves as the basis for trust quantification. At this stage, the primary concern is determining which types of data should be utilized for trust evaluation. In ZTA environments, various types of information may be collected, including user identity attributes, device security status, network traffic characteristics, and behavioral logs.

In this stage, the analysis focuses on whether existing studies perform training and evaluation using data that reflect the principles of ZTA tenets. Specifically, the analysis examines whether the datasets used in TQ research—either public datasets or those generated in simulation environments—are composed of the four key data elements in ZTA contexts (Entity, User, Environment, and Context). In addition, the analysis considers whether the data collection process captures information continuously throughout the entire session and whether both direct observational data and indirect contextual data are collected. Through this examination, the study evaluates whether the data used in TQ research are collected and utilized in a manner consistent with ZTA tenets.

### B. DATA PRE-PROCESSING

The Data Pre-Processing stage refers to the process of transforming collected raw data into a form suitable for trust computation. Observational data are often heterogeneous, large in scale, and difficult to directly compare or process computationally. Therefore, procedures such as normalization, scaling, and feature extraction are applied to structure the meaning of the data and make them suitable for analysis.

The key aspect of this stage is not merely data organization but the design of information representation that influences trust evaluation. Even when the same data are used, the interpretation of the resulting trust value may differ depending on how the data are transformed into features. Accordingly, this stage analyzes whether the preprocessing methods reflect ZTA tenets, including aspects such as temporal dependency, context-awareness, and multi-attribute integration in the representation of trust-related information.

### C. TRUST QUANTIFICATION MODEL

The Trust Quantification Model stage refers to the computational structure that derives the final trust value based on the pre-processed data. At this stage, specific mathematical models, statistical methods, rule-based structures, or learning-based algorithms are employed to generate trust levels in forms such as scores, probabilities, or risk values.

This stage focuses on analyzing and organizing the overall structure of the trust quantification model. In particular, it examines the types of models used for trust evaluation—such as rule-based approaches, probabilistic models, and machine learning–based methods—as well as the mechanisms used to derive trust values. Furthermore, because ZTA requires session-based access control and continuous verification, the analysis also considers key characteristics of the trust models, including real-time capability, scalability, and the ability to support continuous re-evaluation.

## V. EVALUATION CRITERIA

To systematically organize and analyze TQ research within ZTA environments, this section designs a set of evaluation criteria for assessing TQ studies in ZTA.

The proposed evaluation criteria are derived from the ZTA tenets discussed in Section II. The ZTA tenets normatively

define the security principles and operational directions required in Zero Trust environments and include key elements such as dynamic policy decision-making, session-based access control, and continuous verification. These principles extend beyond architectural design guidelines and can serve as structural requirements that trust quantification models should satisfy. Importantly, not only the criteria themselves but also the individual score levels (0/1/2) within each criterion are derived from the corresponding tenet rather than defined arbitrarily. Each score level is designed to represent the increasing degree to which a study satisfies the property that the tenet requires. For example, because the ''all entities as resources'' tenet calls for protection across diverse resource types, the corresponding criterion assigns higher scores to studies that cover more resource categories (infrastructure, platform, and service); and because the ''continuous verification'' tenet requires trust to be re-evaluated over time, its criterion assigns higher scores to data that incorporate temporal and, at the highest level, historical behavioral information. In this way, each score level reflects a graded fulfillment of the underlying tenet, and the complete mapping from each tenet to its operationalized score levels is given in the criterion definitions and in Tables 3–5 below.

- **All entities as resources**: Since all data sources and computing services are considered resources, protection should not be limited to specific servers but should extend to all entities within the system. Therefore, datasets or simulation environments used for trust evaluation should be constructed with this principle in mind, ensuring that relevant data are collected across diverse entities and resources.
- **Location-independent trust prohibition**: Because all communications must be secured regardless of the network location, data should be collected across both internal and external environments. In addition, network location should not be used as a direct basis for trust evaluation.
- **Least privilege principle**: Access should be granted on a per-session basis, and permissions must follow the principle of least privilege. Accordingly, trust evaluation should be conducted at the session or request level rather than solely at the user level, ensuring that the assigned trust level is appropriate for the specific request.
- **Dynamic policy decision**: In addition to access request data, behavioral and environmental attributes should also be considered in trust evaluation. Therefore, datasets should include not only access request information but also additional contextual
- data and logs. Furthermore, the TQ model should be capable of updating the trust values in response to environmental changes.
- **Continuous monitoring and log analysis**: When evaluating trust, the security posture of the relevant assets should also be assessed, and mechanisms for internal monitoring and diagnostics should be incorporated. Accordingly, TQ models should include mechanisms that support continuous system improvement and adaptation during access decision processes.
- **Continuous verification**: Because trust must be continuously re-evaluated until a session is terminated, the data used for trust evaluation should incorporate temporal context. Consequently, the TQ model should be capable of updating trust values based on temporal dynamics.
- **Full information-based security**: Trust quantification should utilize as much relevant information as possible. Therefore, diverse and multidimensional data sources should be collected and integrated for trust evaluation.

Based on the explanations of the seven tenets described above, evaluation criteria are designed for each stage of the TQ process. Tables 3–5 present the evaluation criteria used to assess TQ studies in ZTA environments. Among the seven tenets, the criteria applicable to each stage were selected and formulated as stage-specific evaluation metrics. The corresponding criteria are summarized as follows.

### A. DATA COLLECTION CRITERIA

#### 1) ALL ENTITIES AS RESOURCES

Since ZTA considers all data sources and computing services as resources that must be protected, a TQ model should maintain the same security requirements regardless of the type of resource. Accordingly, a higher score was assigned when a study considered a wider variety of resource types. Resource types are categorized into three levels: infrastructure level (e.g., PCs, servers, and devices), platform level (e.g., virtual machines and containers), and service level (e.g., web applications and API services). The evaluation score was determined based on the number of these resource categories included in the study.

#### 2) LOCATION-INDEPENDENT TRUST PROHIBITION

Because all communications must be protected regardless of the network location, the evaluation examines whether the service communications or attack scenarios considered in a study include both internal and external communications. In this context, internal communication refers to communications occurring within an internal network environment, such as an enterprise network, whereas external communication refers to communications occurring outside the internal network.

#### 3) LEAST PRIVILEGE PRINCIPLE

Since access should be granted on a per-session basis, trust quantification should ideally be performed at the level of individual request actions. In this context, a session refers to the process in which a specific entity requests access to a particular resource and maintains the connection until the task is completed and the session is terminated. If the same entity performs different tasks on the same resource for different purposes, these interactions are considered separate sessions. Accordingly, trust evaluation granularity can be categorized into three levels. The user-level evaluation assesses the trustworthiness of the user as the primary subject of trust. The session-level evaluation evaluates the state of each access session. Action-level evaluation continuously assesses trust

**TABLE 3.** Data collection analysis criteria.

| | 0 | 1 | 2 |
|---|---|---|---|
| 1. All Entities as Resources | One resource type | Two resource type | Three resource types |
| 2. Location-independent Trust Prohibition | Only internal communication scenarios are considered | Both internal and external communication scenarios are considered | Boundaryless real-time open environment |
| 3. Least Privilege Principle | User-level evaluation | Session-level evaluation | Action-level evaluation |
| 4. Dynamic Policy Decision | Only data from the access request itself | Includes two or fewer element-level data types | Includes all element-level data types |
| 5. Continuous Monitoring and Log Analysis | - | - | - |
| 6. Continuous verification | No temporal information included | Temporal information included | Temporal information included with the ability to incorporate historical behavior data |
| 7. Full Information-based Security | Only access request data are used | Additional data sources exist but are not publicly available | Additional collected data sources are available |

**TABLE 4.** Data pre-processing analysis criteria.

| | 0 | 1 | 2 |
|---|---|---|---|
| 1. All Entities as Resources | - | - | - |
| 2. Location-independent Trust Prohibition | Location information used as a label | Location information not used | Location information used as a feature |
| 3. Least Privilege Principle | No session structure information | Indirectly included in the data | Session structure information explicitly used |
| 4. Dynamic Policy Decision | One or fewer elements used | Two or three elements used | All four elements used |
| 5. Continuous Monitoring and Log Analysis | - | - | - |
| 6. Continuous verification | Temporal information lost | Partial preservation of temporal information | Explicit temporal information retained |
| 7. Full Information-based Security | - | - | - |

**TABLE 5.** Trust quantification model analysis criteria.

| | 0 | 1 | 2 |
|---|---|---|---|
| 1. All Entities as Resources | - | - | - |
| 2. Location-independent Trust Prohibition | Location information used as a label | Location information not used as a label | Location information dependency |
| 3. Least Privilege Principle | Binary classification | Level-based classification | Scoring-based evaluation |
| 4. Dynamic Policy Decision | Static evaluation | Periodic score updates | Environment change detection |
| 5. Continuous Monitoring and Log Analysis | No internal monitoring | Internal monitoring performed | System improvement logic (e.g., model updates) |
| 6. Continuous verification | Single trust computation | Continuous time-series updates | Event-driven re-evaluation |
| 7. Full Information-based Security | - | - | - |

for each individual request or action performed within a session.

#### 4) DYNAMIC POLICY DECISION

Because ZTA requires that trust evaluation consider not only the data associated with the access request itself but also additional behavioral and environmental attributes, the evaluation examines whether the data used in the study include the four key ZTA elements: Entity, User, Environment, and Context. An Entity refers to the physical information of the requester (e.g., PC, server, or device). The user refers to the requester's account information (e.g., ID and password). The Environment represents the environmental conditions at the time of the access request, such as network status and resource information. Context refers to contextual information related to a request, such as the purpose of access or the security state of the requested resource.

#### 5) CONTINUOUS MONITORING AND LOG ANALYSIS

Since ZTA requires trust evaluation to leverage continuously collected data over time, this criterion examines whether the data collection structure supports repeated re-collection of comparable data, rather than relying on a single fixed snapshot. A study is scored according to whether its collection setup is limited to one-time fixed data, permits repeated re-collection (e.g., a re-executable simulation environment), or continuously gathers data as a stream that supports ongoing re-evaluation throughout a session.

#### 6) CONTINUOUS VERIFICATION

Since ZTA requires trust to be continuously evaluated until a session is terminated, this criterion assesses whether the input data include temporal information. Temporal information refers to timestamps or other forms of time-series contextual data that enable trust to be evaluated and updated over time.

#### 7) FULL INFORMATION-BASED SECURITY

In ZTA, trust evaluation should utilize as much relevant information as possible. This implies that data should be collected not only from the access request itself but also from additional monitoring mechanisms. Accordingly, this criterion evaluates whether there exist additional data sources collected beyond the data directly associated with the access request used for the trust evaluation.

### B. DATA PRE-PROCESSING CRITERIA

#### 1) ALL ENTITIES AS RESOURCES

ZTA considers all data sources and computing services as assets that must be protected, and criterion C1 evaluates the diversity of resource types—infrastructure, platform, and service levels—covered by a study. However, this diversity is determined entirely by what is gathered during the Data Collection stage; the set of resource types present in the data is fixed once the collection is complete. The Data Pre-Processing stage transforms and structures the already-collected data—through operations such as normalization, scaling, and feature extraction—but does not add or remove resource types. Consequently, evaluating C1 at the preprocessing stage would simply reproduce the assessment already made in the Data Collection stage and would provide no additional discriminative information. For this reason, this criterion is evaluated only in the Data Collection stage and is not assessed here.

#### 2) LOCATION-INDEPENDENT TRUST PROHIBITION

Because all communications must be protected regardless of the network location, location-related information should be treated as contextual information during the preprocessing stage rather than being used as a direct label for trust evaluation. Accordingly, this criterion evaluates whether trust decisions are made solely based on location-related attributes (e.g., IP addresses or entity location information).

#### 3) LEAST PRIVILEGE PRINCIPLE

Since access should be granted on a per-session basis, this criterion evaluates whether session-related information is preserved in the data after preprocessing. Specifically, the evaluation examined the presence of attributes that enable session identification, such as timestamps or session identifiers, within the processed dataset. The category ''indirectly included in the data'' indicates that session structure information is not used as an explicit feature but that its semantic meaning remains embedded within the preprocessed data.

#### 4) DYNAMIC POLICY DECISION

Because ZTA requires that trust evaluation consider not only the data associated with the access request but also additional behavioral and environmental attributes, this criterion examines whether all four ZTA elements—Entity, User, Environment, and Context—are preserved and utilized after the data preprocessing stage. Accordingly, the evaluation focused on whether these four elements remained represented in the processed data and were incorporated into the subsequent trust evaluation.

#### 5) CONTINUOUS MONITORING AND LOG ANALYSIS

Unlike the Data Collection stage, where the continuity of the collection structure meaningfully distinguishes studies, this criterion is not evaluated in the Data Pre-Processing stage. Preprocessing transformations such as feature extraction and normalization are functional operations that can, by their nature, be reapplied to new inputs in virtually all studies. Scoring this property at the preprocessing stage would therefore provide little discriminative value across studies, and the criterion is accordingly not evaluated at this stage. Continuous monitoring was assessed at the Data Collection and Trust Quantification Model stages.

#### 6) CONTINUOUS VERIFICATION

ZTA requires that trust be continuously evaluated until a session is terminated. In the Data Pre-Processing stage, this criterion evaluates whether the processed data retain temporal information. The category ''partial preservation of temporal information'' indicates that explicit time-series data may not be directly used as input features, but temporal context is indirectly incorporated through techniques such as embedding or similar representation methods.

#### 7) FULL INFORMATION-BASED SECURITY

ZTA requires trust evaluation to utilize as many diverse data sources as possible. In the Data Collection stage, this criterion (C7) is assessed independently, since the existence of additional data sources beyond the access request can be distinguished from the coverage of the four ZTA elements (C4). In the Data Pre-Processing stage, however, the diversity of information can only be judged from what remains in the processed data, which converges with what the Dynamic policy decision criterion (P4) already measures—namely, whether the four ZTA elements are preserved after preprocessing. Evaluating this criterion separately at the preprocessing stage would therefore provide little discriminative value, and it is accordingly not evaluated here.

### C. TRUST QUANTIFICATION MODEL CRITERIA

#### 1) ALL ENTITIES AS RESOURCES

In the Trust Quantification Model stage, the analysis primarily focuses on aspects such as the model outputs and the underlying decision logic. Therefore, the diversity of the resource types considered in the system was not evaluated under this criterion at this stage.

#### 2) LOCATION-INDEPENDENT TRUST PROHIBITION

Consistent with NIST SP 800-207, which prohibits relying on network location as the sole determinant of trust rather than prohibiting its use as a signal altogether, this criterion penalizes only the use of location as a trust label in the Trust Quantification Model stage. A model that uses location-related attributes (e.g., IP addresses or port numbers) as the ground-truth label for trust decisions receives the lowest score, since this makes location the dominant determinant of trust. A model that does not use location information at all was placed at an intermediate level. A model that uses location-related attributes as one feature among multiple signals, rather than as a label, receives the highest score, as this aligns with the dynamic policy decision principle while avoiding location-based trust labeling.

#### 3) LEAST PRIVILEGE PRINCIPLE

Because ZTA requires that access permissions be granted according to the principle of least privilege, this criterion evaluates the type of output produced by the trust model in the Trust Quantification Model stage. Specifically, the evaluation examines how the model expresses trust outcomes, such as through discrete decisions, graded trust scores, or risk-based indicators, and whether these outputs support fine-grained access control consistent with the least privilege principle.

#### 4) DYNAMIC POLICY DECISION

Since ZTA requires that trust models detect environmental changes and continuously update trust evaluations, this criterion assesses the frequency at which the trust model updates trust values. Specifically, the evaluation examined whether the model supports periodic or event-driven trust updates in response to changing contextual conditions.

#### 5) CONTINUOUS MONITORING AND LOG ANALYSIS

ZTA requires the establishment of internal diagnostic mechanisms and system improvement processes. Accordingly, this criterion evaluates whether the trust model includes logic that performs internal assessments for each data input and supports system improvement based on the observed data. For machine learning–based models, a score of 1 point is assigned, considering that such models can be updated through offline retraining.

#### 6) CONTINUOUS VERIFICATION

Since ZTA requires trust to be continuously evaluated until a session is terminated, this criterion assesses whether the trust model includes logic that repeatedly re-evaluates trust after the initial trust assessment. Event-driven re-evaluation refers to cases where trust is recalculated not through simple continuous time-series updates but in response to specific events, such as detected environmental changes or data transmission and reception events.

#### 7) FULL INFORMATION-BASED SECURITY

ZTA requires that trust evaluation utilizes as many diverse data sources as possible. However, in the Trust Quantification Model stage, the analysis primarily focuses on aspects such as the model outputs and decision logic. Therefore, this criterion—emphasizing data diversity—was not evaluated at this stage.

## VI. ANALYSIS AND COMPARISON

The scoring process was carried out as follows. Each of the surveyed studies was evaluated against the stage-specific criteria defined in Section V, using the 0/1/2 rubric in which each score level corresponds to an explicitly defined and operationalized condition. Scoring was based primarily on verifying the presence, count, or type of specific elements described in each study—such as the number of resource types, the inclusion of the four ZTA data elements, or the presence of temporal identifiers—rather than on subjective judgment. The evaluation was conducted by a single reviewer who applied the same rubric uniformly across all studies. Because the 0/1/2 rubric necessarily discretizes continuous phenomena, borderline cases were handled according to a consistent rule. The intermediate level (score 1) of each criterion was defined to absorb partial or implicit satisfaction; for example, in the Least privilege criteria at the Pre-Processing stage, session-aware features that retain session semantics without an explicit session identifier are assigned to the intermediate ''indirectly included'' category rather than the highest level. When a study did not provide explicit evidence for a higher level, the lower score was assigned (a conservative rule), and such cases were resolved by returning to the operational definitions in Section V. A second pass over the complete set was then performed to ensure that this rule was applied uniformly across all studies. The full scoring results are reported in Tables 6–8, and together with the rubric in Section V they allow any reader to independently reproduce and verify the evaluation.

Based on the evaluation criteria defined above, the collected TQ studies in ZTA environments were systematically analyzed and compared. Using the search keywords for ZTA-related TQ studies summarized in Section III-A, a total of 50 studies were identified. Specifically, each study is organized according to the three-stage structure of Data Collection, Data Pre-Processing, and Trust Quantification Model. At the same time, the ZTA tenet-based evaluation criteria are applied to examine how faithfully each study reflects the core principles of Zero Trust.

### A. DATA COLLECTION ANALYSIS & COMPARISON

The Data Collection stage summarizes the datasets or experimental environments used to evaluate the proposed TQ models and evaluates the types and structures of the data employed. The results of the analysis are presented in Table 6.

According to the summarized results, most TQ studies in ZTA environments perform their evaluations using simulation-based environments. Specifically, 68% of the surveyed studies constructed their own simulation environments for training and testing. Various tools were used to build these environments, including CARLA, SUMO, NS-3, and Mininet, which are commonly used research platforms for validating real-world systems in virtual environments. In some cases, simulation environments were directly implemented using tools such as MATLAB or Python to perform analysis and testing.

In addition to simulation environments, several studies conducted evaluations using publicly available security datasets, including UNSW-NB15 [112], CICIDS2017 [113], CICIDS2018 [113], IoTID20 [114], CERT Insider Threat v4.2, Kitsune [115], RT-IoT2022 [116], and CIC IoT 2023 [117]. Fig. 5 illustrates the distribution of the datasets and experimental environments used in the surveyed studies.

Among the studies that used publicly available datasets, those in [64], [73], [78], and [84] conducted evaluations using only the datasets without constructing simulation environments. The total scores assigned to these studies were 3, 6, 5, and 7, respectively. Considering that the average score for the Data Collection stage across all the surveyed studies was 9.34, these scores were relatively low. This result suggests that relying solely on public datasets makes it difficult to fully reflect the ZTA tenets. In particular, to satisfy the Dynamic policy decision criterion, additional data beyond network communication data must be collected.

Conversely, a high Data Collection score does not by itself imply empirical validation. For instance, [101] is a conceptual framework whose data considerations are described analytically rather than verified through a public dataset or a constructed simulation environment; although it considers diverse resource types and ZTA data elements at the conceptual level, its score reflects the breadth of data design that the framework describes rather than empirically collected data. Scores assigned to such conceptual studies should therefore be interpreted with this distinction in mind.

The high proportion of simulation-based studies can largely be attributed to two characteristics of ZTA: Dynamic policy decision and Full information-based security. Traditional perimeter-based security models typically perform anomaly detection or attack classification using only the data associated with the access request itself. In contrast, ZTA requires trust evaluation to incorporate diverse and multi-dimensional data sources, including system-generated data and external contextual information in addition to access request data. Because existing datasets often lack such comprehensive contextual information, they present limitations for evaluating ZTA-based trust models. As a result, many studies have adopted simulation environments to generate richer contextual data and better reflect the operational characteristics of ZTA.

Among the surveyed TQ studies in ZTA environments, the studies that achieved the highest score of 14 in the Data Collection stage (seven criteria $\times$ maximum score of 2 per criterion $=$ 14) are [81], [85], and [96].

Study [81] evaluated trust in an IoT simulation environment and constructed a multi-layered resource structure that included devices, cloud systems, and servers. In addition, the dataset incorporates all four ZTA elements by integrating information such as threat intelligence and vulnerability management data. Study [85] investigated trust evaluation for attacks in vehicular communication environments. It considers communications in an open V2X environment and constructs model inputs by integrating multidimensional trust indicators, including behavior, recommendations, resource information, and link quality. A Study [96] performed a trust evaluation in a realistic open cloud environment implemented using an FPGA-based infrastructure. The input data are organized at the event level, such as authentication events and access requests, and are collected as a continuous identity event stream. Various events, including session transitions and system logs, were also collected to form multidimensional input data. Taken together with the low scores of the studies that rely solely on public datasets ([64], [73], [78], [84]), these results indicate that the assigned scores correspond to the actual degree to which each study reflects ZTA requirements rather than being arbitrary. Studies that construct multi-layered resources and integrate all four ZTA elements receive the highest scores, whereas those with more limited data coverage receive lower scores, suggesting that the criteria discriminate among studies in a meaningful way.

When averaging the scores of all the surveyed studies across the evaluation criteria, the results for C1–C7 were 0.84, 1.10, 1.14, 1.22, 1.68, 1.78, and 1.58. Among these, C1 (All entities as resources), C2 (Location-independent trust prohibition), C3 (Least privilege principle), and C4 (Dynamic policy decision) received relatively lower scores compared to the other criteria. Specifically, C1 evaluates the diversity of resource types, C2 focuses on the diversity of communication scenarios, C3 emphasizes the granularity of data units, and C4 evaluates the diversity of the input data. The relatively low scores in these criteria suggest that current data collection approaches do not fully reflect the characteristics required in ZTA environments. In particular, many studies still rely on traditional datasets or simulation environments that reflect pre-ZTA security assumptions, and there remain practical limitations in collecting real communication data from operational ZTA environments.

Overall, while many studies have constructed simulation environments that incorporate certain ZTA characteristics during the Data Collection stage, further improvements are required. These include increasing resource diversity (infrastructure, platform, and service levels), expanding data collection environments to boundaryless contexts, refining data collection granularity toward request-level observations rather than user- or session-level aggregation, and incorporating more diverse ZTA four-element data sources.

In addition, the Full Information-based Security tenet, which underlies criterion C7, suggests that a tension with data privacy may also warrant consideration. Since this tenet encourages collecting and integrating as much relevant information as possible, pursuing it to its extreme could conflict with the data minimization requirements of privacy

**TABLE 6. Analysis results of trust quantification studies in the data collection.**

| No | Year | Dataset/Environment | Setup Tool | C1 | C2 | C3 | C4 | C5 | C6 | C7 |
|---|---|---|---|---|---|---|---|---|---|---|
| [62] | 2020 | Simulation Environment | Not specified | 0 | 0 | 1 | 1 | 2 | 2 | 2 |
| [63] | 2021 | Simulation Environment | Java | 0 | 2 | 2 | 1 | 2 | 2 | 2 |
| [64] | 2022 | Advogato, Pretty Good Privacy | - | 0 | 2 | 0 | 1 | 0 | 0 | 0 |
| [65] | 2023 | Real Environment | Online Boutique | 0 | 1 | 2 | 1 | 2 | 2 | 2 |
| [66] | 2023 | Simulation Environment | MATLAB | 1 | 0 | 2 | 1 | 2 | 2 | 1 |
| [67] | 2024 | Simulation Environment | MATLAB | 0 | 0 | 0 | 1 | 1 | 0 | 2 |
| [68] | 2024 | Simulation Environment | MATLAB | 1 | 0 | 2 | 1 | 2 | 2 | 0 |
| [69] | 2025 | [113], [114], Simulation Environment | - | 1 | 2 | 1 | 2 | 2 | 2 | 2 |
| [70] | 2025 | Simulation Environment | Not specified | 2 | 1 | 2 | 2 | 2 | 2 | 2 |
| [71] | 2025 | [114], CITv4.2, Simulation Environment | OpenStack | 2 | 1 | 2 | 2 | 2 | 2 | 2 |
| [72] | 2025 | Simulation Environment | Not specified | 0 | 0 | 2 | 2 | 2 | 2 | 2 |
| [73] | 2025 | GPNSACS | - | 0 | 0 | 2 | 1 | 0 | 1 | 2 |
| [74] | 2025 | CITv4.2, Simulation Environment | Not specified | 0 | 1 | 0 | 2 | 2 | 2 | 2 |
| [75] | 2025 | Real Environment | - | 0 | 1 | 1 | 2 | 2 | 2 | 2 |
| [76] | 2025 | Simulation Environment | Not specified | 0 | 0 | 0 | 0 | 2 | 2 | 0 |
| [77] | 2025 | [114], [115], Simulation Environment | Python | 2 | 1 | 2 | 1 | 2 | 2 | 2 |
| [78] | 2025 | MNIST, FMNIST, SVHN, CIFAR10 | - | 1 | 2 | 0 | 0 | 0 | 2 | 0 |
| [79] | 2025 | Simulation Environment | Hyperledger Fabric | 0 | 2 | 0 | 1 | 2 | 2 | 2 |
| [80] | 2025 | CITv4.2, Simulation Environment | Python | 2 | 1 | 1 | 2 | 2 | 2 | 2 |
| [81] | 2025 | Simulation Environment | Not specified | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| [82] | 2025 | Simulation Environment | Not specified | 0 | 0 | 2 | 1 | 2 | 2 | 2 |
| [83] | 2025 | Simulation Environment | MATLAB | 0 | 2 | 2 | 1 | 2 | 2 | 2 |
| [84] | 2025 | Kitsune Network Attack | - | 0 | 2 | 2 | 1 | 0 | 2 | 0 |
| [85] | 2025 | NGSIM I-80, Simulation Environment | CARLA | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| [86] | 2025 | Simulation Environment | Vmware, Java8 | 2 | 1 | 2 | 2 | 2 | 2 | 0 |
| [87] | 2025 | Simulation Environment | MATLAB | 1 | 2 | 0 | 1 | 2 | 2 | 2 |
| [88] | 2025 | Real Environment | Python | 0 | 1 | 1 | 1 | 2 | 2 | 2 |
| [89] | 2025 | Simulation Environment | MATLAB | 2 | 1 | 1 | 1 | 2 | 2 | 2 |
| [90] | 2025 | Real Environment | Remote Desktop | 2 | 0 | 1 | 1 | 2 | 2 | 2 |
| [91] | 2025 | Simulation Environment | Not specified | 1 | 2 | 0 | 1 | 2 | 2 | 0 |
| [92] | 2025 | Illustrative Evaluation | - | 1 | 2 | 0 | 0 | 0 | 0 | 2 |
| [93] | 2025 | Simulation Environment | FuzzyC | 2 | 0 | 0 | 1 | 2 | 0 | 2 |
| [94] | 2025 | Simulation Environment | OPAL-RT | 1 | 0 | 0 | 0 | 2 | 2 | 0 |
| [95] | 2025 | Simulation Environment | CARLA | 1 | 2 | 1 | 2 | 2 | 2 | 2 |
| [96] | 2025 | Real Environment | FPGA | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| [97] | 2025 | Simulation Environment | NS-3 | 0 | 2 | 1 | 1 | 2 | 2 | 2 |
| [98] | 2025 | Simulation Environment | iFogSim2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 |
| [99] | 2025 | Simulation Environment | Python | 0 | 2 | 0 | 1 | 2 | 2 | 2 |
| [100] | 2025 | Simulation Environment | Python, OpenSSL | 1 | 1 | 2 | 1 | 1 | 0 | 2 |
| [101] | 2025 | - | - | 2 | 2 | 2 | 2 | 0 | 2 | 2 |
| [102] | 2025 | Simulation Environment | Nessus, Rapid7, OpenVAS | 0 | 0 | 1 | 1 | 2 | 2 | 2 |
| [103] | 2025 | Simulation Environment | Mininet | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| [104] | 2025 | Simulation Environment | Not specified | 0 | 0 | 0 | 1 | 2 | 2 | 0 |
| [105] | 2025 | [118], Simulation Environment | Not specified | 0 | 0 | 0 | 1 | 2 | 2 | 2 |
| [106] | 2025 | [119], Simulation Environment | Not specified | 1 | 2 | 2 | 1 | 2 | 2 | 2 |
| [107] | 2025 | Not Specified | - | 2 | 2 | 0 | 2 | 0 | 2 | 2 |
| [108] | 2025 | CITv4.2, CMU Behavioral Logs Repository, Simulation Environment | Python | 1 | 0 | 2 | 2 | 2 | 2 | 2 |
| [109] | 2026 | Real Environment | BeautifulSoup | 1 | 1 | 2 | 2 | 2 | 2 | 2 |
| [110] | 2026 | Simulation Environment | SUMO, MATLAB | 1 | 1 | 1 | 1 | 2 | 2 | 0 |
| [111] | 2026 | Simulation Environment | Python | 0 | 2 | 2 | 1 | 2 | 2 | 2 |

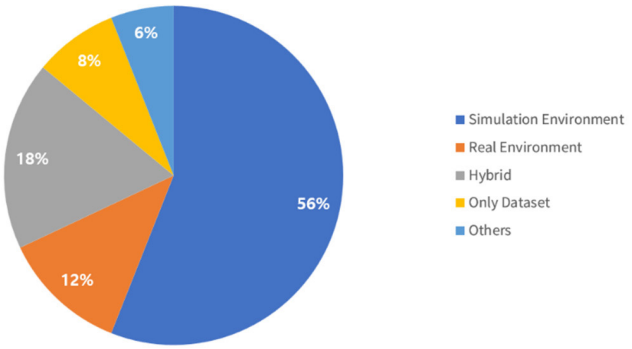


**FIGURE 5.** Distribution of datasets and experimental environments.

regulations such as the GDPR and the CCPA, which require that only data necessary for a specified purpose be collected and processed. In this sense, collecting more diverse data for trust evaluation may also raise privacy and compliance concerns. While such considerations fall outside the scope of the present evaluation, future work on ZTA-based TQ may need to consider how comprehensive information collection can be balanced against data minimization and regulation-compliant data practices, for example through privacy-enhancing techniques or purpose-bound data scoping.

### B. DATA PRE-PROCESSING ANALYSIS & COMPARISON

In the Data Pre-Processing stage, the methodologies used to process the collected data are summarized and analyzed, with particular attention to whether the preprocessing methods reflect the characteristics of ZTA. The evaluation results are presented in Table 7.

In this analysis, the preprocessing methods are classified into four categories according to how the collected data are transformed into model inputs: Mathematical Feature Extraction, which derives statistical or mathematical features from the raw data; ML/Graph Feature Engineering, which constructs features through learning-based or graph-based representations; Fuzzy/Probabilistic Transformation, which converts data into fuzzy or probabilistic forms; and State Space Extraction, which represents data as state-space structures. According to this classification, Mathematical Feature Extraction was the most common approach (58%), followed by ML/Graph Feature Engineering (24%), Fuzzy/Probabilistic Transformation (16%), and State Space Extraction (2%).

Among the surveyed TQ studies in ZTA environments, the studies that achieved the highest score of 8 in the Data Pre-Processing stage (four criteria $\times$ maximum score of 2 per criterion $= 8$) were [71], [72], [81], [86], [101], and [108].

Study [71] processed input data such as user IDs, IP reputation scores, and access times by converting them into numerical values normalized within the range $[1, 0]$. Study [72] normalized input data using mathematical functions while preserving statistical properties such as mean, variance, minimum, and maximum values. Study [81] applied a field-level structuring approach, extracting fields from traffic packets and organizing their attributes into structured representations. These structured attributes were then used for policy matching and provided as input to the detection module.

A study [86] maintained temporal information using a sliding window technique and structured the input data into key features such as privilege escalation attempts and login failures for model input. Study [101] generated feature vectors and structured them into four categories: Membership, Behavior, Transactional, and Environment feature vectors.

Across all the studies, when the scores for each evaluation criterion were averaged, the results for P2, P3, P4, and P6 were 1.6, 0.9, 1.2, and 1.6, respectively. Among these, P3 (Least privilege principle) and P4 (Dynamic policy decision) received relatively lower scores—0.9 and 1.2, respectively—compared to the other criteria. Criterion P3 focuses on whether the data structure is preserved, while P4 evaluates whether the four ZTA elements are retained in the processed data. These results indicate that many TQ studies in ZTA environments rely on transformation-based preprocessing methods—such as mathematical feature extraction and learning-based feature engineering—which convert the input data into derived feature representations and consequently lead to the loss of the original data structure and the partial loss of the four ZTA elements. The relatively low score for P4 is consistent with the observations made in the Data Collection stage, where the datasets themselves often lack sufficient representation of the four ZTA elements. However, the low score for P3 highlights a different issue: such transformation-based methods frequently eliminate structural information, including session-related information, from the data. While the resulting features can provide useful indicators for identifying attacks or suspicious behavior, they may be insufficient for detecting long-term attacks, such as Advanced Persistent Threats (APTs) or long-term account compromise. Because such attacks unfold over extended periods, the loss of session and temporal structure during preprocessing may prevent these threats from being properly identified.

Consequently, current TQ research in ZTA environments still predominantly relies on feature-based representations derived from processed input data, which inherently introduces information loss. Although feature-based representations can provide valuable clues for detecting attacks or estimating attack likelihood, additional strategies should be considered to preserve the temporal and structural information. Preprocessing approaches that leverage time-series information and structured data representations should be further explored to better capture the contextual and sequential characteristics of security events.

### C. TRUST QUANTIFICATION MODEL ANALYSIS & COMPARISON

In the Trust Quantification Model stage, the analysis focuses on the trust evaluation logic of the models. Specifically, the models were examined to determine whether the ZTA characteristics were properly considered during the trust quantification process. The evaluation results are presented in Table 8.

**TABLE 7.** Analysis results of trust quantification studies in the data pre-processing.

| No | year | Pre-Processing Method | P2 | P3 | P4 | P6 |
|---|---|---|---|---|---|---|
| [62] | 2020 | Fuzzy/Probabilistic Transformation | 1 | 1 | 1 | 1 |
| [63] | 2021 | Mathematical Feature Extraction | 1 | 1 | 1 | 2 |
| [64] | 2022 | ML/Graph Feature Engineering | 1 | 0 | 0 | 0 |
| [65] | 2023 | Mathematical Feature Extraction | 2 | 1 | 1 | 2 |
| [66] | 2023 | Mathematical Feature Extraction | 1 | 2 | 1 | 2 |
| [67] | 2024 | Fuzzy/Probabilistic Transformation | 1 | 0 | 1 | 0 |
| [68] | 2024 | Mathematical Feature Extraction | 2 | 1 | 1 | 2 |
| [69] | 2025 | Mathematical Feature Extraction | 2 | 0 | 2 | 1 |
| [70] | 2025 | Mathematical Feature Extraction | 2 | 1 | 2 | 2 |
| [71] | 2025 | Mathematical Feature Extraction | 2 | 2 | 2 | 2 |
| [72] | 2025 | Mathematical Feature Extraction | 2 | 2 | 2 | 2 |
| [73] | 2025 | ML/Graph Feature Engineering | 2 | 0 | 1 | 2 |
| [74] | 2025 | Mathematical Feature Extraction | 2 | 0 | 2 | 1 |
| [75] | 2025 | Mathematical Feature Extraction | 1 | 1 | 1 | 2 |
| [76] | 2025 | ML/Graph Feature Engineering | 1 | 0 | 0 | 1 |
| [77] | 2025 | ML/Graph Feature Engineering | 2 | 0 | 1 | 1 |
| [78] | 2025 | Mathematical Feature Extraction | 1 | 0 | 0 | 1 |
| [79] | 2025 | Mathematical Feature Extraction | 1 | 0 | 1 | 1 |
| [80] | 2025 | ML/Graph Feature Engineering | 2 | 0 | 2 | 1 |
| [81] | 2025 | Mathematical Feature Extraction | 2 | 2 | 2 | 2 |
| [82] | 2025 | Fuzzy/Probabilistic Transformation | 1 | 2 | 1 | 2 |
| [83] | 2025 | Mathematical Feature Extraction | 1 | 2 | 1 | 2 |
| [84] | 2025 | ML/Graph Feature Engineering | 2 | 0 | 1 | 2 |
| [85] | 2025 | Mathematical Feature Extraction | 2 | 1 | 2 | 2 |
| [86] | 2025 | Mathematical Feature Extraction | 2 | 2 | 2 | 2 |
| [87] | 2025 | Mathematical Feature Extraction | 2 | 0 | 1 | 2 |
| [88] | 2025 | Fuzzy/Probabilistic Transformation | 2 | 1 | 1 | 2 |
| [89] | 2025 | Mathematical Feature Extraction | 1 | 1 | 1 | 2 |
| [90] | 2025 | ML/Graph Feature Engineering | 2 | 2 | 1 | 2 |
| [91] | 2025 | Mathematical Feature Extraction | 2 | 1 | 1 | 2 |
| [92] | 2025 | Mathematical Feature Extraction | 1 | 0 | 0 | 0 |
| [93] | 2025 | Fuzzy/Probabilistic Transformation | 1 | 0 | 1 | 0 |
| [94] | 2025 | Mathematical Feature Extraction | 1 | 0 | 0 | 2 |
| [95] | 2025 | ML/Graph Feature Engineering | 2 | 1 | 2 | 2 |
| [96] | 2025 | ML/Graph Feature Engineering | 1 | 2 | 2 | 2 |
| [97] | 2025 | Mathematical Feature Extraction | 2 | 1 | 1 | 2 |
| [98] | 2025 | Fuzzy/Probabilistic Transformation | 1 | 1 | 1 | 2 |
| [99] | 2025 | Mathematical Feature Extraction | 1 | 0 | 1 | 1 |
| [100] | 2025 | Mathematical Feature Extraction | 1 | 1 | 1 | 0 |
| [101] | 2025 | ML/Graph Feature Engineering | 2 | 2 | 2 | 2 |
| [102] | 2025 | Mathematical Feature Extraction | 1 | 0 | 0 | 2 |
| [103] | 2025 | State Space Extraction | 2 | 0 | 0 | 2 |
| [104] | 2025 | Fuzzy/Probabilistic Transformation | 2 | 1 | 1 | 2 |
| [105] | 2025 | Mathematical Feature Extraction | 1 | 0 | 1 | 2 |
| [106] | 2025 | ML/Graph Feature Engineering | 2 | 1 | 1 | 2 |
| [107] | 2025 | Mathematical Feature Extraction | 2 | 0 | 2 | 2 |
| [108] | 2025 | Fuzzy/Probabilistic Transformation | 2 | 2 | 2 | 2 |
| [109] | 2026 | Mathematical Feature Extraction | 2 | 1 | 2 | 2 |
| [110] | 2026 | Mathematical Feature Extraction | 2 | 2 | 1 | 2 |
| [111] | 2026 | ML/Graph Feature Engineering | 1 | 2 | 1 | 2 |

**TABLE 8.** Analysis results of trust quantification studies in the trust quantification model.

| No | year | Model | T2 | T3 | T4 | T5 | T6 |
|---|---|---|---|---|---|---|---|
| [62] | 2020 | Fuzzy Logic | 1 | 2 | 1 | 0 | 1 |
| [63] | 2021 | Weighted Sum Model | 1 | 2 | 1 | 0 | 1 |
| [64] | 2022 | GNN | 2 | 1 | 0 | 1 | 0 |
| [65] | 2023 | Weighted Sum Model | 1 | 2 | 2 | 0 | 2 |
| [66] | 2023 | Weighted Sum Model | 1 | 2 | 1 | 0 | 1 |
| [67] | 2024 | Fuzzy Logic | 2 | 2 | 0 | 0 | 0 |
| [68] | 2024 | Weighted Sum Model | 1 | 2 | 1 | 2 | 1 |
| [69] | 2025 | Weighted Sum Model | 2 | 2 | 1 | 0 | 1 |
| [70] | 2025 | Probabilistic Model | 2 | 2 | 2 | 0 | 1 |
| [71] | 2025 | Weighted Sum Model | 2 | 2 | 2 | 0 | 1 |
| [72] | 2025 | Weighted Sum Model | 1 | 2 | 2 | 0 | 2 |
| [73] | 2025 | Hybrid(Weighted Sum + FastKAN) | 2 | 2 | 0 | 1 | 2 |
| [74] | 2025 | Weighted Sum Model | 1 | 2 | 1 | 0 | 1 |
| [75] | 2025 | Weighted Sum Model | 1 | 2 | 2 | 0 | 1 |
| [76] | 2025 | Probabilistic Model | 2 | 2 | 1 | 0 | 1 |
| [77] | 2025 | Weighted Sum Model | 1 | 2 | 2 | 1 | 2 |
| [78] | 2025 | Hybrid(CNN + Gaussian Process Regression) | 2 | 2 | 2 | 2 | 1 |
| [79] | 2025 | Hybrid(Clustering + RNN) | 2 | 2 | 1 | 1 | 1 |
| [80] | 2025 | Hybrid(Random Forest + BP Neural Network) | 2 | 2 | 2 | 1 | 2 |
| [81] | 2025 | Hybrid(CNN + LSTM, Rule-based) | 2 | 2 | 2 | 2 | 2 |
| [82] | 2025 | Bayesian Model | 2 | 2 | 2 | 1 | 2 |
| [83] | 2025 | Weighted Sum Model | 1 | 2 | 2 | 0 | 1 |
| [84] | 2025 | Autoencoder | 2 | 2 | 2 | 2 | 1 |
| [85] | 2025 | Weighted Sum Model | 1 | 2 | 2 | 0 | 2 |
| [86] | 2025 | Fuzzy Logic | 2 | 2 | 1 | 0 | 1 |
| [87] | 2025 | Hybrid(Bayesian + Weighted Sum Model) | 2 | 2 | 2 | 2 | 1 |
| [88] | 2025 | Fuzzy Logic | 1 | 2 | 2 | 0 | 1 |
| [89] | 2025 | Weighted Sum Model | 1 | 2 | 1 | 0 | 1 |
| [90] | 2025 | HGNN | 2 | 1 | 1 | 1 | 1 |
| [91] | 2025 | Weighted Sum Model | 1 | 2 | 2 | 0 | 1 |
| [92] | 2025 | Weighted Sum Model | 1 | 2 | 0 | 0 | 0 |
| [93] | 2025 | Fuzzy Logic | 1 | 2 | 0 | 0 | 0 |
| [94] | 2025 | Weighted Sum Model | 1 | 2 | 0 | 0 | 1 |
| [95] | 2025 | LSTM | 2 | 2 | 1 | 1 | 1 |
| [96] | 2025 | Weighted Sum Model | 1 | 1 | 2 | 0 | 2 |
| [97] | 2025 | Weighted Sum Model | 1 | 2 | 1 | 0 | 1 |
| [98] | 2025 | Bayesian Model | 1 | 2 | 2 | 2 | 1 |
| [99] | 2025 | Weighted Sum Model | 1 | 2 | 1 | 2 | 1 |
| [100] | 2025 | Weighted Sum Model | 1 | 2 | 2 | 0 | 2 |
| [101] | 2025 | XGBoost | 2 | 2 | 2 | 1 | 2 |
| [102] | 2025 | Hybrid(Game Theory + Bayesian) | 1 | 2 | 2 | 1 | 1 |
| [103] | 2025 | Hybrid(Weighted Sum + DRL) | 2 | 2 | 2 | 2 | 1 |
| [104] | 2025 | Neutrosophic Logic | 2 | 2 | 1 | 1 | 1 |
| [105] | 2025 | Random Forest | 1 | 2 | 1 | 1 | 0 |
| [106] | 2025 | Hybrid(Random Forest + XGBoost) | 2 | 2 | 2 | 1 | 1 |
| [107] | 2025 | Supervised ML | 2 | 2 | 1 | 1 | 1 |
| [108] | 2025 | Bayesian Model | 2 | 2 | 2 | 1 | 1 |
| [109] | 2026 | Weighted Sum Model | 1 | 2 | 1 | 0 | 1 |
| [110] | 2026 | Weighted Sum Model | 1 | 2 | 1 | 0 | 1 |
| [111] | 2026 | Hybrid(Bayesian + Weighted Sum Model) | 1 | 2 | 2 | 1 | 1 |

According to the summarized results, a large proportion of studies employed the Weighted Sum model. Specifically, 50% of the surveyed studies adopted the Weighted Sum approach, while the remaining studies utilized various models, including Fuzzy Logic, Bayesian models, and machine learning–based methods. This indicates that approaches that assign weights to multiple attributes—such as behavior, context, and feedback—and combine them through linear aggregation are widely adopted in practice.

The Weighted Sum model is relatively simple to implement, offers high interpretability, and is suitable for real-time evaluations. For these reasons, it can be considered a preferred structure from the perspective of practical deployment in ZTA environments. Fig. 6 illustrates the distribution of the models used in the surveyed TQ studies for ZTA.

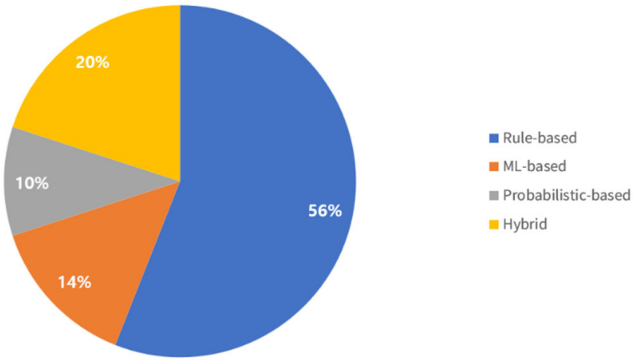


**FIGURE 6.** Distribution of trust quantification model.

From 2020 to 2024, Fuzzy Logic and Weighted Sum models appeared relatively frequently in TQ studies. This trend indicates that many studies have focused on handling uncertainty through fuzzy inference and rule-based reasoning defined by domain experts. However, since 2025, additional models such as Bayesian approaches and machine learning (ML) models—including XGBoost, LSTM, and Transformer-based architectures—have been proposed. Although the Weighted Sum model remains widely used, the increasing introduction of ML-based models indicates a growing interest in learnable trust models, suggesting that trust evaluation is gradually evolving toward a dynamic trust prediction problem. While this trend may partly result from the minimum citation threshold applied in the search strategy, it nevertheless demonstrates that ML-based approaches are becoming increasingly prominent. In addition, various hybrid models have been proposed, combining rule-based models with ML-based models or integrating multiple ML-based approaches.

Among the surveyed studies, study [81] achieved a maximum score of 10 in the Trust Quantification Model stage (five criteria $\times$ maximum score of 2 per criterion $=$ 10). A study [81] presented a hybrid framework integrating CNN, LSTM, and rule-based models, where trust computation is structured into four components: behavior-based trust assessment, federated learning–based anomaly detection, challenge–response trust evaluation, and direct and indirect trust calculation. This design enables the model to use location-related attributes as one of multiple signals rather than as a trust label, to express trust through graded scores, and to update trust values in response to environmental changes, thereby satisfying the criteria at the highest level.

Across all studies, when the scores for each evaluation criterion were averaged, the results for T2–T6 were 1.5, 1.9, 1.4, 0.6, and 1.1, respectively. Among these, T5 (Continuous Monitoring and Log Analysis) and T6 (Continuous Verification) received relatively lower scores—0.6 and 1.1, respectively—compared to the other criteria. Criterion T5 focuses on whether the TQ model includes mechanisms that allow the system to continuously improve as more data are received, while T6 evaluates whether the model supports repeated trust re-evaluation during operation. The relatively high scores for T2, T3, and T4 indicate that most studies do not use location information as a trust label, represent trust as quantified levels or scores, and allow trust models to update trust values when environmental changes are detected. However, the results suggest that the ZTA principles of continuous monitoring and log analysis for system improvement and continuous verification of trust have not been sufficiently considered in many studies. This observation implies that most existing works primarily focus on the computation of trust values rather than the long-term operational improvement of trust models.

Overall, the results indicate a growing trend toward machine learning–based approaches, and many studies have proposed hybrid models that combine multiple techniques to perform more systematic trust quantification. Nevertheless, current research largely concentrates on the trust quantification process itself, while mechanisms for continuous model improvement remain underexplored. In addition, most TQ models perform continuous time-series updates, indicating that trust evaluation is commonly implemented as sequential recalculation rather than as adaptive system-level improvement.

Beyond these observations, the analysis reveals a trade-off between ZTA tenet fidelity and computational performance that the proposed framework does not explicitly capture. In ZTA, trust must be computed in real time to support per-request access decisions, yet several of the mechanisms associated with high tenet fidelity—such as the event-driven re-evaluation and continuous model improvement assessed under T5 and T6—inherently entail repeated and costly computation. Consequently, a study that scores highly on criteria such as continuous verification may still be unsuitable for practical deployment if it incurs substantial computation or latency per request. As noted earlier, the predominance of the Weighted Sum model—computationally light and well suited to real-time evaluation—can be interpreted as a practical choice reflecting real deployment conditions, whereas ML- and hybrid-based models offer richer trust representations at greater computational cost. Because the proposed framework evaluates how faithfully each study reflects the ZTA tenets rather than its computational efficiency, a high score should be understood as indicating alignment with ZTA principles rather than deployability in itself. Accounting for computational cost and latency therefore constitutes an important

complementary dimension for assessing the practical applicability of ZTA-based TQ models.

## VII. CONCLUSION

This paper presents a survey study that systematically analyzes and compares TQ research within ZTA environments. Although the two research areas have progressed with little cross-referencing, no integrated framework that integrates TQ studies while reflecting the structural principles and operational requirements of ZTA has not been sufficiently established. To address this gap, this study reviews the existing ZTA and TQ survey literature to identify research gaps and proposes a taxonomy that analyzes ZTA-based TQ research by dividing the TQ process into three stages.

The main contribution of this study is the development of a taxonomy that structures ZTA-based TQ research into three stages: Data Collection, Data Pre-Processing, and Trust Quantification Model, and the design of ZTA tenet–based evaluation criteria for each stage. The proposed taxonomy interprets trust quantification not merely as the computation of a final trust score but as a structured process consisting of interrelated stages, including the collection of data that form the basis of trust evaluation, preprocessing to transform these data into computable representations, and the design of models that generate the final trust values. Furthermore, the evaluation criteria incorporate the core ZTA tenets—all entities as resources, location-independent trust prohibition, least privilege principle, dynamic policy decision, continuous monitoring and log analysis, continuous verification, and full information-based security. By reflecting these principles, the proposed framework enables the reinterpretation of existing studies not only from a performance comparison perspective but also from the standpoint of ZTA compliance and architectural suitability.

Based on the proposed analytical framework, 50 ZTA-based TQ studies were systematically compared and analyzed, revealing several important trends and limitations.

First, in the Data Collection stage, many studies have conducted evaluations using simulation environments rather than public datasets. This tendency can be interpreted as a result of the difficulty of adequately representing the multidimensional and dynamic data structures required by ZTA using existing public datasets alone. Nevertheless, limitations still remain in terms of resource diversity, boundaryless environment configuration, request-level data collection, and the comprehensiveness of the four ZTA data elements.

Second, in the Data Pre-Processing stage, most studies adopted transformation-based preprocessing methods—predominantly mathematical feature extraction and learning-based feature engineering—which often resulted in the loss of session structure and temporal context. While such approaches may be effective for short-term anomaly detection, they may present structural limitations in detecting persistent attacks, such as long-term account compromise or Advanced Persistent Threats (APTs).

Third, in the Trust Quantification Model stage, the Weighted Sum model is the most widely used approach. Recently, however, an increasing number of studies have expanded toward Bayesian, machine learning (ML), and hybrid models. Despite this trend, many studies have primarily focused on calculating trust scores, while the continuous improvement of models and event-driven trust re-evaluation mechanisms, which are essential requirements of ZTA's continuous verification principle, have not been sufficiently considered.

These findings suggest that although ZTA-based TQ research is gradually becoming more sophisticated, it has not yet reached a stage where it fully satisfies the structural requirements of ZTA. Building on the gaps identified at each stage, several concrete research directions can be outlined. In the Data Collection stage, where existing datasets inadequately represent ZTA contexts, future work should address how to construct benchmark datasets that capture diverse resource types (infrastructure, platform, and service), both internal and external communications, and request-level activity together with the four ZTA data elements—and how such datasets can complement or replace the simulation environments that current studies predominantly rely on. In the Data Pre-Processing stage, where transformation-based methods lead to the loss of session and temporal structure, a key question is how to design preprocessing techniques that preserve session identity and temporal ordering while retaining the statistical expressiveness needed for trust computation, and whether such structure-preserving representations measurably improve the detection of long-term threats such as APTs. In the Trust Quantification Model stage, where continuous improvement and event-driven re-evaluation remain underexplored, future research should investigate how to realize online or event-driven trust re-evaluation that satisfies the continuous verification principle, and how to balance ZTA tenet fidelity against the computational cost and latency constraints of real-time access decisions. Addressing these questions would move ZTA-based TQ research beyond performance-oriented model refinement toward trust quantification that structurally embodies the principles of Zero Trust.

Beyond the limitations of the surveyed studies, this work itself is subject to a methodological limitations concerning the use of Google Scholar as a single search source. Although its broad indexing coverage and support for title-based search enabled comprehensive retrieval, two threats to validity remain. First, Google Scholar does not guarantee full reproducibility, as its indexing and ranking results may vary over time and across query conditions. Second, the absence of cross-database verification means that some relevant studies indexed exclusively in other platforms may not have been captured. To mitigate these threats, title-based keyword searching was applied to ensure topical relevance, and year-specific citation thresholds were used to prioritize substantively referenced works. Future studies may further strengthen retrieval completeness by complementing Google Scholar with searches across IEEE Xplore, ACM Digital Library, and Scopus.

Another limitation concerns the scoring procedure. Because the evaluation was performed by a single reviewer, inter-rater reliability metrics such as Cohen's kappa could

not be computed. To mitigate the resulting subjectivity, the evaluation relied on an explicitly operationalized rubric in which each criterion and score level is defined by verifiable conditions (Section V), and the complete set of scores is made available (Tables 6–8) so that the evaluation can be independently reproduced and audited.

In addition, the title-only search strategy, while chosen to maximize topical precision, may have excluded studies that address trust quantification substantively in the body text but not in the title. A broad set of synonymous title terms was used to mitigate this effect.

In summary, this study contributes by proposing a systematic analytical framework for TQ research in ZTA environments and by organizing the trends and limitations of existing studies from the perspective of ZTA tenets. The taxonomy and evaluation criteria presented in this work can serve as a common references for designing, comparing, and evaluating future ZTA-based TQ studies, and they are expected to facilitate the advancement of trust quantification research that reflects the fundamental principles of Zero Trust, rather than focusing solely on performance-oriented approaches.

## REFERENCES

[1] S. Rose, "Zero trust architecture," NIST Special Publication, Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-207, 2020, pp. 207–800, doi: 10.6028/NIST.SP.800-207.

[2] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," *Comput. Secur.*, vol. 110, Nov. 2021, Art. no. 102436.

[3] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.

[4] L. Alevizos, V. T. Ta, and M. Hashem Eiza, "Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review," *Secur. Privacy*, vol. 5, no. 1, p. e191, Jan. 2022.

[5] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wireless Commun. Mobile Comput.*, vol. 2022, no. 1, Jan. 2022, Art. no. 6476274.

[6] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of zero trust networks in cloud computing: A comparative review," *Sustainability*, vol. 14, no. 18, p. 11213, Sep. 2022.

[7] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and application of zero trust security: A brief survey," *Entropy*, vol. 25, no. 12, p. 1595, Nov. 2023.

[8] E. A. Shaikh Ashfaq, "Zero trust security paradigm: A comprehensive survey and research analysis," *J. Electr. Syst.*, vol. 19, no. 2, pp. 28–37, Jan. 2024.

[9] P. P. Ray, "web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 213–248, 2023.

[10] N. Nahar, K. Andersson, O. Schelén, and S. Saguna, "A survey on zero trust architecture: Applications and challenges of 6G networks," *IEEE Access*, vol. 12, pp. 94753–94764, 2024.

[11] P. Dhiman, N. Saini, Y. Gulzar, S. Turaev, A. Kaur, K. U. Nisa, and Y. Hamid, "A review and comparative analysis of relevant approaches of zero trust network model," *Sensors*, vol. 24, no. 4, p. 1328, Feb. 2024.

[12] A. Gupta, P. Gupta, U. P. Pandey, P. Kushwaha, B. P. Lohani, and K. Bhati, "ZTSA: Zero trust security architecture a comprehensive survey," in *Proc. Int. Conf. Commun., Comput. Sci. Eng. (IC3SE)*, May 2024, pp. 378–383.

[13] S. Al-Tamimi, Q. A. Al-Haija, and K. Alrawashdeh, "Zero-trust architecture for securing Internet of Things (IoT) networks: A review," in *Proc. 5th Int. Conf. Commun., Inf., Electron. Energy Syst. (CIEES)*, Nov. 2024, pp. 1–6.

[14] A. Itzhak Weinberg and K. Cohen, "Zero trust implementation in the emerging technologies era: Survey," 2024, *arXiv:2401.09575*.

[15] A. A. Alquwayzani and A. A. Albuali, "A systematic literature review of zero trust architecture for military UAV security systems," *IEEE Access*, vol. 12, pp. 176033–176056, 2024.

[16] C. Itodo and M. Ozer, "Multivocal literature review on zero-trust security implementation," *Comput. Secur.*, vol. 141, Jun. 2024, Art. no. 103827.

[17] M. James, T. Newe, D. O'Shea, and G. D. O'Mahony, "Authentication and authorization in zero trust IoT: A survey," in *Proc. 35th Irish Signals Syst. Conf. (ISSC)*, Jun. 2024, pp. 1–7.

[18] F. Mensah, "Zero trust architecture: A comprehensive review of principles, implementation strategies, and future directions in enterprise cybersecurity," *Int. J. Academic Ind. Res. Innov.*, vol. 10, pp. 339–346, Jun. 2024.

[19] D. Ajish, "The significance of artificial intelligence in zero trust technologies: A comprehensive review," *J. Electr. Syst. Inf. Technol.*, vol. 11, no. 1, p. 30, Aug. 2024.

[20] S. M. Zohaib, S. M. Sajjad, Z. Iqbal, M. Yousaf, M. Haseeb, and Z. Muhammad, "Zero trust VPN (ZT-VPN): A systematic literature review and cybersecurity framework for hybrid and remote work," *Information*, vol. 15, no. 11, p. 734, 2024.

[21] M. A. Azad, S. Abdullah, J. Arshad, H. Lallie, and Y. H. Ahmed, "Verify and trust: A multidimensional survey of zero-trust security in the age of IoT," *Internet Things*, vol. 27, Oct. 2024, Art. no. 101227.

[22] M. Annabi, A. Zeroual, and N. Messai, "Towards zero trust security in connected vehicles: A comprehensive survey," *Comput. Secur.*, vol. 145, Oct. 2024, Art. no. 104018.

[23] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, "A systematic literature review on the implementation and challenges of zero trust architecture across domains," *Sensors*, vol. 25, no. 19, p. 6118, Oct. 2025.

[24] S. Rahman and N. Perumath, "Implementing zero trust management in IoT environment-challenges and solutions: Scoping review," Dept. Comput. Syst. Sci., Stockholm Univ., Stockholm, Sweden, Tech. Rep., 2025.

[25] A. Soni, S. Kumar Nanda, R. Priyadarshini, and G. Panda, "A comprehensive review and comparative analysis of zero trust architecture: Evolution, implementation strategies, and key challenges," *J. Comput. Secur.*, vol. 34, no. 2, pp. 85–110, Mar. 2026.

[26] I. U. Onwuegbuzie and O. A. Alabi, "A review of authentication and authorization mechanisms in zero trust architecture: Evolution and efficiency," *Tech-Sphere J. Pure Appl. Sci.*, vol. 2, no. 1, pp. 1–34, 2025.

[27] K. Zakhmi, A. Ushmani, M. Ranjan Mohanty, S. Agrawal, A. Banduni, and S. S. Kakatum Rao, "Evolving zero trust architectures for ai-driven cyber threats in healthcare and other high-risk data environments: A systematic review," *Cureus*, vol. 17, no. 6, 2025, Art. no. e85446.

[28] G. Muriithi, B. Papari, A. Arsalan, L. Timilsina, A. Muriithi, E. Buraimoh, A. Khan, G. Ozkan, C. Edrington, and A. Papari, "Zero trust architecture for electric transportation systems: A systematic survey and deep learning framework for replay attack detection," *IEEE Open J. Veh. Technol.*, vol. 6, pp. 2171–2194, 2025.

[29] K. Denzel, "A survey of security in zero trust network architectures," *GSC Adv. Res. Rev.*, vol. 22, no. 2, pp. 182–214, Feb. 2025.

[30] A. Mehrban, Z. Abou El Houda, H. Moudoud, and L. Bao Le, "Integrating zero trust architecture in O-RAN: A comprehensive survey and analysis," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 10465–10495, 2025.

[31] N. E. Cicek and N. Shafae, "Zero trust micro-segmentation in cloud environments: A systematic literature review of strategies, challenges, and future trends," School Eng., Jönköping Univ., Jönköping, Sweden, Tech. Rep., 2025.

[32] D. R. Sripathi and N. Murali, "A systematic literature review of zero trust architecture and software-defined perimeters," Wilfrid Laurier Univ., Waterloo, Canada, Paper 5358310, 2025.

[33] A. Poirrier, L. Cailleux, and T. Heide Clausen, "Is trust misplaced? A zero-trust survey," *Proc. IEEE*, vol. 113, no. 1, pp. 5–39, Jan. 2025.

[34] S. M. M. Ali, "Artificial intelligence in zero trust architecture for 5G and 6G networks: A systematic literature review," Jamk Univ. Appl. Sci., Jyväskylä, Finland, Tech. Rep., 2025.

[35] T. Zhang and L. Chen, "A review of zero trust architecture security research," in *Proc. 5th Int. Conf. Netw. Commun. Inf. Secur. (ICNCIS)*, Oct. 2025, pp. 80–86.

[36] D. Xu, I. Gondal, X. Yi, T. Susnjak, P. Watters, and T. R. McIntosh, "The erosion of cybersecurity zero-trust principles through generative AI: A survey on the challenges and future directions," *J. Cybersecur. Privacy*, vol. 5, no. 4, p. 87, Oct. 2025.

[37] R. Harish, F. Marothia, S. Nag, D. Gangrade, D. Govindasamy, and P. Poonguzhali, "A comprehensive survey on zero trust architecture in IoT networks," in *Proc. IEEE Int. Conf. Internet Things Intell. Syst. (IoTaIS)*, Nov. 2025, pp. 90–96.

[38] Z. Senan Mahmod Attar Bashi and S. Senan, "A comprehensive review of zero trust network architecture (ZTNA) and deployment frameworks," *Int. J. Perceptive Cognit. Comput.*, vol. 11, no. 1, pp. 148–153, Jan. 2025.

[39] A. A. Albuali, "Zero trust meets AI: A survey across multi-cloud and hybrid environments," in *Proc. IEEE 12th Int. Conf. Commun. Netw. (ComNet)*, Nov. 2025, pp. 1–10.

[40] S. Kulkarni, A. Mylonas, and S. Vidalis, "Using the zero trust five-step implementation process with smart environments: State-of-the-art review and future directions," *Future Internet*, vol. 17, no. 7, p. 313, Jul. 2025.

[41] M. H. Bashaa, W. S. Bhaya, and N. H. K. Al-Aaraji, "Integration of zero trust architecture and machine learning for improving the security of software defined networking: A review," *J. Intell. Informat., Netw., Cybersecur.*, vol. 1, no. 1, p. 1, May 2025.

[42] I. U. Khan, F. M. Khan, Z. A. Haider, and F. Alturise, "Integrating AI, blockchain, and edge computing for zero-trust IoT security: A comprehensive review of advanced cybersecurity framework," *Comput., Mater. Continua*, vol. 85, no. 3, pp. 4307–4344, 2025.

[43] O. Segun Adanigbo, B. Iyanu Adekunle, E. Ogbuefi, O. Timothy Odofin, O. Aderemi Agboola, and D. Kisina, "Implementing zero trust security in multi-cloud microservices platforms: A review and architectural framework," *Int. J. Adv. Multidisciplinary Res. Stud.*, vol. 4, no. 6, pp. 2402–2409, Dec. 2024.

[44] K. Sandhu, S. G. R. Bojja, S. Venkataramanan, V. K. R. Vangoor, and S. Thota, "AI-powered anomaly detection in zero trust environments: A comprehensive review of methods and evaluation," *Nanotechnology Perceptions*, vol. 20, p. S16, Jan. 2024, doi: 10.62441/nano-ntp.vi.5083.

[45] Y. Liu, R. Zhang, H. Luo, Y. Lin, G. Sun, D. Niyato, H. Du, Z. Xiong, Y. Wen, A. Jamalipour, D. In Kim, and P. Zhang, "Secure multi-LLM agentic AI and agentification for edge general intelligence by zero-trust: A survey," 2025, *arXiv:2508.19870*.

[46] K. Qu, M. Zhao, and S. Cui, "Zero trust security in modern networks: A survey of applications, challenges, and future directions," in *Proc. IEEE 8th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC)*, Aug. 2025, pp. 209–214.

[47] V. V. Sangaraju, S. V. A. Rao, A. Shaik, V. G. Prasuna, and P. Nagaraju, "A survey on zero trust security—Applications and challenges," *Proc. Eng. Sci.*, vol. 7, no. 1, pp. 437–446, 2025.

[48] M. Mukhlisin and R. A. Firmansyah, "Zero trust architecture: Solusi keamanan dan privasi untuk institusi pendidikan, systematic literature review," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 4, pp. 6926–6935, May 2025.

[49] A. Dibouliya, "Zero-trust data warehousing for cross-bank AI collaboration: A technical review," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 8, pp. 25–34, Jul. 2025.

[50] S. Chennamsetty and S. A. Averineni, "From network segmentation to AI-driven zero trust: A systematic survey of micro-segmentation technologies," in *Proc. 7th Int. Conf. Electron. Commun., Netw. Comput. Technol. (ECNCT)*, Jul. 2025, pp. 111–117.

[51] D. Schönle and C. Reich, "Hardening zta by AI-driven observation: Survey and case studies of aerospace cyber defence architecture," *Authorea Preprints*, Jun. 2025.

[52] W. O. Hundeyin, "Modernizing IT audit function to support to support zero trust and cloud security—A systematic review," Bowie State Univ. Bowie, USA, vol. 10, no. 10, pp. 249–259, 2025.

[53] M. Liman Gambo and A. Almulhem, "Zero trust architecture: A systematic literature review," 2025, *arXiv:2503.11659*.

[54] D. V. Volkov and K. Agyapong, "Adaptive trust boundary enforcement: A comprehensive review of zero trust architecture implementation and usability challenges," *Int. J. Cyber Threat Intell. Secure Netw.*, vol. 2, no. 10, pp. 11–17, 2025.

[55] J. Wang, X. Jing, Z. Yan, Y. Fu, W. Pedrycz, and L. T. Yang, "A survey on trust evaluation based on machine learning," *ACM Comput. Surv.*, vol. 53, no. 5, pp. 1–36, Sep. 2021.

[56] B. Liu, "A survey on trust modeling from a Bayesian perspective," *Wireless Pers. Commun.*, vol. 112, no. 2, pp. 1205–1227, May 2020.

[57] S. A. Alhandi, H. Kamaludin, and N. A. M. Alduais, "Trust evaluation model in IoT environment: A comprehensive survey," *IEEE Access*, vol. 11, pp. 11165–11182, 2023.

[58] T. Lenard, A. Collen, M. Benyahya, N. A. Nijdam, and B. Genge, "Exploring trust modeling and management techniques in the context of distributed wireless networks: A literature review," *IEEE Access*, vol. 11, pp. 106803–106832, 2023.

[59] E. Saeedi Taleghani, R. I. Maldonado Valencia, A. L. Sandoval Orozco, and L. J. García Villalba, "Trust evaluation techniques for 6G networks: A comprehensive survey with fuzzy algorithm approach," *Electronics*, vol. 13, no. 15, p. 3013, Jul. 2024.

[60] A. Seddighi, S. Asghari, M. Romoozi, and H. Babaei, "A review of game theory-based trust modeling approaches in infrastructure-free social networks," *Manage. Strategies Eng. Sci.*, vol. 7, no. 4, pp. 81–95, 2025.

[61] F. A. Ruambo, D. Zou, I. O. Lopes, B. Yuan, A. Muthanna, M. Zakarya, and M. S. A. Muthanna, "Trust scoring algorithms for zero trust-based software-defined perimeter architectures: A systematic literature review of advancements, challenges, and future directions," *Comput. Electr. Eng.*, vol. 132, Apr. 2026, Art. no. 111002.

[62] L. Yang, Y. Lu, S. X. Yang, T. Guo, and Z. Liang, "A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 4837–4847, Jul. 2021.

[63] Z. Yan, L. Peng, W. Feng, and L. T. Yang, "Social-chain: Decentralized trust evaluation based on blockchain in pervasive social networking," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–28, Feb. 2021.

[64] N. Jiang, J. Wen, J. Li, X. Liu, and D. Jin, "GATrust: A multi-aspect graph attention network model for trust assessment in OSNs," *IEEE Trans. Knowl. Data Eng.*, vol. 35, no. 6, pp. 5865–5878, Jun. 2023.

[65] R. Alboqmi, S. Jahan, and R. F. Gamble, "A runtime trust evaluation mechanism in the service mesh architecture," in *Proc. 10th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2023, pp. 242–249.

[66] T. Khan, K. Singh, K. Ahmad, and K. A. B. Ahmad, "A secure and dependable trust assessment (SDTS) scheme for industrial communication networks," *Sci. Rep.*, vol. 13, no. 1, p. 1910, Feb. 2023.

[67] J. John and K. John Singh, "Trust value evaluation of cloud service providers using fuzzy inference based analytical process," *Sci. Rep.*, vol. 14, no. 1, p. 18028, Aug. 2024.

[68] V. Pathak, K. Singh, T. Khan, M. Shariq, S. A. Chaudhry, and A. K. Das, "A secure and lightweight trust evaluation model for enhancing decision-making in resource-constrained industrial WSNs," *Sci. Rep.*, vol. 14, no. 1, p. 28162, Nov. 2024.

[69] E. Jeong and D. Yang, "A trust score-based access control model for zero trust architecture: Design, sensitivity analysis, and real-world performance evaluation," *Appl. Sci.*, vol. 15, no. 17, p. 9551, Aug. 2025.

[70] S. Xu and Y. Qian, "Quantum-inspired trust scoring for zero trust security: Concepts, models, and research directions," *IEEE Netw.*, pp. 1–8, Dec. 2025.

[71] Y. Mao, W. Fu, Y. Zhao, Z. Yuan, Z. Sun, and Y. Zhao, "A zero-trust access control model based on attribute and dynamic trust evaluation for cloud environments," *Symmetry*, vol. 17, no. 12, p. 2059, Dec. 2025.

[72] S. Xu and Y. Qian, "Dynamic trust scoring for zero trust at the edge: A multi-factor, context-aware approach," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2025, pp. 1–6.

[73] M. Zhang, Y. Cheng, H. Wang, and F. Lv, "OMATE-ZT: Optimized multi-attribute trust evaluation model for zero-trust in industrial Internet of Things," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2025, pp. 5088–5094.

[74] G. Chen, Q. Zhou, J. Huang, and X. Li, "A multidimensional trust assessment method for zero trust dynamic access control," in *Proc. 40th Youth Academic Annu. Conf. Chin. Assoc. Autom. (YAC)*, May 2025, pp. 3170–3176.

[75] X. Liao, S. Yang, J. Xu, L. Liu, W. Liang, S. Yu, Y. Ji, and S. Liu, "Improved trust evaluation model based on PBFT and zero trust integrated power network security defense method," *Symmetry*, vol. 17, no. 11, p. 1982, Nov. 2025.

[76] S. Xu and Y. Qian, "Quantum-inspired trust scoring for zero trust security: A simulation-based approach," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Aug. 2025, pp. 46–49.

[77] C. A. Baykara, I. Şafak, and K. Kalkan, "ZETROS: A zero-trust IoT network security framework using distributed blacklisting, trust scoring and smart contracts," *Comput. Netw.*, vol. 271, Oct. 2025, Art. no. 111601.

[78] L. Sun, S. Liu, Z. Qu, and Y. Zhang, "A federated learning-based zero-trust model with secure dynamic trust evaluation and knowledge transfer," *IEEE J. Sel. Areas Commun.*, vol. 43, no. 6, pp. 2087–2099, Jun. 2025.

[79] M. Bampatsikos, "Advanced trust evaluation and estimation solutions for the Internet of Things," Ph.D. dissertation, Univ. Piraeus, Piraeus, Greece, 2025.
[80] Z. Li, X. Du, X. Wu, A. Liu, and S. Wang, "Gatac: Research on microservice access control techniques based on trust assessment and game analysis," *Cybersecurity*, vol. 8, no. 1, p. 122, Dec. 2025.
[81] X. Wang, Q. Yuan, Y. Wang, J. Teng, J. Tao, and M. Shen, "Zero trust-driven collaborative intrusion detection in Internet of Things: A continuous trust assessment approach," *IEEE Internet Comput.*, vol. 29, no. 4, pp. 37–47, Jul. 2025.
[82] D. Huang, L. Zhu, Z. Zhang, Y. Na, Z. Li, and X. Fang, "Dynamic splitting and merging control strategy for vehicle platoon based on trust evaluation in a zero-trust environment," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 12693–12709, 2025.
[83] R. Wei, D. Huang, and Y. Na, "Realtime cross-layered trust quantification enhancing security resilience of V2X platoons under zero-trust framework," in *Proc. 9th CAA Int. Conf. Veh. Control Intell. (CVCI)*, Oct. 2025, pp. 1–6.
[84] S. Bhola, "Tenko: A zero trust inspired framework for real-time network defense via intelligent thresholding and node-level anomaly scoring," Ph.D. thesis, Virginia Polytech. Inst. State Univ., Blacksburg, VA, USA, 2025.
[85] Y. Zhou, D. Huang, and Y. Na, "Blockchain-based trust evaluation for intelligent connected vehicles in a zero-trust environment," in *Proc. 9th CAA Int. Conf. Veh. Control Intell. (CVCI)*, Oct. 2025, pp. 1–6.
[86] Z. Xiao, K. Jiang, M. Tan, and Y. Lin, "A web identity and attribute assessment-based zero trust access control model," in *Proc. 18th Int. Congr. Image Signal Process., Biomed. Eng. Informat. (CISP-BMEI)*, Oct. 2025, pp. 1–9.
[87] D. Huang, Y. Bao, Y. Na, and Z. Li, "Consistency control method for intelligent connected vehicle platoon based on dynamic trust evaluation under the zero-trust framework," *Chaos, Solitons Fractals*, vol. 200, Nov. 2025, Art. no. 117024.
[88] S. Amanlou, R. Doss, and J. Li, "Implementing a dynamic and context-aware trust evaluation model for zero trust architecture (ZTA): A fuzzy logic approach," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, May 2025, pp. 404–411.
[89] J. Xu, D. Huang, Y. Na, and Y. Zhou, "Trust evaluation of intelligent ships and shore-based service platforms in a zero trust environment," in *Proc. CAA Symp. Fault Detection, Supervision, Saf. Tech. Processes (SAFEPROCESS)*, Aug. 2025, pp. 1–6.
[90] H. Zhang, H. Yang, H. Li, Y. Zhang, P. Chen, W. Wang, and D. Tang, "A heterogeneous GNN based trust evaluation method for remote desktop access," in *Proc. IEEE 24th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Nov. 2025, pp. 2346–2354.
[91] R. Ma, D. Huang, and Y. Na, "Lightweight dynamic evaluation models in a zero trust environment," in *Proc. 9th CAA Int. Conf. Veh. Control Intell. (CVCI)*, Oct. 2025, pp. 1–6.
[92] S. Swami, I. Singh, and C. Prawah Pant, "SCI-IoT: A quantitative framework for trust scoring and certification of IoT devices," 2025, *arXiv:2511.18045*.
[93] S. Higashi, P. Kraikritayakul, Y. Liu, M. Ikeda, K. Matsuo, and L. Barolli, "Design and performance comparison of two implemented trust evaluation models for fifth generation (5G) and beyond 5G (B5G) network slicing using an interval type-2 fuzzy logic system," *J. High Speed Netw.*, vol. 32, no. 1, pp. 37–59, Feb. 2026.
[94] A. Arsalan, B. Papari, G. K. Muriithi, A. A. Khan, G. Ozkan, and C. S. Edrington, "Trust evaluation framework for adaptive load optimization in motor drive system," *Electronics*, vol. 14, no. 18, p. 3697, Sep. 2025.
[95] P. N. Renjith, S. Balasubramani, K. Ramesh, and E. Patnala, "An initial risk assessment for multimodal with LSTM-based trust evaluation framework for autonomous vehicle security," *Social Netw. Comput. Sci.*, vol. 6, no. 2, p. 172, Feb. 2025.
[96] O. J. M. Smith, "FPGA-accelerated gnn pipelines for real-time identity threat scoring in zero-trust cloud systems," *J. Reconfigurable Hardw. Archit. Embedded Syst.*, vol. 2, no. 3, pp. 17–25, 2025.
[97] A. Akli and K. Chougdali, "Towards tamper-proof trust evaluation of Internet of Things nodes leveraging IOTA ledger," *Sensors*, vol. 25, no. 15, p. 4697, Jul. 2025.
[98] N. Kaur, A. Mittal, A. Jain, U. K. Lilhore, S. M. Aldossary, S. Simaiya, E. S. Ghith, A. Baihan, H. A. Abdallah, and M. M. Khan, "Blockchain-enhanced security and Bayesian trust assessment for secure task scheduling in latency-critical fog computing environments," *J. Cloud Comput.*, vol. 14, no. 1, p. 53, Sep. 2025.
[99] P. K. Mishra, R. R. Kumar, D. Muduli, and S. Raj, "A hybrid AHP and rule-based trust evaluation framework for dynamic multi-cloud environments," in *Proc. Int. Conf. Cognit., Green Ubiquitous Comput. (IC-CGU)*, Oct. 2025, pp. 1–6.
[100] D. Zhao, Y. Zhao, and X. Dou, "Dynamic access control and fine-grained searchable encryption for cloud data using trust evaluation and B-tree indexing," *Informatica*, vol. 49, no. 34, Aug. 2025.
[101] S. H. Konda, "Membership-driven shrink reduction with a privacy-centric retail architecture and trust-scoring framework," Arkansas, USA, Tech. Rep., 2025, doi: 10.36227/techrxiv.176541757.73983335/v1.
[102] V. M. Avalos and C. Tunc, "Trust evaluation based on a risk assessment and game theory for virtual machines in a cloud environment," in *Proc. 10th Int. Conf. Fog Mobile Edge Comput. (FMEC)*, May 2025, pp. 58–65.
[103] Y. Xia, Y. Liu, W. Zhang, J. Yin, J. Hu, T. Liang, and H. Zhang, "DRL-aided trust evaluation for malicious host detection in artificial intelligence of things," *IEEE Trans. Netw. Sci. Eng.*, vol. 13, pp. 2777–2792, 2026.
[104] M. Mann, R. P. Badoni, P. Narooka, M. Janarthanan, R. A. Mahajan, J. K. Samriya, and D. Panwar, "Spatiotemporal trust evaluation using a neutrosophic model under sensor uncertainty," *Discover Comput.*, vol. 28, no. 1, p. 249, Nov. 2025.
[105] X. Li, Y. Xiao, W. Mei, C. Kang, Y. Li, and L. Shen, "An adaptive trust evaluation method for distribution terminal based on multi-dimensional behavior features," in *Proc. IEEE 3rd Int. Conf. Control, Electron. Comput. Technol. (ICCECT)*, Apr. 2025, pp. 478–482.
[106] O. Hussien and H. Jahankhani, "DTLS-trust: A blockchain-enhanced security framework with AI based trust scoring for UDP communications," in *Proc. 5th Int. Conf. Innov. Res. Appl. Sci., Eng. Technol. (IRASET)*, May 2025, pp. 1–16.
[107] P. Selvaprasanth and P. Meenalochini, "Design and implementation of a context-aware artificial intelligence framework integrating trust evaluation for personalized cloud service recommendation systems," *J. Sci. Technol. Res.*, vol. 6, no. 2, pp. 1–14, 2025.
[108] A. N. Kalejaiye, "Causal modeling of insider threat behavior using probabilistic graphical networks to strengthen organizational cyber-resilience and trust architectures," *Int. J. Res. Publication Rev.*, vol. 6, no. 7, pp. 2370–2387, Jul. 2025.
[109] J. Gu, J. Feng, and Z. Gao, "Multimodal dynamic weighted authentication trust evaluation under zero trust architecture," *Electronics*, vol. 15, no. 3, p. 592, Jan. 2026.
[110] D. Huang, L. Zhang, Y. Na, F. Bu, and Z. Li, "A trust assessment method for intelligent connected vehicles based on data consistency verification matched with adaptive leader election in a zero-trust framework," *IEEE Trans. Dependable Secure Comput.*, vol. 23, no. 3, pp. 5355–5370, May 2026.
[111] X. Wang, Q. Yuan, C. Liu, P. Wang, J. Tao, L. Li, X. Wang, and Y. Wang, "Who is the wolf in sheep's clothing? A context-aware trust evaluation model for malicious UAV detection during authentication," *Comput. Netw.*, vol. 279, Apr. 2026, Art. no. 112145.
[112] N. Moustafa, "Designing an online and reliable statistical anomaly detection framework for dealing with large high-speed network traffic," Ph.D. thesis, UNSW Sydney, Sydney, NSW, Australia, 2017.
[113] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, 2018, pp. 108–116.
[114] I. Ullah and Q. H. Mahmoud, "A scheme for generating a dataset for anomalous activity detection in IoT networks," in *Proc. Can. Conf. Artif. Intell.* Cham, Switzerland: Springer, 2020, pp. 508–520.
[115] *Kitsune Network Attack*, UCI Machine Learning Repository, Beersheba, Israel, 2019, doi: 10.24432/C5D90Q.
[116] B. S. Sharmila and R. Nagapadma, "RT-IoT2022," UCI Mach. Learn. Repository, Mysuru, Karnataka, India, Tech. Rep., 2023, doi: 10.24432/C5P338.
[117] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors*, vol. 23, no. 13, p. 5941, Jun. 2023.

**SEUNG-WOO NAM** received the B.S. degree from Korea University, Sejong Campus, in 2024, where he is currently pursuing the integrated M.S. and Ph.D. degrees in computer and information software.

He has extensive experience in data-intensive research involving large-scale session data and network traffic analysis and in machine learning-based feature extraction and embedding representations. His work emphasizes memory-efficient data preprocessing, structured feature generation, and representation learning for security analytics, while bridging theoretical modeling with practical implementation challenges in real-world systems. His research interests include trust modeling in zero trust architecture, trust-aware access control, machine learning and deep learning for security analytics, data-driven decision-making frameworks, and bridge the gap between conceptual trust models and their practical applicability in real-world security systems, contributing to a clearer and more structured understanding of trust quantification in modern cybersecurity architecture.

**GYEONG-MIN YU** (Graduate Student Member, IEEE) received the M.S. degree from Korea University, Sejong Campus, in 2026, where she is currently pursuing the Ph.D. degree in computer and information software.

Her research experience includes network traffic analysis, data-driven network behavior analysis, and system-level experimentation involving real network environments. Her work focuses on analyzing network behavior patterns and extracting meaningful features from network data for intelligent network management and security analytics. Her research interests include network traffic analysis, intelligent network management, machine learning-based network behavior analysis, the understanding of complex network environments through data-driven methodologies, and to contribute to the development of efficient and intelligent network monitoring and management systems.

**YOON-SEONG JANG** (Graduate Student Member, IEEE) received the B.S. degree from Korea University, Sejong Campus, in 2024, where he is currently pursuing the integrated M.S. and Ph.D. degrees in computer and information software.

His research experience includes network traffic analysis, data-driven network behavior analysis, and experimental system research based on real network environments. His work focuses on analyzing structural characteristics of network traffic data and extracting meaningful features to support intelligent network management and security analytics. His research interests include network traffic analysis, application traffic classification, and machine learning-based network data analysis. His work aims to enhance the understanding of complex network environments through data-driven methodologies and to contribute to the development of intelligent network monitoring and traffic analysis systems.

**JU-SUNG KIM** received the B.S. degree from Korea University, Sejong Campus, in 2024, where he is currently pursuing the integrated M.S. and Ph.D. degrees in computer and information software.

His research experience includes network traffic analysis, network data processing, and system-level experimentation based on real network environments. His work focuses on analyzing network traffic patterns and extracting structured features from network data to support intelligent network monitoring and security analytics. His research interests include network traffic analysis, intelligent network management, and machine learning-based network data analysis, improve the understanding of complex network environments through data-driven methodologies, and to contribute to the development of efficient network monitoring and traffic analysis systems.

**JI-MIN KIM** received the B.S. degree from Korea University, Sejong Campus, in 2026, where he is currently pursuing the integrated M.S. and Ph.D. degrees in computer and information software.

His research experience includes network traffic analysis, network data processing, and experimental studies based on real network environments. His work focuses on analyzing network traffic patterns and extracting structured features from network data to support intelligent network monitoring and security analytics. His research interests include network traffic analysis, intelligent network management, and machine learning-based network data analysis, to enhance the understanding of complex network environments through data-driven methodologies, and to contribute to the development of efficient and intelligent network monitoring systems.

**MYUNG-SUP KIM** received the Ph.D. degree from Pohang University of Science and Technology, in 2004.

He is currently a Professor in computer and information software at Korea University, Sejong Campus. His research interests include network traffic analysis, internet traffic monitoring, and data-driven network management. He has extensive experience in large-scale network measurement, traffic classification, and the design of intelligent network monitoring systems based on machine learning and data analytics. His work emphasizes the analysis and modeling of network behavior through large-scale traffic data to improve the efficiency, reliability, and security of modern network infrastructures. His research interests include network traffic analysis, internet traffic classification, network monitoring and management, and machine learning-based network analytics. His work aimed to advance data-driven methodologies for understanding complex network environments and developing scalable and intelligent systems for next-generation network management and security.