

Securing Reliable Fog Computing Environments: A Systematic Literature Review and Future Research Directions

Vina Gautam¹, Ujwal Lanjewar²

¹Research Scholar, ¹Assistant Professor, ²Principal

¹Department Of Electronics and Computer Science, Rastrasant Tukadoji Maharaj Nagpur University, Nagpur

¹Dhote Bandhu Science College, Gondia

²Shrimati Binzani Mahila Mahavidyalaya, RTM Nagpur University, Nagpur, India

¹vinal.vina.gtm@gmail.com, ²ualanjewar@gmail.com

Abstract: Fog computing extends cloud services toward edge nodes by distributing computation, storage, and networking closer to data sources. This architecture can reduce network latency and bandwidth requirements. However, the distribution of computing resources also introduces reliability challenges and increases the attack surface. Traditional security mechanisms may provide limited protection when attackers use valid credentials or compromise legitimate fog nodes. This systematic literature review examines the development and integration of reliability mechanisms, security frameworks, behavioural analytics, dynamic trust evaluation, and deception-based approaches in fog computing, with particular attention to data-theft prevention and insider threats. The review considers studies published between 2012 and 2025 and uses a structured literature-search, screening, eligibility assessment, quality evaluation, and thematic synthesis process. The findings indicate that existing fog-security approaches are largely based on preventive mechanisms, including authentication, encryption, access control, and trust management. These mechanisms provide essential protection but may be insufficient against insiders or compromised entities using legitimate privileges. Data theft can occur without disrupting service availability. The review further indicates that deception mechanisms are commonly investigated separately from behavioural analytics and dynamic trust evaluation, while adaptive integration remains limited. Effective protection against stealthy data theft in fog computing therefore requires a shift from isolated security controls toward integrated and adaptive protection. Future fog-security architectures should combine continuous behaviour profiling, dynamic trust evaluation, anomaly detection, and context-aware decoy selection while considering the resource, latency, scalability, and reliability constraints of fog environments.

Keywords: Fog computing; reliability; security; data theft; insider threats; behavioral analytics; trust management; anomaly detection; adaptive security; deception; decoy data;

1. Introduction

Fog computing extends cloud computing by bringing computation, storage, and networking closer to IoT devices and end users. This approach can reduce latency and bandwidth use and support applications that require faster local processing [1–4]. However, fog environments consist of distributed, heterogeneous, resource-limited, and sometimes mobile nodes. These conditions create challenges related to reliability, resource management, fault tolerance, availability, and recovery [5–8]. Fog environments may include gateways, routers, access points, micro-data centers, and other heterogeneous computing nodes distributed across different geographical locations, as illustrated in Figure 1.

Security is another major concern because fog nodes may operate across different locations and administrative environments and can be physically exposed. Common threats include unauthorized access, eavesdropping, denial-



of-service attacks, node compromise, privacy violations, and malicious or compromised devices [9–12]. Fog computing faces several security risks because of its distributed architecture, heterogeneous devices, limited resources, and exposure to physical environments [9–12,31]. The major threats affecting fog environments are summarized in Figure 2. Conventional mechanisms such as authentication, authorization, access control, encryption, privacy protection, and trust management provide important protection, but they may be less effective when legitimate credentials are misused or a trusted fog node is compromised [9–12,16,17,23,25–28].

Insider-driven data theft is particularly difficult because an attacker may access sensitive information without disrupting normal services. Such attacks can therefore remain unnoticed when security decisions depend mainly on identity and authorization [13,14]. Behaviour-based anomaly detection can help identify unusual access patterns [14,15], while trust-management approaches provide additional information about the reliability of users, devices, and fog nodes [16,17]. Deception techniques such as decoy data, decoy documents, and honeypots can further help detect, mislead, or divert attackers [13,18,19]. However, these approaches have largely been studied separately, and adaptive integration between behaviour analysis, trust evaluation, anomaly detection, and deception remains limited [20].

The literature also shows that reliability and security are closely connected in fog computing. Security mechanisms consume computational and communication resources, while node failures, overload, and connectivity problems can affect the availability of security services [6–8]. Therefore, a practical data-theft protection mechanism must provide effective security without creating excessive overhead or affecting fog-service reliability.

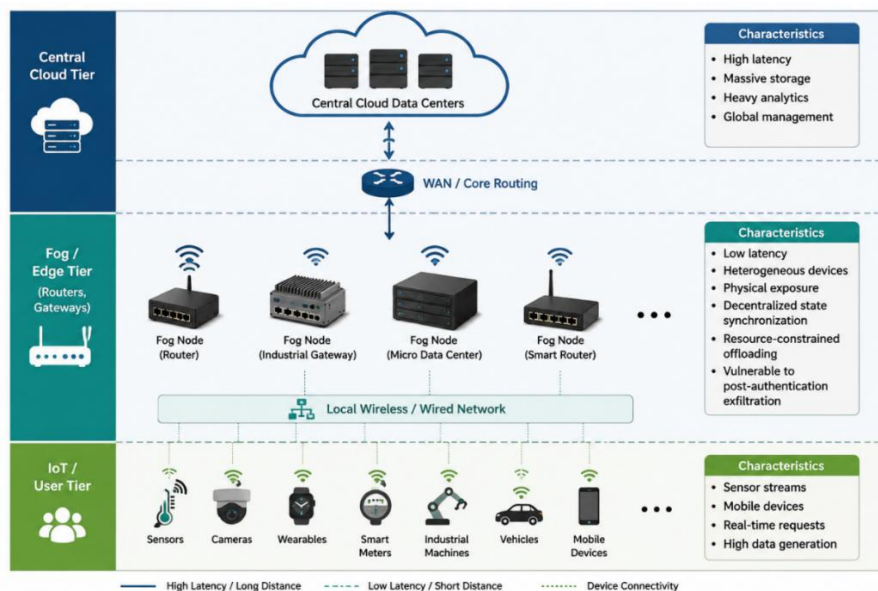


Figure 1. Fog Computing Architecture

This systematic literature review examines research on reliable and secure fog computing from **2012 to 2025**, with particular focus on insider threats, data theft, behaviour-based anomaly detection, trust management, and deception-based protection. The review compares existing approaches in terms of security effectiveness, detection capability, adaptability, computational overhead, latency, scalability, and reliability. It also identifies the main research gaps and future directions for developing an integrated and lightweight approach to data-theft prevention in fog computing.

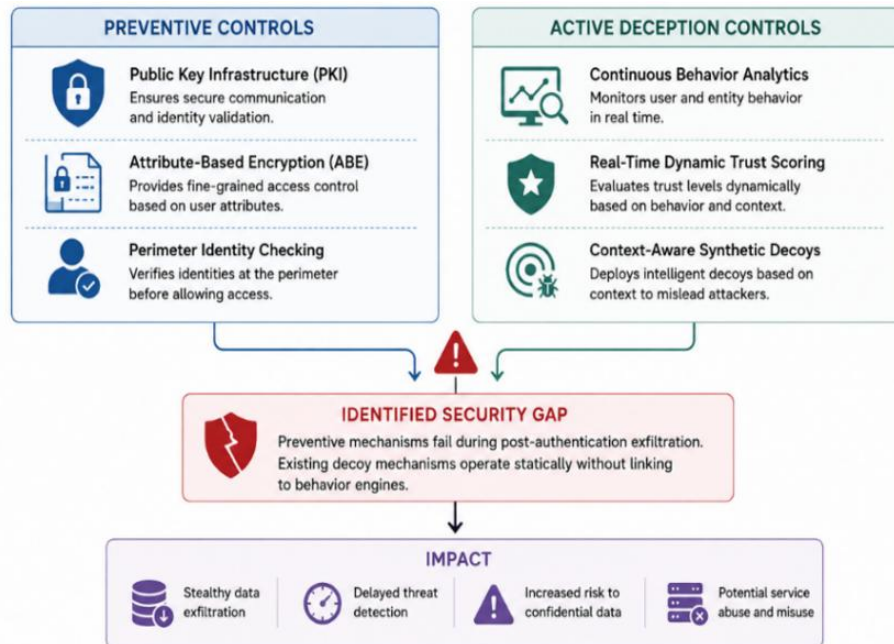


Figure 2. Security Threat Landscape in Fog Computing

Organization of the Paper

The remainder of the paper is organized as follows. Section 2 presents the systematic review methodology, including the search strategy, databases, eligibility criteria, study selection, quality assessment, and data extraction process. Section 3 presents the systematic results and thematic synthesis of the reviewed studies. Section 4 discusses the integrated evidence and research gap identified from the literature. Section 5 provides a critical synthesis of the major research gaps. Section 6 presents an illustrative healthcare case study showing the application of behaviour-aware and deception-based data-theft prevention in a fog-based healthcare environment. Section 7 discusses the limitations and threats to validity of the review. Section 8 presents future research directions and a strategic roadmap. Finally, Section 9 concludes the review and summarizes the main findings.

Research Objectives

The objectives of this systematic literature review are formulated to progressively examine the broader evolution of fog computing and its reliability and security requirements and then focus on the specific research gap concerning adaptive, behaviour-aware prevention of data theft.

OBJ1: To examine the evolution of fog computing research and identify major trends in reliability and security from 2012 to 2025.

OBJ2: To analyze major reliability and dependability challenges in fog computing, including fault tolerance, redundancy, resource management, load distribution, availability, resilience, and recovery.

OBJ3: To classify major security threats and structural vulnerabilities across different layers of fog-computing architectures.

OBJ4: To critically evaluate conventional fog-security mechanisms, including authentication, authorization, access control, encryption, privacy preservation, and trust management.

OBJ5: To investigate data-theft and data-exfiltration attack vectors in fog computing, with particular emphasis on insider threats, compromised entities, and misuse of legitimate credentials.

OBJ6: To examine behaviour-based and anomaly-detection techniques for identifying suspicious activities involving users, devices, and fog nodes.

OBJ7: To assess adaptive security mechanisms capable of dynamically responding to changing user behaviour, system conditions, and threat patterns.

OBJ8: To examine the application of honeypots, decoy data, decoy documents, honeyfiles, and other deception-based mechanisms for detecting, delaying, misleading, and preventing unauthorized data access and theft.

OBJ9: To comparatively evaluate existing reliability and security approaches in terms of security effectiveness, detection capability, adaptability, computational overhead, latency, scalability, and impact on system reliability.

OBJ10: To identify major research gaps and develop a future research roadmap for an integrated, lightweight, behavior-aware, trust-informed, and adaptive deception framework for data-theft prevention in fog computing.

Research Questions

The research questions are designed to progressively narrow the review from the broader development of fog computing to the specific problem of adaptive and behavior-aware data-theft prevention.

RQ1: How has research on reliability and security in fog computing evolved between 2012 and 2025, and what major research trends can be identified during this period?

RQ2: What are the major reliability challenges in fog computing, and what techniques have been proposed to address fault tolerance, redundancy, resource management, availability, and recovery?

RQ3: What are the major security vulnerabilities and data-theft threats affecting fog computing, and what are the limitations of conventional cryptographic and access-control mechanisms against such threats?

RQ4: How do external attacks differ from insider and compromised-entity threats in fog environments, particularly when legitimate credentials or privileges are misused for data theft?

RQ5: How can behavior analytics, dynamic trust evaluation, anomaly detection, adaptive security, and deception-based mechanisms be integrated to improve data-theft prevention in fog computing?

The mapping between the research questions, corresponding objectives, and their main analytical focus is presented in **Table 1**.

Table 1. Research Question–Objective Alignment

RQ	Related Objectives	Main Analytical Focus
RQ 1	OBJ1, OBJ10	Evolution, trends, research development, and emerging directions
RQ 2	OBJ2, OBJ9	Reliability, fault tolerance, redundancy, resource management, availability, recovery, and reliability impact
RQ 3	OBJ3, OBJ4, OBJ9	Security vulnerabilities, threats, preventive security mechanisms, and their limitations
RQ 4	OBJ5, OBJ9	Insider threats, compromised entities, credential misuse, data theft/exfiltration, and detection challenges
RQ 5	OBJ6, OBJ7, OBJ8, OBJ9, OBJ10	Behaviour analytics, anomaly detection, trust, adaptive security, deception, decoys, comparative effectiveness, research gaps, and future directions

2. Methodology

This systematic literature review employed a structured and reproducible methodology for literature identification, screening, eligibility assessment, quality evaluation, data extraction, and thematic synthesis. The review

process was designed to ensure transparency, consistency, and reproducibility in the identification, screening, eligibility assessment, and selection of relevant studies. The search covered literature published from January 2012 to December 2025. The starting year was selected to capture the emergence of fog computing as a distinct computing paradigm. Studies published during till 2025 were treated as recent evidence because the year represents a partial publication period.

Search Strategy and Databases

A structured literature search was conducted across major scientific databases and digital libraries. The primary sources included IEEE Xplore, ACM Digital Library, Scopus, Web of Science, ScienceDirect, SpringerLink, PubMed, and Google Scholar. These sources were selected to provide broad coverage of computer science, networking, cybersecurity, distributed systems, Internet of Things, and reliability research.

The search strategy was developed around four thematic concepts: fog computing, reliability, security and data protection, and behavior-aware or deception-based defense. Synonyms and related terms were included to reduce the possibility of missing relevant studies because of differences in terminology across research communities.

The general search structure was defined as:

("Fog Computing" OR "Fog Environment" OR "Fog-Cloud Computing"

OR "Edge Computing")

AND

("Reliability" OR "Dependability" OR "Fault Tolerance"

OR "Availability" OR "Redundancy" OR "Recovery")

AND

("Security" OR "Privacy" OR "Authentication" OR "Authorization"

OR "Access Control" OR "Trust" OR "Intrusion Detection"

OR "Anomaly Detection")

A second search string was used to specifically identify literature related to data theft, insider threats, behaviour analysis, adaptive security, and deception:

("Fog Computing" OR "Fog Environment" OR "Edge Computing")

AND

("Data Theft" OR "Data Exfiltration" OR "Insider Threat"

OR "Credential Misuse" OR "Malicious Insider")

AND

("Behaviour Analysis" OR "Behavior Analytics"

OR "User Behaviour Profiling" OR "Anomaly Detection"

OR "Adaptive Security" OR "Dynamic Trust"

OR "Decoy Data" OR "Honeyfile" OR "Honeypot"

OR "Deception")

A broader supplementary search was also considered necessary because terminology related to deception and insider-threat detection is not consistently associated with the term *fog computing*. Therefore, studies from closely related distributed environments were examined when their mechanisms had clear applicability to fog computing:

("Edge Computing" OR "Cloud Computing"
 OR "Distributed Computing")
 AND
 ("Insider Threat" OR "Data Exfiltration"
 OR "User Behavior Profiling" OR "Behavior Analytics"
 OR "Decoy" OR "Honeyfile" OR "Deception")

The supplementary search was not used to classify non-fog studies as fog-specific evidence. Instead, such studies were categorized as transferable evidence and were used to examine whether behavioral and deception mechanisms developed in adjacent computing environments could inform future fog-security research.

Search Concept Framework

The four domains were conceptually defined for search construction and were not treated as mutually exclusive analytical categories, since individual studies may address multiple domains simultaneously. These four domains and their corresponding keywords are summarized in **Table 2**.

Table 2. Domain Classification and Keyword Mapping Framework

Domain	Primary terms	Purpose
D1: Computing Environment	Fog computing, fog environment, fog-cloud, edge computing	Identify the target computing paradigm
D2: Reliability	Reliability, dependability, fault tolerance, redundancy, availability, recovery	Identify reliability mechanisms and challenges
D3: Security & Data Protection	Security, privacy, authentication, authorization, access control, trust, IDS, anomaly detection	Identify conventional and intelligent security mechanisms
D4: Behaviour & Deception	Behaviour analytics, behaviour profiling, data theft, insider threat, adaptive security, dynamic trust, decoy, honeyfile, deception	Identify mechanisms relevant to stealthy data theft

Eligibility Criteria

Predefined eligibility criteria were established before study screening to ensure consistent and reproducible study selection. The criteria were aligned with the research questions and the main thematic areas of the review, including fog-computing reliability, security, data protection, behavioural analysis, adaptive security, trust management, and deception-based mechanisms.

Inclusion Criteria

Studies were included when they satisfied the following conditions:

1. **Publication type:** Peer-reviewed journal articles and full-length peer-reviewed conference papers were considered.
2. **Publication period:** Studies published between 2012 and 2025 were considered.

3. **Research relevance:** Studies addressing fog computing, fog-cloud environments, or closely related edge-computing environments were considered when their findings were directly relevant to the research questions.
4. **Reliability:** Studies addressing fault tolerance, redundancy, resource management, load distribution/load balancing, availability, resilience, recovery, dependability, or related reliability mechanisms were eligible.
5. **Security:** Studies addressing authentication, authorization, access control, encryption, privacy, trust management, intrusion detection, anomaly detection, or other fog-security mechanisms were eligible.
6. **Data security:** Studies investigating unauthorized data access, data leakage, data theft, data exfiltration, insider threats, credential misuse, or compromised entities were considered.
7. **Behaviour and adaptive security:** Studies examining user/device behaviour, behavioural profiling, anomaly detection, dynamic trust, adaptive security, or context-aware security were included.
8. **Deception mechanisms:** Studies investigating honeypots, honeyfiles, decoy data, honeytokens, deception environments, or other deception-based defense mechanisms were included when they had relevance to data protection or threat detection.
9. **Technical contribution:** The study had to present a clearly described technical model, framework, algorithm, protocol, architecture, experiment, simulation, or empirical evaluation.
10. **Accessibility:** The publication had to provide sufficient bibliographic and methodological information for systematic data extraction and quality assessment.

Exclusion Criteria

Studies were excluded when they met one or more of the following conditions:

1. Studies focused exclusively on centralized cloud computing without a meaningful fog or edge-computing context.
2. Studies unrelated to the security, reliability, privacy, trust, behavioural analysis, data protection, or deception aspects covered by the research questions.
3. Non-peer-reviewed material, including editorials, magazine articles, posters, abstracts, theses, dissertations, technical reports, and non-reviewed preprints, unless specifically retained for supplementary background evidence.
4. Duplicate publications or multiple reports describing substantially the same study. Where multiple versions existed, the most complete and authoritative version was retained.
5. Studies that did not provide sufficient technical information to understand the proposed mechanism or methodology.
6. Studies lacking meaningful technical evaluation, validation, simulation, experimentation, formal analysis, or empirical assessment, where such evaluation was necessary to support the study's claims.
7. Studies for which the full text could not be obtained after reasonable retrieval attempts.
8. Studies published outside the defined **2012–2025** period.

Eligibility decision process

The study-selection process was conducted through sequential stages. First, duplicate records were removed from the combined database results. Second, titles and abstracts were screened against the predefined inclusion and exclusion criteria. Finally, potentially relevant studies underwent full-text assessment. Reasons for exclusion at the

full-text stage were recorded to ensure transparency and consistency in the study-selection process. The study-selection process consisted of the following stages:

Identification → Deduplication → Title/Abstract Screening → Full-Text Assessment → Quality Assessment → Final Inclusion

The study-selection process was conducted through sequential stages, beginning with identification and duplicate removal, followed by title and abstract screening, full-text assessment, quality assessment, and final inclusion. The overall study-selection process is presented in Figure 3.

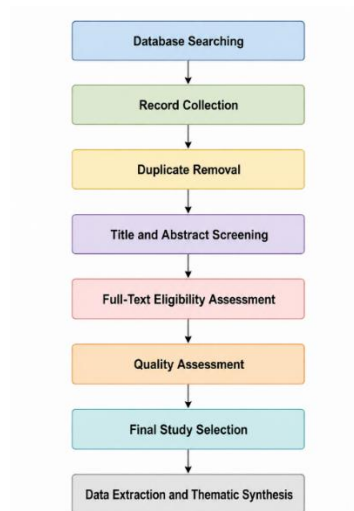


Figure 3. Systematic Literature Review Study-Selection Process

Quality Assessment

Each potentially eligible study was assessed using predefined methodological and technical quality criteria. The assessment considered the clarity of the research objective, description of the proposed method, technical contribution, evaluation or validation procedure, clarity of reported results, and availability of sufficient methodological information for comparison. Studies with insufficient methodological or technical information were excluded during the quality-assessment stage. The quality assessment also informed the interpretation of evidence and the identification of research gaps.

Data Extraction and Synthesis

Data were extracted from the selected studies using a predefined evidence-extraction framework. The extracted information included publication year, computing environment, application domain, reliability mechanism, security mechanism, threat type, data-theft relevance, behaviour analysis, anomaly detection, trust management, deception mechanism, adaptive capability, evaluation method, computational overhead, latency, scalability, and reported limitations. The extracted evidence was grouped according to the research questions and synthesized thematically to identify research trends, common approaches, limitations, and unresolved research gaps.

3. Systematic Results and Thematic Synthesis

Characteristics and Thematic Distribution of the Reviewed Studies

The included literature demonstrates a progressive evolution of fog-computing research from foundational architectural and resource-management concerns toward more specialized security, trust, anomaly-detection, and

deception-based mechanisms. The reviewed studies were therefore grouped according to their dominant research contribution, while recognizing that several studies address more than one thematic area. Foundational studies established fog computing as a distributed extension of cloud capabilities toward network-edge locations, emphasizing proximity to data sources, reduced latency, resource distribution, and support for IoT applications [1–5]. Subsequent research increasingly addressed the reliability, resilience, security, and privacy challenges associated with geographically distributed and resource-constrained fog environments [6–12,21,31–34].

The evidence also shows that reliability and security have developed as closely related but largely distinct research streams. Reliability-oriented studies primarily investigate resource management, fault tolerance, resilience, availability, load balancing, and recovery [6–8,21,22]. Security-oriented studies, in contrast, predominantly examine authentication, access control, privacy preservation, cryptographic protection, intrusion detection, and trust management [9–12,23,25,31–34]. Although these mechanisms provide important protection, relatively few studies evaluate their combined effect on both security and fog-service reliability.

A separate research stream has focused on insider threats and anomalous behaviour. Stolfo et al. specifically examined insider data-theft threats in cloud/fog environments and proposed the use of decoy information as an additional protection mechanism [13]. Chen et al. investigated anomalous insider behaviour in collaborative information systems, demonstrating the relevance of behavioural characteristics for identifying potentially malicious insiders [14]. Deep-learning-based distributed attack detection subsequently extended anomaly detection toward fog-to-things environments [15]. More recent systematic reviews confirm the growing importance of intrusion detection, anomaly detection, and intelligent security mechanisms in fog environments [29,30].

Trust management represents another important research direction. Trust-based mechanisms have been investigated for fog-enabled vehicular environments and general fog services to support more informed security decisions concerning nodes, users, and interactions [16,17,26–28]. These studies demonstrate the potential of dynamically updating trust information according to observed behaviour and interaction history. However, trust evaluation has generally been investigated as a mechanism for authentication, node selection, access control, or service management rather than as an explicit decision mechanism for adaptive data-theft deception.

Deception-based security forms a comparatively smaller but strategically important research stream. Decoy documents were investigated as a means of detecting and misleading malicious insiders and increasing the uncertainty associated with stolen information [13,18]. Broader defensive-deception research subsequently established taxonomies and strategic models for deception in cybersecurity [19]. However, the reviewed literature indicates that deception is still less extensively investigated in fog computing than conventional security mechanisms, particularly when deception must be dynamically selected according to observed behaviour, trust level, threat context, and fog-resource conditions. The main research themes, representative references, and their relevance to the present review are summarized in **Table 3**.

Table 3. Thematic distribution of the core evidence base

Research theme	Representative references	Principal contribution	Relationship to the present review
Fog architecture and evolution	[1–5]	Defines fog computing, edge proximity, resource distribution, and IoT applications	Establishes the technological context
Reliability and resilience	[6–8,21,22]	Fault tolerance, resource management, resilience, availability, and recovery	Addresses RQ1–RQ2
Conventional fog security	[9–12,23,25,31–34]	Authentication, access control, privacy,	Addresses RQ3

		encryption, and security frameworks	
Insider threats and data theft	[13,14]	Insider data theft, anomalous insider behaviour, and data-access monitoring	Addresses RQ4
ML/anomaly-based detection	[15,29,30]	Machine learning, deep learning, intrusion detection, and anomaly detection	Addresses RQ4–RQ5
Trust management	[16,17,26–28]	Trust evaluation, node/service trust, and trust-based security decisions	Addresses RQ3–RQ5
Deception and decoy mechanisms	[13,18,19]	Decoy documents and defensive deception	Addresses RQ5
Integrated security research	[6,25,31–34]	Reviews relationships among security, privacy, trust, and emerging mechanisms	Supports cross-theme synthesis

Research Evolution and Reliability Analysis (RQ1 and RQ2)

The reviewed literature shows a gradual development of fog-computing research from 2012 to 2025. Early studies focused on defining fog computing and its role in reducing latency and bringing computation and storage closer to IoT devices [1–4]. Later surveys expanded this work to fog architectures, resource management, applications, and research challenges [2,5]. During this period, reliability and security were mostly studied as separate concerns.

From 2017 onward, the use of fog computing in areas such as healthcare, vehicular systems, and IoT brought new challenges, including changing workloads, node failures, mobility, limited resources, and unstable connectivity [16,17,24]. As a result, researchers increasingly studied resource allocation, load balancing, fault tolerance, resilience, task management, and recovery [6–8,21,22]. The literature also shows that reliability and security are closely related in fog environments. Security mechanisms require computing, memory, communication, and energy resources, while node failures, overload, and connectivity problems can reduce the availability of security services [6,8]. Therefore, stronger security should not create excessive overhead or latency on resource-limited fog nodes.

Recent studies have given greater attention to intelligent and adaptive security, including trust management, intrusion detection, anomaly detection, and privacy protection based on changing user, node, and system behaviour [16,17,26–34]. Reviews of fog security and intrusion detection also show a shift from static security policies toward more intelligent and adaptive monitoring [29,30,34]. However, the literature is still largely divided. Reliability studies mainly focus on service continuity and resource management, while security studies focus on confidentiality, authentication, access control, privacy, trust, and intrusion detection. The integration of reliability constraints with behaviour-aware data-theft prevention remains limited. This gap is important because security mechanisms in fog computing must work effectively despite limitations in latency, resources, mobility, and service continuity.

Figure 3 illustrates the evolution of fog-computing research from its early foundations in 2012–2016 to more adaptive and intelligent security approaches during 2022–2025. The first phase focuses mainly on establishing fog computing as a distributed computing paradigm, with emphasis on reducing latency, task offloading, and efficient use of computing and network resources. During 2017–2021, research expanded toward IoT applications and placed greater emphasis on security, reliability, fault tolerance, trust, and authentication. From 2022 onward, increasing

attention has been given to continuous monitoring, machine-learning-based anomaly detection, dynamic trust evaluation, and adaptive security.

The figure also highlights the identified research gap emerging from this evolution. Although behaviour profiling, trust management, anomaly detection, and deception have been investigated individually, their integration remains limited. The identified future direction is therefore to combine behaviour profiling, dynamic trust evaluation, anomaly detection, and adaptive deception into a lightweight and reliability-aware security framework capable of responding to suspicious data-access and potential data-theft activities in fog environments.

Security Threat Landscape and Insider Dynamics (RQ3 & RQ4)

Fog computing faces several security risks because of its distributed architecture, heterogeneous devices, limited resources, and exposure to physical environments [9–12,31]. Common threats include unauthorized access, eavesdropping, man-in-the-middle attacks, denial-of-service, node compromise, privacy violations, and malicious entities [9–12].

Traditional security measures such as authentication, authorization, access control, encryption, privacy protection, and trust management remain essential for securing fog environments [9–12,16,17,23,25–28]. However, these measures may be less effective when an attacker uses valid credentials or compromises a trusted entity. This issue is particularly important for insider-driven data theft. Stolfo et al. highlighted that an insider may misuse legitimate access to obtain sensitive information without causing an obvious service disruption [13]. Chen et al. also showed that unusual behavioural patterns can help identify potentially malicious insiders [14]. Thus, having valid authorization does not always mean that the access is legitimate.

The key difference is that external attackers often try to bypass security controls, whereas insiders or compromised entities can operate within existing security boundaries. This creates a post-authentication security problem that cannot be adequately addressed through identity and static authorization alone [13,14,25]. Therefore, fog security needs to move beyond asking “Who is authorized?” and also consider “Is the current behaviour legitimate?” This provides the basis for behaviour-based monitoring and adaptive security mechanisms. The key difference between external attacks and insider or compromised-entity attacks is their position relative to existing security controls. This distinction is illustrated in **Figure 4**.

COMPARATIVE THREAT CHARACTERISTICS: OUTSIDER VS. INSIDER		
Operational Parameter	External Network Threat	Malicious / Compromised Insider
 System Entry Point	 External Gateway	 Authorized Fog Node
 Authentication State	 Unauthenticated	 Authenticated (Valid Keys)
 Primary Target	 Perimeter Access	 Confidential Data Stores
 Encryption Status	 Blocked by TLS / IPsec	 Bypasses Decryption Layer
 Detection Method	 Network Firewalls / IDS	 User Behavior Analytics

Figure 4. Comparative Analysis of External and Insider Data-Security Threats

Behaviour Analytics and Anomaly Detection (RQ4 and RQ5)

Behaviour-based security provides an additional layer of analysis by examining activity patterns rather than relying exclusively on identity and predefined access privileges. The reviewed literature demonstrates the relevance of behavioural information for detecting anomalous insider activity and distributed attacks [13–15]. Behavioural

characteristics may include access frequency, request patterns, resource usage, temporal activity, and other observable interactions with system resources.

Chen et al. demonstrated the use of behavioural characteristics for identifying anomalous insiders in collaborative information systems [14]. In fog-related environments, machine-learning and deep-learning approaches have subsequently been investigated for distributed attack detection and intrusion detection [15,29,30]. These approaches indicate that behavioural and activity-related information can complement conventional authentication and access-control mechanisms by identifying deviations from expected operational patterns.

However, anomaly detection and behaviour analytics primarily provide a detection capability. Detection alone does not necessarily determine how the system should respond when suspicious activity is identified. In particular, the reviewed literature provides limited evidence of mechanisms that use behavioural deviations to dynamically determine whether a suspicious entity should receive normal data, restricted access, synthetic information, or a specifically selected decoy resource.

This distinction is important for data-theft prevention. A security architecture that only detects anomalous behaviour may identify a potential threat after sensitive information has already been accessed. A more proactive architecture could use behavioural evidence to modify subsequent interactions with the suspicious entity and thereby reduce the probability or value of successful data exfiltration.

Trust Management and Adaptive Security (RQ5)

Trust management provides a complementary mechanism for representing the confidence associated with users, devices, nodes, or services. Fog-oriented trust models have investigated direct and indirect trust information, behavioural observations, interaction history, and other factors to support security-related decisions [16,17,26–28].

Soleymani et al. proposed trust-based mechanisms for fog-enabled vehicular environments, demonstrating how trust information can contribute to secure communication and node-related decisions [16,17]. More general fog trust-management research has subsequently examined dynamic approaches for evaluating and updating trust among fog entities [26–28]. These studies demonstrate that trust can provide a dynamic security signal that complements static identity-based authorization.

Nevertheless, trust management and behaviour analytics are not equivalent. Behaviour analytics primarily observes and classifies activity, whereas trust management aggregates evidence into a representation of confidence or reliability. Their combination therefore provides an opportunity for more context-sensitive security decisions. For example, repeated anomalous access behaviour could contribute to a reduction in the trust associated with an entity, which could subsequently influence access privileges or security responses.

The reviewed literature, however, provides limited evidence of trust scores being directly coupled with data-specific deception decisions. In particular, few approaches establish a complete decision chain in which observed behaviour influences anomaly detection, anomaly evidence updates trust, and the resulting trust state determines the type, content, placement, or activation of a decoy resource.

Deception and Decoy-Based Data-Theft Protection (RQ5)

Deception mechanisms provide a different security strategy from conventional preventive controls. Instead of attempting only to block an attacker, deception can introduce misleading or synthetic resources that increase attacker uncertainty, generate detection signals, or reduce the value of compromised information [13,18,19].

Stolfo et al. proposed the use of decoy information to mitigate insider data theft, establishing an important connection between data-exfiltration threats and deception-based protection in distributed computing environments [13]. Voris et al. subsequently investigated the design of decoy documents to make deceptive information more plausible and useful for detecting and misleading malicious users [18]. Pawlick et al. provided a broader taxonomy of defensive deception and demonstrated that deception can be viewed as a strategic cybersecurity mechanism rather than simply as a static honeypot technique [19].

The evidence therefore suggests that decoy-based mechanisms can provide three complementary benefits: detection, by generating signals when suspicious entities interact with decoys; delay or diversion, by directing attackers away from genuine information; and misinformation, by reducing the value of information obtained by an attacker [13,18,19].

However, a major limitation identified from the reviewed literature is that deception mechanisms are frequently designed independently of continuous behaviour assessment and dynamic trust evaluation. Predefined decoy resources may not account for differences in attacker behaviour, user context, sensitivity of requested data, fog-node capabilities, or current system conditions. Consequently, the effectiveness of a decoy may vary according to the context in which it is deployed.

This limitation is particularly significant in fog environments, where resource and latency constraints restrict the feasibility of continuously deploying computationally expensive security mechanisms. An adaptive deception mechanism should therefore consider not only the likelihood of malicious activity but also the current operational state of the fog environment.

4. Integrated Evidence and Research Gap

The cross-study comparison reveals that the major research components required for adaptive data-theft prevention already exist in the literature, but they are predominantly distributed across separate research streams. Reliability studies address availability, resilience, resource management, and recovery [6–8,21,22]. Security studies provide authentication, authorization, access control, encryption, privacy, and trust mechanisms [9–12,23,25–28]. Insider-threat and anomaly-detection studies demonstrate the value of behavioural evidence for identifying suspicious activity [13–15,29,30]. Deception research provides mechanisms for detecting, misleading, and diverting attackers through decoy resources [13,18,19]. The cross-study comparison shows that the major components required for adaptive data-theft prevention are present in the literature, but they are mainly addressed in separate research streams. The extent to which each evidence stream, addresses reliability, behaviour analytics, anomaly detection, dynamic trust, data-theft protection, deception, adaptive response, and fog-specific constraints is summarized in **Table 4**.

Table 4. Evidence-based integration and research-gap matrix

Evidence stream	Reliability	Behaviour Analytics	Anomaly Detection	Dynamic Trust	Data-Theft Protection	Deception	Adaptive Response	Fog Constraints
Reliability/resilience studies [6–8,21,22]	✓	✗	✗	✗	✗	✗	●	✓
Conventional security studies [9–12,23,25,31–34]	●	●	✓	✓	●	●	●	✓
Insider-threat studies [13,14]	●	✓	✓	✗	✓	✓	●	●
ML/IDS studies [15,29,30]	●	✓	✓	●	●	✗	✓	✓
Trust-management	●	✓	●	✓	●	✗	✓	✓

studies [16,17,26–28]								
Deception studies [18,19]	✗	◐	◐	✗	✓	✓	✓	◐
Integrated evidence identified	◐	◐	◐	◐	◐	◐	◐	◐

✓ = explicitly/substantively addressed; ◐ = partially or indirectly addressed; ✗ = not addressed.

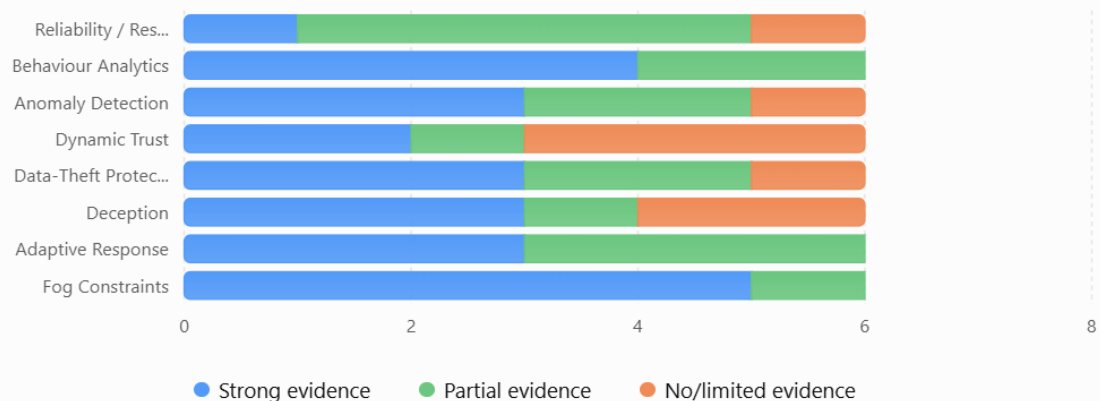
The matrix indicates that the literature provides substantial evidence for individual components but limited evidence of their integration into a single fog-specific data-theft prevention framework. In particular, behaviour analytics and anomaly detection are primarily used for identifying suspicious activity; trust mechanisms are primarily used for evaluating entities or interactions; and deception mechanisms are generally investigated as independent defensive strategies. The explicit coupling of these mechanisms for adaptive data-theft prevention remains comparatively underdeveloped.

A second gap concerns the interaction between security adaptation and fog reliability. Existing approaches frequently evaluate security effectiveness through detection accuracy, authentication performance, or attack-detection capability, while comparatively less attention is given to the combined effects of adaptive security decisions on computational overhead, latency, resource consumption, availability, and service reliability.

Accordingly, the evidence supports a research direction in which continuous behaviour profiling provides behavioural evidence, anomaly detection identifies deviations from expected activity, dynamic trust evaluation converts accumulated evidence into an updated security state, and context-aware deception determines an appropriate response to suspicious data-access activity. Such a framework should additionally consider fog-specific resource, latency, scalability, availability, and reliability constraints.

The cross-study comparison shows that the reviewed literature covers the major security components to different degrees. The evidence coverage across reliability, behaviour analytics, anomaly detection, dynamic trust, data-theft protection, deception, adaptive response, and fog constraints is presented in Figure 5.

Aggregated evidence coverage across the representative research streams. Complete evidence = 2, partial evidence = 1, and no or limited evidence = 0.



Higher total scores indicate broader evidence coverage across the reviewed literature.

Figure 5. Evidence Coverage Across Key Security Dimensions

5. Critical Synthesis of Research Gaps

The systematic synthesis of the reviewed literature reveals five interconnected research gaps concerning the reliability and security of fog-computing environments. These gaps emerge from the comparison of conventional security mechanisms, reliability approaches, insider-threat detection, behaviour analytics, trust management, anomaly detection, and deception-based mechanisms. The comparison of existing studies indicates that the main research gap is not the absence of individual security techniques, but their limited integration into a reliability-aware and adaptive data-theft prevention approach. The identified research gap and the proposed integration direction are summarized in **Figure 6**.

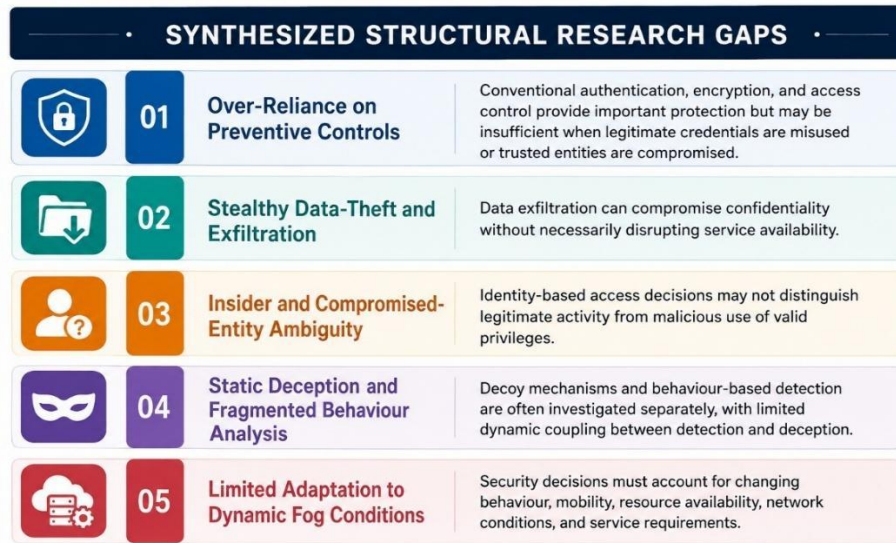


Figure 6. Synthesized Research Gap and Proposed Integration Direction

Existing fog-security research predominantly emphasizes authentication, access control, encryption, privacy, and trust mechanisms [9–12,23,25–28]. These mechanisms establish essential security boundaries but may provide limited protection when valid credentials are misused or trusted fog entities are compromised [13,25,26]. This creates a need for security mechanisms that evaluate behaviour after authentication, rather than relying exclusively on identity and authorization.

Insider-threat research demonstrates that sensitive information can be accessed and exfiltrated without necessarily disrupting service availability [13,14]. Behaviour-based anomaly detection can identify suspicious access patterns [14,15,29,30], but detection does not inherently prevent subsequent access to genuine data. Thus, an important gap exists between detecting suspicious behaviour and actively protecting data from subsequent exfiltration.

Behaviour analytics, trust management, and deception have each been investigated in fog and related computing environments [13–19,26–30]. However, they generally operate as separate security capabilities. Behaviour analysis identifies deviations, trust mechanisms assess entity credibility, and deception mechanisms provide misleading resources. Limited evidence exists of a closed-loop mechanism in which behavioural evidence → anomaly assessment → trust update → adaptive deception forms a continuous security process.

Fog environments experience changing workloads, mobility, resource availability, connectivity, and node conditions [6–8,21,22]. Although dynamic trust and intelligent intrusion-detection approaches have been investigated [16,17,26–34], security responses are not consistently adapted simultaneously to threat behaviour and fog-system conditions. This limits the applicability of computationally intensive or static security mechanisms in resource-constrained environments.

Reliability and security are commonly evaluated as separate research dimensions. Reliability-oriented studies focus on resilience, resource management, availability, and recovery [6–8,21,22], whereas security studies primarily evaluate protection and detection effectiveness [9–12,29–34]. Consequently, limited evidence exists for adaptive security mechanisms that explicitly evaluate their effects on latency, computational overhead, resource consumption, scalability, availability, and overall fog-service reliability.

6. Illustrative Healthcare Case Study

A fog-based healthcare environment can be used to demonstrate the practical application of the security mechanisms identified in this review. Patient data generated by wearable devices, medical IoT devices, monitoring applications, and EHR terminals are first processed at a hospital fog node before being forwarded to the cloud [24]. As shown in **Figure 7**, the fog node monitors user and device behaviour and uses anomaly detection and dynamic trust evaluation to assess each access request [14–17]. Normal requests are provided with genuine patient data, while unusual or high-risk requests can trigger an adaptive deception mechanism that provides decoy data, honeyfiles, or decoy documents instead [13,18,19]. Suspicious activities are logged and reported to the security team. This scenario shows how **behaviour monitoring, anomaly detection, dynamic trust, and deception** can work together to reduce the risk of post-authentication data theft while maintaining low latency, resource efficiency, availability, and service continuity [6–8].

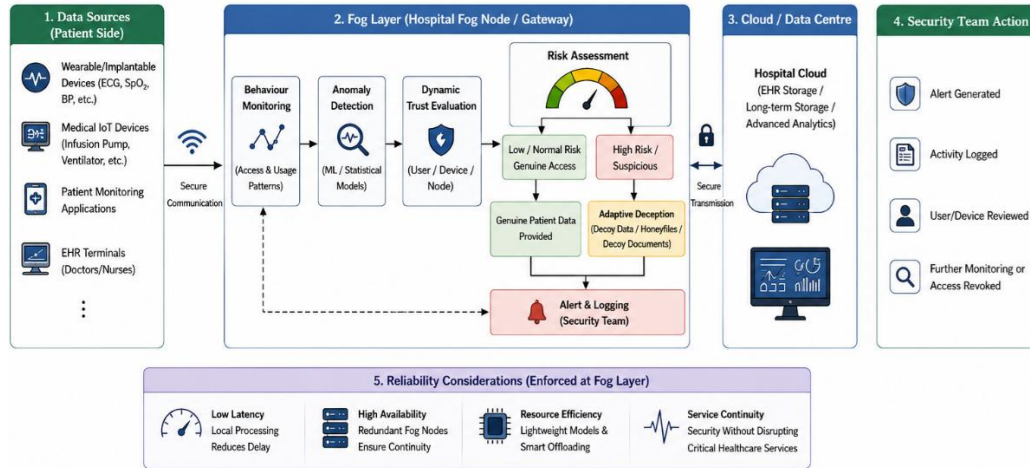


Figure 7. Illustrative Behaviour-Aware and Deception-Based Framework for Data-Theft Prevention in Fog-Based Healthcare

Note: This case study is conceptual and is based on findings from the reviewed literature. It does not represent an experimentally validated or real-world hospital deployment.

The Principal Knowledge Gap

The evidence therefore indicates that the primary gap is not the absence of individual security techniques but their limited integration into a reliability-aware, adaptive data-theft prevention framework.

Existing studies provide the individual building blocks:

Behaviour profiling → [13–15]

Anomaly detection → [15,29,30]

Trust management → [16,17,26–28]

Deception/decoy mechanisms → [13,18,19]

Reliability and resilience → [6–8,21,22]

Based on the reviewed literature, the major research gaps can be summarized into five points:

1. Limitations of traditional security:

Authentication, encryption, and access control may not be sufficient when valid credentials are misused or trusted fog nodes are compromised.

2. Insufficient protection against stealthy data theft:

Existing approaches often focus on unauthorized access or service disruption, while data can be quietly accessed and exfiltrated without affecting normal services.

3. Limited integration of behaviour, anomaly detection, and trust:

User and node behaviour, anomaly detection, and trust management are often studied separately rather than being combined into a continuous security process.

4. Static and limited use of deception:

Many decoy-based approaches use predefined resources and are not dynamically selected according to user behaviour, trust level, threat conditions, or fog-system state.

5. Lack of a reliability-aware adaptive framework:

There is limited research on an integrated, lightweight framework that combines behaviour monitoring, anomaly detection, dynamic trust evaluation, and adaptive decoy selection while maintaining low latency, efficient resource usage, scalability, availability, and overall fog-system reliability.

7. Limitations and Threats to Validity

Evaluating potential threats to validity ensures transparency and rigor in systematic literature reviews:

- **Construct Validity:** Search queries may omit relevant studies using alternate terminology. To minimize this risk, keyword combinations were tested across multiple iterations and validated against known benchmark publications [35].
- **Internal Validity:** Selection bias may influence study inclusion. This risk was minimized by applying predefined inclusion and exclusion criteria consistently throughout the screening and study-selection process.
- **External Validity:** Fog computing encompasses diverse application domains, including smart cities, healthcare, and industrial IoT. The findings of this review reflect general architectural principles, but specific hardware constraints may alter deployment requirements.
- **Database Indexing Constraints:** Studies were selected only if indexed in established scientific databases and verified on Google Scholar. The review focused primarily on peer-reviewed journal articles and full-length conference papers identified through the selected databases and supplementary searches. Unindexed technical reports and non-English publications were excluded.
- **Temporal Limitation:** The review covers publications from 2012 to 2025. Research developments published after 2025 are therefore outside the defined evidence base.

8. Future Research Directions and Strategic Roadmap

The findings of this review show that future research should focus on bringing different security mechanisms together rather than studying them separately. Four important directions are identified.

1. Lightweight Behaviour Monitoring

Future work should focus on developing lightweight methods for continuously monitoring the behaviour of users, devices, and fog nodes. Machine-learning techniques can be used to identify unusual access or usage patterns, but they should require limited processing power, memory, energy, and communication. Their effect on latency and overall fog-system performance should also be carefully evaluated.

2. Dynamic and Context-Aware Decoys

Future research should move beyond fixed or predefined decoy files and resources. Decoys should be selected or generated according to the situation, such as the type of data being requested, the behaviour of the user, the level of trust, the detected threat, and the current condition of the fog node. This can make deception more useful for detecting and slowing down potential data theft.

3. Integration of Behaviour, Trust and Deception

An important research direction is to connect behaviour monitoring, anomaly detection, trust evaluation, and deception. For example, unusual behaviour could first increase the anomaly level of a user or node. This evidence could then reduce its trust level and trigger an appropriate response, such as additional monitoring, restricted access, or delivery of decoy data. Such a continuous process could provide better protection against users or nodes that misuse legitimate access.

4. Reliability-Aware Fog Security

Future security solutions should also consider the reliability of fog nodes and the availability of resources. A compromised, overloaded, or failed node should not be able to affect the entire security process. Therefore, future research should investigate fault-tolerant and distributed approaches for maintaining behaviour information, trust decisions, and security policies. These approaches should be designed carefully so that additional security does not create excessive computational or communication overhead.

9. Conclusion

Fog computing brings computing and storage closer to IoT devices, which can reduce latency and network traffic. At the same time, its distributed and resource-constrained nature creates important reliability and security challenges.

The literature reviewed in this study shows that authentication, access control, encryption, privacy protection, trust management, anomaly detection, and deception have all been studied in fog and related computing environments. These mechanisms provide important protection, but they are generally investigated separately. In particular, conventional security mechanisms may provide limited protection when an insider or a compromised fog node uses legitimate credentials to access sensitive information [9–14,23,25].

Behaviour-based approaches can help identify unusual activities [14,15,29,30], while trust-management techniques can provide information about the reliability of users, devices, and fog nodes [16,17,26–28]. Decoy-based approaches can further help detect and mislead attackers [13,18,19]. However, there is limited evidence of a single fog-specific framework that combines these capabilities for preventing stealthy data theft. The main research gap identified by this review is therefore the lack of an integrated, lightweight, and adaptive approach that connects behaviour monitoring, anomaly detection, trust evaluation, and decoy-based protection while maintaining fog-system reliability and performance.

Future research should focus on developing such integrated approaches and evaluating them under realistic fog conditions. Particular attention should be given to latency, resource consumption, scalability, availability, computational overhead, and service reliability, in addition to security effectiveness.

Overall, the review suggests that future fog-security systems should move from isolated and mainly preventive mechanisms toward continuous, behaviour-aware, trust-informed, and adaptive protection. Such an approach can

provide an additional layer of defense against insider and compromised-entity data theft while maintaining the performance and reliability expected from fog-computing environments.

10. Declarations & Compliance

- Funding: No specific external grant supported this systematic literature review.
- Conflict of Interest: The authors declare no conflicts of interest.
- Data Availability Statement: No new data were created or analyzed in this study.

REFERENCES

1. Bonomi F, Milito R, Zhu J, Addepalli S. Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing. New York: ACM; 2012. p. 13-16. doi:10.1145/2342509.2342513.
2. Yi S, Li C, Li Q. A survey of fog computing: concepts, applications and issues. In: Proceedings of the 2015 Workshop on Mobile Big Data. New York: ACM; 2015. p. 37-42. doi:10.1145/2757384.2757397.
3. Chiang M, Zhang T. Fog and IoT: an overview of research opportunities. IEEE Internet Things J. 2016;3(6):854-864. doi:10.1109/JIOT.2016.2584538.
4. Luan TH, Gao L, Li Z, Xiang Y, Wei G, Sun L. Fog computing: focusing on mobile users at the edge. arXiv. 2015;arXiv:1502.01815.
5. Mahmud R, Kutagiri R, Buyya R. Fog computing: a taxonomy, survey and future directions. In: Di Martino B, Li KC, Yang LT, Esposito A, editors. Internet of Everything. Singapore: Springer; 2018. p. 103-130. doi:10.1007/978-981-10-5861-5_5.
6. Shiriaev E, Ermakova T, Bezuglova E, Lapina MA, Babenko M. Reliability and Security for Fog Computing Systems. Information. 2024;15(6):317. doi:10.3390/info15060317.
7. Ghobaei-Arani M, Soury A, Rahmanian AA, et al. Resource management approaches in fog computing: a comprehensive review. J Grid Comput. 2020;18:1-42. doi:10.1007/S10723-019-09491-1.
8. Moura JA, Hutchison D. Fog computing systems: state of the art, research issues and future trends, with a focus on resilience. J Netw Comput Appl. 2020;169:102784. doi:10.1016/j.jnca.2020.102784.
9. Alrawais A, Alhothaily A, Hu C, Cheng X. Fog computing for the internet of things: security and privacy issues. IEEE Internet Comput. 2017;21(2):34-42. doi:10.1109/MIC.2017.37.
10. Ni J, Zhang K, Lin X, Shen XS. Securing fog computing for internet of things applications: challenges and solutions. IEEE Commun Surv Tutor. 2018;20(1):601-628. doi:10.1109/COMST.2017.2762345.
11. Mukherjee M, Matam R, Shu L, Maglaras L, Ferrag MA, Choudhury N, Kumar V. Security and privacy in fog computing: challenges, solutions, and future directions. IEEE Access. 2017;5:19293-19304. doi:10.1109/ACCESS.2017.2749422.
12. Roman R, Lopez J, Mambo M. Mobile edge computing, Fog et al.: a survey and analysis of security threats and challenges. Future Gener Comput Syst. 2018;78:680-698. doi:10.1016/j.future.2016.11.009.
13. Stolfo SJ, Salem MB, Keromytis AD. Fog computing: mitigating insider data theft attacks in the cloud. In: 2012 IEEE Symposium on Security and Privacy Workshops. IEEE; 2012. p. 125-128. doi:10.1109/SPW.2012.23.
14. Chen Y, Nyemba S, Malin B. Detecting anomalous insiders in collaborative information systems. IEEE Trans Dependable Secure Comput. 2012;9(3):332-344. doi:10.1109/TDSC.2012.11.
15. Diro AA, Chilamkurti N. Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Commun Mag. 2018;56(2):169-175. doi:10.1109/MCOM.2018.1700332.
16. Soleymani SA, Abdullah AH, Zareei M, Anisi MH, Vargas-Rosales C, Khan MK, Goudarzi S. A secure trust model based on fuzzy logic in vehicular ad hoc networks with fog computing. IEEE Access. 2017;5:15619-15629. doi:10.1109/ACCESS.2017.2733225.
17. Soleymani SA, Goudarzi S, Anisi MH, Zareei M, Abdullah AH, Kama N. A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. Veh Commun. 2021;29:100335. doi:10.1016/j.vehcom.2021.100335.
18. Voris J, Boggs N, Stolfo SJ. Lost in translation: improving decoy documents via automated translation. In: 2012 IEEE Symposium on Security and Privacy Workshops. IEEE; 2012. p. 129-133. doi:10.1109/SPW.2012.20.
19. Pawlick J, Colbert E, Zhu Q. A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. ACM Comput Surv. 2019;52(4):1-28. doi:10.1145/3337772.
20. Park D, Dagher GG. Adaptive honeypot allocation in multi-attacker networks via Bayesian Stackelberg games. Comput Secur. 2026;168:104949.
21. Singh J, Singh P, Gill SS. Fog computing: a taxonomy, systematic review, current trends and research challenges. J Parallel Distrib Comput. 2021;157:56-85. doi:10.1016/j.jpdc.2021.06.005.
22. Salem AH, Algaphari GH. Resource allocation in fog computing: a systematic review. J Sci Technol. 2023;27(2):9-31. doi:10.20428/jst.v27i2.2052.

23. Huang Q, Yang Y, Wang L. Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things. *IEEE Access*. 2017;5:12941-12950. doi:10.1109/ACCESS.2017.2727054.
24. Kraemer F, Braten AE, Tamkittikhun N, Palma D. Fog computing in healthcare—a review and discussion. *IEEE Access*. 2017;5:9206-9222. doi:10.1109/ACCESS.2017.2704100.
25. Zhang P, Zhou M, Fortino G. Security and trust issues in fog computing: a survey. *Future Gener Comput Syst*. 2018;88:16-27. doi:10.1016/j.future.2018.05.008.
26. Al-Khafajiy M, Baker T, Asim M, Guo Z, Ranjan R, Longo A, Puthal D, Taylor M. COMMITMENT: a fog computing trust management approach. *J Parallel Distrib Comput*. 2020;137:1-16. doi:10.1016/j.jpdc.2019.10.006.
27. Ogundoyin SO, Kamil IA. A trust management system for fog computing services. *Internet Things*. 2021;14:100382. doi:10.1016/j.iot.2021.100382.
28. Nikravan M, Haghi Kashani M. A review on trust management in fog/edge computing: techniques, trends, and challenges. *J Netw Comput Appl*. 2022;204:103402. doi:10.1016/j.jnca.2022.103402.
29. de Souza CA, Westphall CB, Machado RB, Loffi L, Westphall CM, Geronimo GA. Intrusion detection and prevention in fog based IoT environments: a systematic literature review. *Comput Netw*. 2022;214:109154. doi:10.1016/j.comnet.2022.109154.
30. Yi L, Yin M, Darbandi M. A deep and systematic review of the intrusion detection systems in the fog environment. *Trans Emerg Telecommun Technol*. 2023;34(1):e4632. doi:10.1002/ett.4632.
31. Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. *Sensors*. 2022;22(3):927. doi:10.3390/s22030927.
32. Sicari S, Rizzardi A, Coen-Porisini A. Insights into security and privacy towards fog computing evolution. *Comput Secur*. 2022;120:102822. doi:10.1016/j.cose.2022.102822.
33. Jumani AK, Shi J, Laghari AA, Hu Z, Nabi AU, Qian H. Fog computing security: a review. *Secur Priv*. 2023;6(6):e313. doi:10.1002/spy2.313.
34. Kaur N. A systematic review on security aspects of fog computing environment: challenges, solutions and future directions. *Comput Sci Rev*. 2024;54:100688. doi:10.1016/j.cosrev.2024.100688.