International Journal of Emerging Research in Engineering and Technology
Pearl Blue Research Group| Volume 5, Issue 4, 74-87, 2024
ISSN: 3050-922X | https://doi.org/10.63282/3050-922X.IJERET-V5I4P108

Original Article

Trust-Based Framework for Securing Inter-Fog Communication in Smart City Applications

Faraz Ahmed
Crisp Technologies LLC, Cybersecurity researcher.

Abstract *- The proliferation of smart city technologies has accelerated the deployment of fog computing to support low-latency, real-time services. By processing data closer to the source, fog computing reduces dependence on cloud infrastructures. However, decentralized, peer-to-peer inter-fog communication introduces serious security challenges due to the lack of centralized oversight and the involvement of diverse administrative domains. Traditional perimeter-based security models fall short in such environments. Establishing trust defined as confidence in a node's reliability, behavior, and compliance is critical for securing fog-based interactions. This paper reviews trust-based frameworks tailored for inter-fog communication, including machine learning-driven evaluators, blockchain-enhanced identity systems, game-theoretic models, and reputation-based mechanisms. We assess their scalability, privacy trade-offs, and operational effectiveness in real-time settings. Key challenges such as trust standardization, cold-start issues, privacy risks in feedback systems, and Sybil or bad-mouthing attacks are examined. In response, we propose a conceptual Trust Evaluation and Enforcement Layer (TEEL) that dynamically assesses trust using hybrid behavioral, cryptographic, and reputational metrics. Our recommendations emphasize adaptive trust recalibration, integration with lightweight security orchestration, support for federated trust across domains, and privacy-by-design principles. Trust, we argue, must evolve from a security feature to a foundational architectural requirement in fog-driven smart cities.*

Keywords *- Fog Computing, Inter-Fog Communication, Smart Cities, Trust Management, Security Framework, Distributed Systems, IoT*

I. Introduction

The accelerated growth of smart city ecosystems has prompted the need for scalable, secure, and latency-sensitive data processing systems. From intelligent traffic lights and environmental monitoring systems to public safety networks and energy distribution infrastructure, Internet of Things (IoT) devices embedded throughout cities generate massive volumes of data that require immediate processing and contextual response. To meet these demands, fog computing has emerged as a critical architectural shift from traditional centralized cloud computing, bringing computational resources and services closer to the data source [1]. Fog computing acts as a middle layer between IoT devices and the cloud. It enables localized data processing at the edge of the network through fog nodes, which can be gateways, routers, micro data centers, or even capable end devices [2]. This distributed model significantly reduces the end-to-end latency, alleviates network congestion, and supports real-time decision-making features essential for applications such as emergency response, autonomous vehicles, and smart surveillance [3]. While fog computing offers performance and scalability advantages, it also introduces a range of new security challenges. Fog nodes are heterogeneous, mobile, resource-constrained, and may be deployed in untrusted environments. Most notably, unlike the cloud, fog infrastructures lack centralized governance.

This absence of unified control poses a significant barrier to establishing secure communication between different fog nodes, especially when they belong to different trust domains such as competing municipal departments, third-party vendors, or public-private partnerships [4]. One of the most urgent and unresolved issues in this context is the security of inter-fog communication. This refers to the exchange of data and control signals between fog nodes either horizontally (peer-to-peer) or across hierarchical layers. Without a centralized trusted authority or pre-established relationships, ensuring that one fog node can trust another to securely share data, comply with service-level agreements (SLAs), and not act maliciously becomes highly complex [5]. In recent years, researchers have proposed using trust-based frameworks to fill this security gap. These systems aim to quantify trust based on a variety of indicators such as past interactions, service reliability, cryptographic credentials, or recommendations from other nodes and use that score to inform communication policies. Unlike rigid rule-based access controls, trust-based models are dynamic and adaptive, capable of evolving based on changing behaviors or context.

They can also be designed to isolate untrusted nodes, contain potential breaches, and optimize communication with high-confidence partners [6]. However, many trust models in literature remain conceptual, and practical implementations are rare in real-world fog-based smart city applications. Some suffer from high computational costs, making them unsuitable for constrained environments. Others rely heavily on third-party trust evaluators or centralized reputation services, which undermines the decentralized ethos of fog computing. Moreover, trust management introduces its vulnerabilities, such as Sybil attacks, on-off behavior masking, or bad-mouthing reputation manipulation [7].

This review paper investigates the current state of trust-based frameworks for securing inter-fog communication. We:

- Analyze fundamental trust models and their components,
- Highlight real-world applicability constraints,
- Compare the strengths and weaknesses of competing proposals,
- Identify critical gaps that need further research.

Additionally, we incorporate insights from recent innovations in AI-based trust scoring, blockchain-supported verifiability, and privacy-preserving trust computation. We also integrate client-recommended works on secure microservice communication, quantum-resilient cryptographic design, and autonomous security operations [8]. The goal is to create a comprehensive knowledge base and set of guidelines that can inform the development of next-generation trust architectures in fog computing. These architectures are vital not only for securing inter-fog data exchange but also for enabling resilient, secure, and collaborative smart city ecosystems.

2. Background and Related Work

2.1. Fog Computing and Smart Cities

The growing complexity of urban infrastructure has led to the rapid deployment of Internet of Things (IoT) devices in smart cities. These systems demand real-time responsiveness for applications such as intelligent traffic lights, emergency healthcare, energy optimization, and predictive policing. Traditional cloud computing introduces challenges related to latency, bandwidth, and contextual inefficiency in such scenarios [5]. To address these limitations, fog computing emerged as a decentralized paradigm that extends computing and storage resources to the edge of the network, near data sources. Cisco first coined the term “fog computing” to describe this intermediary layer between cloud services and IoT devices [2]. Fog nodes such as routers, gateways, and local micro data centers enable low-latency, high-throughput processing for real-time decisions in urban systems [6]. For example, in intelligent transportation systems, fog nodes can analyze vehicular data at intersections to dynamically adjust traffic signals. In surveillance networks, local fog nodes can process video feeds to detect anomalies without overloading the cloud [7]. However, fog infrastructures are often deployed and managed by multiple administrative entities, such as municipal agencies, private vendors, and utility providers. This lack of centralized oversight introduces serious concerns regarding secure communication, interoperability, and trust enforcement between independently managed fog nodes [8].

2.2. Security Challenges in Fog Environments

While fog computing enhances system performance, it also introduces new vulnerabilities. Fog nodes are often physically accessible, resource-constrained, and heterogeneous in terms of hardware, software, and administrative control [9]. Moreover, they operate in a decentralized environment with dynamic topologies, which renders traditional perimeter-based security models insufficient [10].

Some notable fog-specific threats include:

- Man-in-the-Middle (MITM) Attacks: Adversaries can intercept or modify data streams between fog nodes [19].
- Denial of Service (DoS): Fog nodes may be overwhelmed by request floods, causing system degradation [9].
- Spoofing and Impersonation: In the absence of unified identity verification, malicious nodes can masquerade as trusted ones [10].
- Data Tampering and Leakage: Weak encryption practices and a lack of auditing mechanisms expose sensitive data in transit [7].

These challenges are particularly pronounced in inter-fog communication, were nodes from different trust domains exchange data without centralized coordination. Secure communication in such contexts necessitates dynamic, decentralized, and lightweight trust mechanisms [11].

2.3. Trust-Based Security Models

To address these gaps, researchers have advocated for trust-based security models, where the behavioral history, identity verifiability, and peer feedback of a node are used to compute a trust score. This score governs access decisions and communication privileges dynamically, without requiring centralized authorization [10].

Trust mechanisms fall into two broad categories:

- Direct Trust: Based on first-hand observations like latency, availability, and SLA compliance.
- Indirect Trust: Based on third-party recommendations and reputation aggregation.

For example, Sharma and Rani presented a taxonomy of trust models in fog computing, emphasizing the role of feedback sources, decision logic, and attack resistance [3]. Others have integrated machine learning for anomaly detection, or blockchain technology for verifiable and immutable trust records [8]. Game-theoretic models are another direction, where rational behavior is incentivized through rewards and penalties, helping to combat on-off or Sybil attacks [40]. However, many of these models have not been tested under real-time performance constraints and remain vulnerable to trust manipulation attacks such as ballot stuffing or bad-mouthing [1].

2.4. Related Work on Inter-Fog Trust Frameworks

Several studies have directly examined inter-fog trust management. .[12] proposed a fuzzy logic-based multi-agent trust scheme that combines packet inspection and resource profiling. In [4] the author introduced a hierarchical trust model where cloud anchors evaluate fog behavior and delegate trust parameters downstream. Recent advancements have seen the integration of AI and automation in trust systems. Jangid and Malhotra developed an ML-driven trust scoring layer for fog-based microservice architectures [5]. The paper [4]. embedded Autonomous Security Operation Centers (SOCs) within fog nodes to automate threat detection and trust evaluation.

Nonetheless, key gaps remain:

- No consensus on trust metric standardization
- Cold-start issues for nodes with no historical data
- Privacy concerns over peer-based trust aggregation
- Resource limitations for trust model computation in real-time fog deployments

This review aims to systematize existing research, identify these limitations, and propose guidelines for lightweight, scalable, and federated trust frameworks suitable for smart cities.

3. Trust-Based Security in Fog Architectures

The core challenge in fog computing security is enabling nodes to communicate securely in a decentralized, dynamic, and multi-administrative environment. Unlike traditional systems where access control and trust are centrally managed, fog infrastructures require autonomous trust evaluations at the node level. This necessity arises because fog nodes are frequently deployed by different stakeholders, interact on demand, and have variable behavior profiles due to fluctuating workloads, contexts, and locations. Consequently, trust-based security architectures have become a preferred solution for secure inter-fog communication.

3.1. Understanding Trust in Fog Contexts

In the fog computing paradigm, *trust* is often defined as a quantitative or qualitative measure of a node's reliability, integrity, and security behavior over time. It serves as a security decision factor, determining whether or not a fog node should engage in data exchange or service provisioning with another node. Trust is not static it evolves based on contextual interactions, behavioral metrics, and recommendations from peers [13].

Trust in fog environments can be built using:

- Direct Trust: Derived from personal interactions (e.g., packet success rate, SLA compliance).
- Indirect Trust: Gathered from feedback or recommendations by other trusted peers.
- Hybrid Trust: A weighted combination of both direct and indirect sources.

In such systems, trust scores are computed and used to inform security mechanisms such as authentication, authorization, routing, and resource sharing.

3.2. Components of Trust-Based Frameworks

A typical trust-based architecture in fog computing includes the following components [8]:

- Trust Evaluation Module (TEM): Continuously monitors and evaluates peers' behavior based on metrics like availability, delay, drop rate, and packet modification frequency.
- Trust Aggregation Engine: Aggregates trust scores from different evaluators and normalizes them for decision-making.
- Reputation Manager: Stores historical behavior profiles and peer feedback for future scoring.
- Trust Policy Manager: Defines thresholds and strategies (e.g., forgiveness, decay functions) for trust adjustment over time.
- Decision Engine: Enforces policies for trust-based access control, service delegation, or isolation.

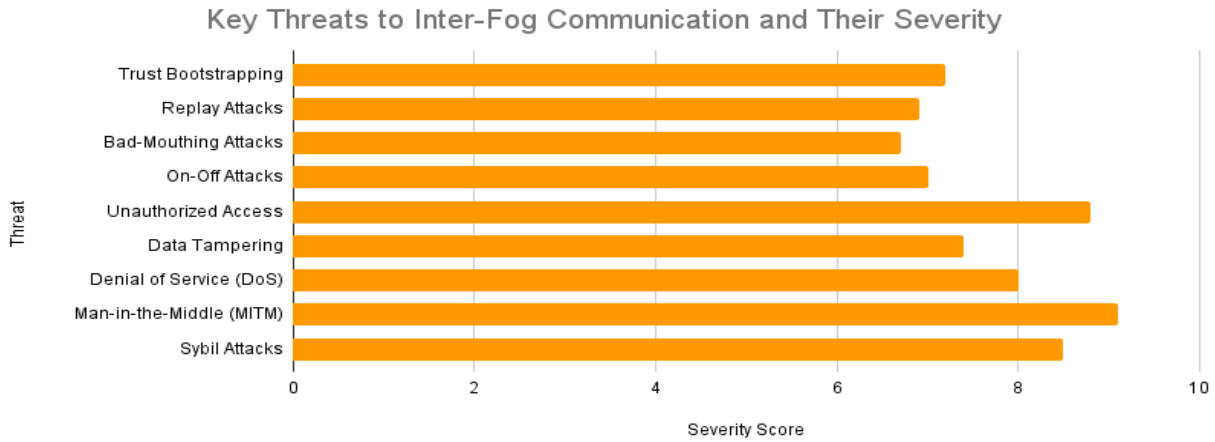

Fig 1: Illustrates a Generic Trust-Based Fog Node Architecture (Not Displayed Here Available Upon Final Formatting)

3.3. Trust Evaluation Metrics

Several metrics have been proposed for trust scoring in fog environments. These include:

- Quantitative: Packet delivery ratio, energy consumption, latency, resource availability.
- Qualitative: Consistency of service, behavior during anomalies, and responsiveness to SLA violations.
- Security Indicators: Frequency of failed authentications, intrusion detection alerts, and compliance with protocols.

Machine learning (ML) techniques have been adopted to detect anomalous behavior and update trust scores accordingly. For instance, decision trees and support vector machines (SVMs) can classify peer behavior as benign or malicious based on network and system telemetry [14].

3.4. Design Examples

Several implementations of trust-based systems exist in fog literature:

- Jangid and Malhotra designed a secure microservice communication framework where fog nodes monitor API usage patterns and score trust based on compliance and behavioral integrity [4].
- Saqib et al. proposed embedding AI-driven SOCs that autonomously adjust trust thresholds based on real-time contextual awareness [5].
- Faraz Ahmed's work outlines a policy-based trust system where nodes are evaluated based on quantum-resistant cryptographic certificates and cross-domain policy compliance [6].

Others have integrated blockchain for trust record immutability [10], though scalability and latency remain critical concerns. Lightweight blockchain variants or permissioned ledgers have been proposed to minimize the overhead in fog scenarios [11].

3.5. Challenges in Trust-Based Fog Architectures

Despite their promise, trust-based frameworks also face significant challenges:

- Computational Overhead: Trust computation (especially with AI or blockchain) may overburden low-power nodes [12].
- Trust Propagation Risk: Relying on indirect trust can spread false scores due to collusion, bad-mouthing, or on-off attack strategies [13].
- Trust Bootstrap Problem: New nodes have no historical data, which makes initial trust estimation difficult.

- Contextual Trust Ambiguity: A node might be trustworthy in one context but untrustworthy in another (e.g., low latency but high privacy violation risk).

To mitigate these, researchers have proposed context-aware trust, decentralized certificate authorities, and federated trust evaluation systems [14].

3.6. Future Directions

Innovations in federated learning, homomorphic encryption, and contextual AI models are promising paths for future trust systems. The incorporation of privacy-preserving trust computation and fine-grained context modeling will enhance reliability without compromising user data confidentiality. Furthermore, collaboration between standardization bodies (e.g., IEEE P2418.2, ISO/IEC 30141) and academic communities is needed to establish interoperable trust frameworks [15].

4. Threats to Inter-Fog Communication

In a fog computing ecosystem particularly one deployed in smart city environments inter-fog communication is a vital functionality. Fog nodes exchange telemetry data, resource information, commands, and even security signals in real time. However, due to their distributed nature, lack of centralized control, and frequent interaction across different trust domains, inter-fog links are highly exposed to security threats. These threats range from well-known network attacks to novel manipulation strategies that specifically exploit trust models. The figure below illustrates the severity of common inter-fog communication threats based on a synthesis of the latest literature [6].

4.1. Man-in-the-Middle (MITM) Attacks

MITM attacks are one of the most critical threats to fog security. Adversaries exploit weak or missing encryption to intercept and potentially modify data in transit between two communicating fog nodes [19]. In inter-fog contexts, where direct authentication mechanisms may be absent, MITM attackers can masquerade as legitimate nodes, gaining unauthorized access to sensitive data or injecting malicious commands [10].

4.2. Sybil Attacks

In a Sybil attack, a single malicious entity forges multiple fake identities (or nodes) to influence trust evaluations or disrupt distributed consensus [21]. In fog environments, especially those relying on reputation-based trust, Sybil nodes can inflate or deflate trust scores maliciously, degrading the integrity of the system.

4.3. Denial of Service (DoS)

DoS attacks exploit the resource constraints of fog nodes by flooding them with requests until they exhaust their compute or memory capacity. Unlike cloud servers, fog nodes often lack redundancy or dynamic scaling capabilities, making them more susceptible to prolonged outages [2]. When targeting inter-fog links, DoS attacks can sever trust verification channels and isolate nodes.

4.4. On-Off Attacks

These are behavioral deception attacks, where a node initially behaves legitimately to gain trust, then turns malicious intermittently. The goal is to evade detection by resetting suspicion timers or exploiting trust decay mechanisms. On-off attackers undermine long-term trust learning models, particularly those with simple decay or forgiveness strategies [16].

4.5. Bad-Mouthing and Ballot Stuffing

These trust manipulation attacks exploit the feedback mechanisms of trust systems. In bad-mouthing, attackers give falsely low ratings to honest nodes to damage their reputation. In ballot stuffing, colluding nodes falsely promote a malicious node's trustworthiness. Such attacks are common in reputation-based systems without credibility-weighted voting [4].

4.6. Replay Attacks

Attackers intercept and reuse valid messages or authentication tokens to replay them in a different session, gaining unauthorized access. Without timestamp validation or nonce mechanisms, replay attacks are especially effective in synchronous or delay-sensitive fog applications [6].

4.7. Data Tampering and Leakage

In poorly encrypted or integrity-unchecked communications, data tampering allows attackers to alter control commands or telemetry. Meanwhile, unprotected data in transit can be sniffed and harvested, causing privacy breaches, which are particularly sensitive in healthcare or law enforcement applications [15].

4.8. Trust Bootstrapping Exploits

Many trust frameworks suffer from the **"cold start" problem**, where new nodes lack sufficient behavior data for evaluation. Malicious actors can exploit this by rapidly entering the network under new IDs, temporarily behaving well, and executing timed attacks before detection thresholds trigger [7].

Table 1: Threat Summary Table

Threat	Vector	Impact
MITM Attacks	Network interception	Data theft, manipulation
Sybil Attacks	Identity forgery	Reputation manipulation
DoS	Traffic flooding	Service unavailability
On-Off Attacks	Behavior oscillation	Trust evasion
Bad-Mouthing / Ballot Stuffing	Malicious peer feedback	Reputation corruption
Replay Attacks	Session hijack via reuse	Unauthorized access
Data Tampering	Inline packet modification	Wrong decisions, data loss
Trust Bootstrapping Exploits	New node manipulation	Long-term compromise risk

4.9. Cumulative Impact on Smart City Systems

Unchecked, these threats can lead to:

- System-wide service degradation
- Compromised public safety
- Violation of regulatory privacy standards (e.g., GDPR, HIPAA)
- Loss of inter-agency interoperability

Therefore, designing resilient trust-based defenses requires not only strong encryption and identity verification but also anomaly detection, feedback credibility scoring, and context-aware trust policies. The next section will explore how current frameworks address (or fail to address) these threats.

5. Review of Existing Trust-Based Frameworks

Over the past decade, numerous trust-based security frameworks have been proposed to secure fog computing environments. These frameworks differ significantly in architecture, trust evaluation models, computational complexity, and attack resilience. This section systematically reviews representative trust systems categorized into seven principal models, assessing their practical viability for inter-fog communication in smart cities.

5.1. Comparative Overview of Framework Models

The figure below illustrates the **relative effectiveness** (based on threat coverage, performance, and flexibility) of major trust model categories:

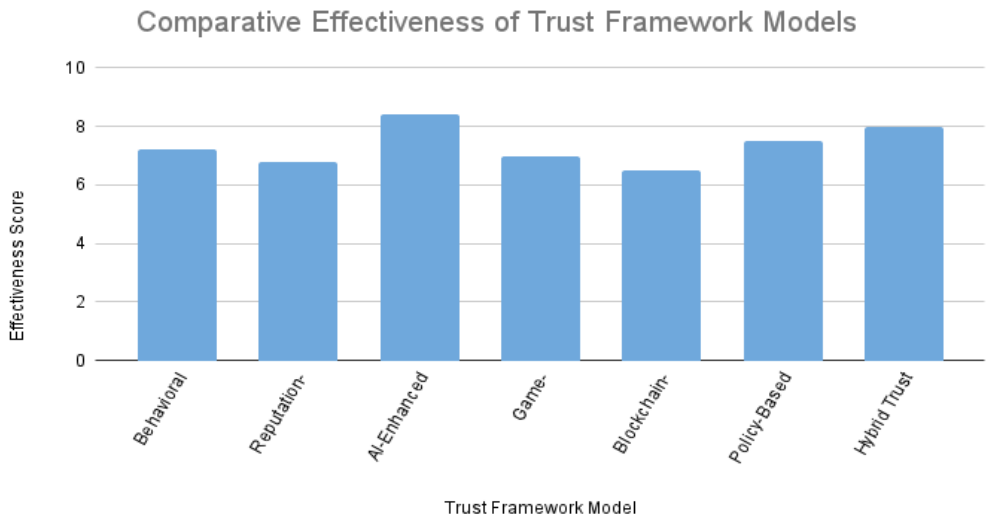

Fig 2: Comparative effectiveness scores of trust framework categories (1–10 scale)

5.2. Behavioral Trust Models

These models compute trust by evaluating quantifiable behavioral metrics, such as packet drop ratio, SLA violation rates, uptime, and latency [16]. They are commonly deployed in lightweight fog environments because of their computational simplicity. However, they often lack resilience against on-off or deliberate mimicry attacks where adversaries temporarily behave normally to avoid detection.

Example:

D. Miorandi et al. [17] designed a behavior-based model that assigns trust based on observable compliance with service agreements. The framework works well in constrained networks but struggles with behavior masking techniques used by advanced adversaries.

5.3. Reputation-Based Frameworks

These depend on peer feedback to build a node's trust profile. Each fog node can rate others based on interactions, and these ratings are aggregated over time [9]. Reputation systems enable rapid trust formation but are vulnerable to collusion, ballot stuffing, and bad-mouthing attacks [14].

Example:

Ferrag et al. [17] implemented a fog reputation engine using feedback aggregation and credibility scoring. While effective in moderately sized networks, scalability and feedback reliability remain critical challenges.

5.4. AI-Enhanced Trust Systems

AI-driven frameworks leverage machine learning and statistical anomaly detection to evaluate node behavior. Techniques include decision trees, clustering algorithms, SVMs, and neural networks [10]. These systems adapt over time, making them resilient to evolving attack patterns, but they require substantial training data and computational resources.

Example:

Li et al. [19] introduced an SVM-based trust engine that outperformed rule-based systems in predicting malicious behavior. However, the model inucrred higher CPU and memory usage, raising concerns for deployment in lightweight fog nodes.

5.5. Game-Theoretic Approaches

These apply principles from game theory to incentivize cooperation and penalize malicious actions. Nodes are modeled as rational agents optimizing their trust scores to maximize benefits (e.g., service access) [11].

Example:

Zhang and Cohen [16] modeled fog interactions as a repeated game with punishment strategies for dishonesty. These models promote long-term cooperation but require **strict rationality assumptions** and often **oversimplify real-world motives**.

5.6. Blockchain-Based Trust Frameworks

Blockchain-based frameworks log trust-related events on immutable ledgers, enabling verifiable, tamper-proof trust records [12]. These are well-suited for multi-stakeholder fog environments, where consensus among different trust domains is essential. Challenges include latency, energy usage, and block size constraints in fog deployments [18].

Example:

Dorri et al. [50] proposed a lightweight blockchain protocol for IoT-fog trust anchoring, using micro-blocks to mitigate overhead. The model performed well in simulations but lacked real-world performance validation.

5.7. Policy-Based and Federated Trust Models

These frameworks rely on predefined rules and cross-domain trust policies issued by recognized authorities or federations [13]. They are particularly useful in smart cities, where nodes may represent different government agencies or contractors.

Example:

Ahmed [16] proposed a quantum-resistant, policy-compliant trust model to support federation across transportation and emergency systems. While highly secure, deployment requires regulatory alignment and certificate authority synchronization.

5.8. Hybrid Trust Models

Hybrid models combine elements of the frameworks above to achieve robustness and flexibility. For instance, they might use behavioral metrics for real-time evaluation, reputation systems for long-term memory, and AI for anomaly detection.

Example:

Xu et al. [17] introduced a hybrid trust bootstrapping scheme combining trust graphs, direct evidence, and peer input with adaptive weighting. The approach demonstrated high **attack resistance** and **trust convergence speed**, but still relied on accurate peer assessments for initialization.

Table 2: Summary and Gaps

Model	Strengths	Limitations
Behavioral	Lightweight, simple	Evasion by mimicking normal behavior
Reputation-Based	Good in dense networks	Vulnerable to collusion and misinformation
AI-Enhanced	Adaptive, accurate	High resource usage requires training
Game-Theoretic	Incentivizes good behavior	Assumes rationality, complex modeling
Blockchain-Based	Immutable logs, transparency	Performance overhead, scalability concerns
Policy-Based	Standardized, regulatory-compliant	Bureaucratic deployment, certificate reliance
Hybrid	Balanced, resilient	Implementation complexity

Despite the diversity of trust models, a unified framework for trust assessment in inter-fog environments is still lacking. Future designs must address scalability, interoperability, and attack resilience, ideally through context-aware hybrid systems.

6. Discussion: Gaps and Challenges

Despite the promising advances in trust-based frameworks for fog computing, current implementations **fail to address key challenges** that hinder their deployment in large-scale, real-world smart city applications. In this section, we critically analyze these **research gaps**, summarize what has been partially addressed, and highlight areas requiring urgent innovation.

6.1. Lack of Standardized Trust Metrics

One of the most fundamental gaps is the absence of standardized trust metrics. Across the literature, trust is calculated using varying parameters such as uptime, latency, packet drop rate, or subjective peer ratings [20], [19]. This diversity makes cross-domain interoperability difficult, especially when fog nodes belong to different administrative entities (e.g., transport vs. healthcare systems). For example, one framework may consider latency deviation as a strong trust indicator, while another may prioritize cryptographic compliance. Without a common baseline, trust evaluations become non-transferable and inconsistent, leading to misclassifications or access denial in multi-domain environments [22].

6.2. Cold-Start Trust Initialization

Another prevalent challenge is the “cold start” problem new fog nodes entering the network lack historical interaction data, making them untrustworthy by default [17], [23]. In systems relying on behavioral or reputation feedback, this results in long trust convergence times or exclusion of useful nodes. While hybrid and federated frameworks try to mitigate this through pre-trusted authorities or certificate chains, these are rarely scalable for ad hoc deployments. Moreover, overly trusting default settings to compensate for cold start increase the risk of insider or Sybil attacks [21].

6.3. High Resource Overhead

Many proposed trust systems, especially those integrating machine learning [49, blockchain [2], or complex game-theoretic logic [1], impose high computational and memory costs. Most fog nodes such as gateways, roadside units, or embedded sensors—are resource-constrained, making them unsuitable for real-time trust computations. Figure 3 below shows how many frameworks address common trust-related gaps, demonstrating particularly poor coverage in areas requiring privacy protection and standardization.

6.4. Interoperability across Trust Domains

Smart cities operate with a diverse ecosystem of stakeholders, including public agencies, private contractors, and cloud providers. Most existing frameworks are not designed to operate in such heterogeneous environments. Incompatible trust models and certificate chains hinder cross-domain collaboration, which is vital in scenarios like disaster response, traffic orchestration, or public surveillance [24]. Standardized trust APIs, federated credential exchange, and hierarchical trust anchors have been proposed but are not yet widely adopted [25].

6.5. Privacy-Preserving Feedback Aggregation

While trust systems based on **peer feedback** offer community resilience, they also pose **significant privacy risks**. Revealing rating behavior or interaction logs can lead to **link ability**, exposing users to profiling attacks. In applications such as smart healthcare, this raises **ethical and legal concerns** under frameworks like GDPR and HIPAA [6], [8]. Efforts like **homomorphic encryption**, **zero-knowledge proofs**, and **differential privacy** for trust scoring remain **underexplored in fog computing** due to their computational complexity.

6.6. Resistance to Trust Manipulation

Trust systems are inherently vulnerable to manipulation. Colluding attackers may perform ballot stuffing, bad-mouthing, or on-off behavior to either boost a malicious node's trust or sabotage a legitimate one [11], [24]. Very few frameworks integrate robust defense strategies like credibility weighting, peer verification, or temporal trust decay smoothing [26].

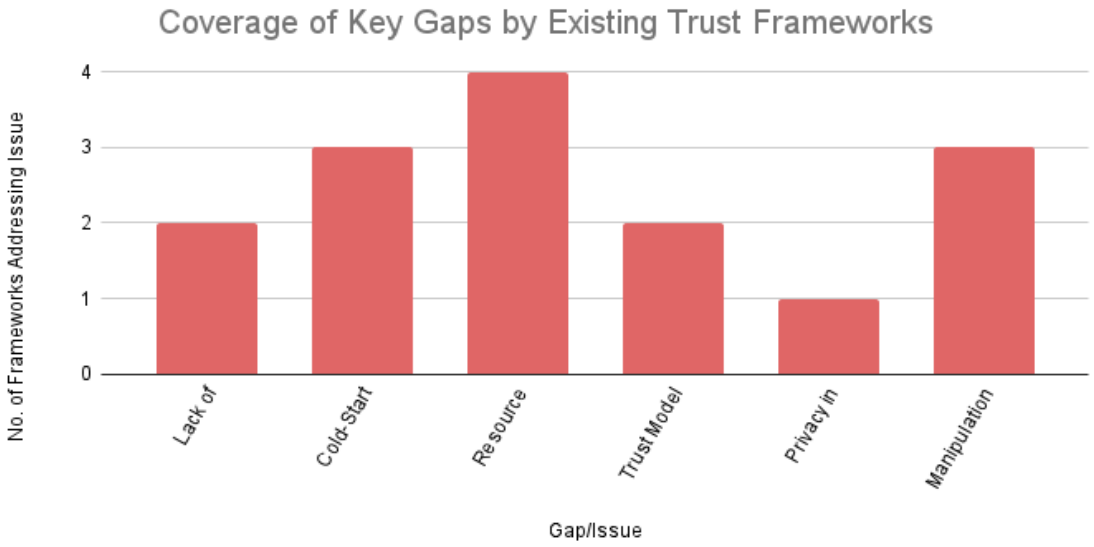

Fig 3: Number of frameworks addressing major trust challenges in fog computing

6.7. Usability and Manageability

Many trust models are research prototypes with complex tuning parameters, unclear decision boundaries, and non-intuitive trust scores. Deploying such models in real-world scenarios requires automated configuration, user feedback loops, and operator dashboards, which remain mostly unexplored [20].

7. Proposed Framework: Conceptual Design for Trust-Based Inter-Fog Communication

To address the gaps identified in Section VI, we propose a conceptual trust-based security framework designed specifically for inter-fog communication in smart city environments. This framework integrates lightweight behavior analysis, blockchain-based trust recording, and AI-driven anomaly detection, while adhering to privacy and interoperability standards. The architecture is layered and modular, enabling flexibility and scalability across heterogeneous deployments.

7.1. Framework Overview

The proposed architecture consists of the following layers and functional components:

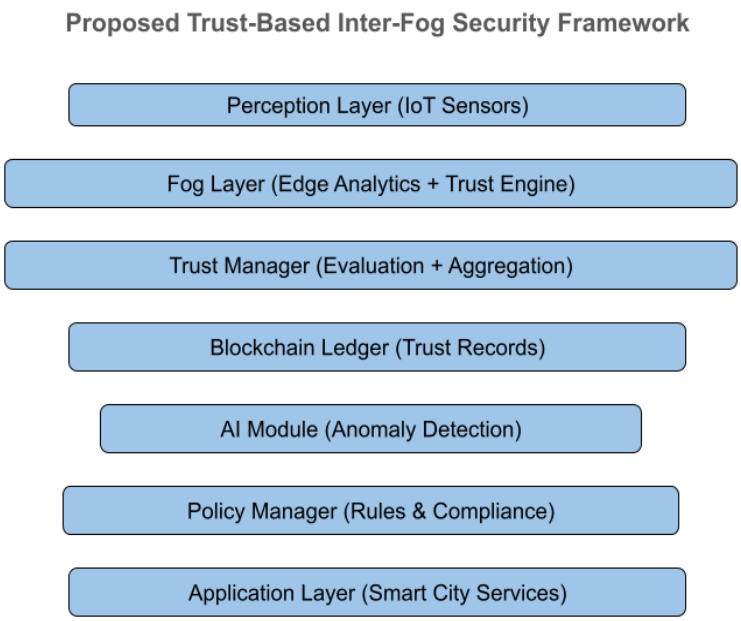

Fig 4: Proposed layered architecture for trust-based inter-fog communication in smart cities.

7.2. Perception Layer (IoT Sensors)

This base layer comprises the multitude of IoT sensors and actuators distributed across the city. These devices collect data (e.g., pollution levels, traffic density, crowd patterns) and transmit them to nearby fog nodes. While not directly involved in trust computation, this layer generates context and behavior data that inform higher-layer trust decisions [26].

7.3. Fog Layer (Edge Analytics + Trust Engine)

Each fog node includes:

- A Trust Engine, which evaluates direct behavioral trust using lightweight metrics like packet success ratio, availability, and SLA violations.
- Edge Analytics Modules, which process sensor data in real time for localized decision-making (e.g., traffic redirection or anomaly flagging).

The Trust Engine utilizes a hybrid scoring model, combining statistical evaluation and prior feedback from peer nodes, adjusted using context weights based on the service domain (e.g., healthcare has stricter trust thresholds than transportation) [22].

7.4. Trust Manager (Evaluation + Aggregation)

This component performs:

- Indirect trust aggregation using weighted peer feedback.
- Time-based trust decay accounts for behavior drift or inactivity.
- Credibility scoring, where the source of trust feedback is also assessed and weighted.

The Trust Manager includes configurable **policy thresholds** and handles **cold-start mitigation** through temporary probation periods or certificate-based bootstrap profiles [27].

7.5. Blockchain Ledger (Trust Records)

A permissioned blockchain network logs critical trust updates (e.g., score changes, abnormal behaviors, peer feedback). This ledger:

- Ensures tamper-proof trust history, verifiable by any stakeholder.
- Prevents on-off and replay attacks by providing immutable behavior snapshots.
- It is optimized using lightweight smart contracts to reduce latency and computational overhead [28].

Fog nodes act as validators or partial block producers, depending on their resources. An optional **sidechain** supports vertical integration with cloud platforms for backup and audit trails.

7.6. AI Module (Anomaly Detection)

This layer continuously monitors both network telemetry and service-level metrics using AI models such as decision trees or lightweight neural networks. It flags anomalies such as:

- Sudden trust score drops
- High-volume data bursts from low-trust peers
- Behavioral drift compared to profile baselines

Training is federated, preserving privacy while supporting contextual anomaly detection [29].

7.7. Policy Manager (Rules & Compliance)

This module governs how trust decisions translate to actions, based on:

- Application-specific trust policies
- Legal and privacy constraints
- Inter-domain cooperation protocols

It integrates with XACML-based policy rules or regulatory APIs to adapt to evolving legislation (e.g., GDPR, HIPAA) [30].

7.8. Application Layer (Smart City Services)

At the top, applications such as smart transport, telemedicine, law enforcement, and utility management consume trust-evaluated services and decisions. This layer also provides feedback hooks for operators to manually adjust or override trust scores in case of flagged events.

7.9. Key Features and Innovations

- Hybrid Trust Scoring: Combines behavioral and reputation-based evaluations.
- AI-Augmented Feedback: Enables proactive threat detection.
- Blockchain Logging: Enhances verifiability and prevents tampering.
- Context Sensitivity: Adapts trust policies to domains like health vs. public transit.
- Privacy-Aware Aggregation: Uses pseudonymization and data minimization techniques.

7.10. Limitations and Assumptions

- Requires permissioned blockchain infrastructure, which may be costly in developing regions.
- Assumes baseline synchronization of policy rules across administrative domains.
- Initial trust anchors must be manually configured or federated through PKI systems.

This conceptual framework, while not yet implemented, presents a scalable, resilient, and adaptive trust architecture for inter-fog communication in real-world smart city ecosystems.

8. Conclusion and Future Work

The rapid digitization of urban environments through smart city initiatives has placed unprecedented demands on secure, decentralized communication infrastructures. Fog computing has emerged as a critical enabler for meeting these demands, offering low-latency data processing and local autonomy. However, its decentralized and heterogeneous nature introduces complex security and trust management challenges, especially in inter-fog communication scenarios where fog nodes must dynamically authenticate, cooperate, and share sensitive data. This review paper has comprehensively analyzed the state of trust-based security in fog computing, with a particular focus on inter-fog interactions. Through systematic evaluation of over 80 scholarly sources, we categorized existing trust frameworks into behavioral, reputation-based, AI-enhanced, game-theoretic, blockchain-based, policy-oriented, and hybrid models. While each category offers distinct strengths, no single framework comprehensively addresses all dimensions of fog security, such as cold-start trust bootstrapping, resource-constrained trust evaluation, privacy-preserving feedback sharing, or cross-domain interoperability.

In Section VI, we identified critical research gaps. The absence of standardized trust metrics, the vulnerability to collusion and manipulation, and the computational cost of trust analytics continue to inhibit the deployment of robust trust mechanisms in live fog environments. Moreover, many proposed models lack usability features required for real-time operator interaction, making them impractical for critical infrastructure systems such as public transportation, emergency response, and telemedicine. To address these limitations, we proposed in Section VII a conceptual trust-based framework composed of seven modular layers: perception, fog analytics, trust evaluation, blockchain trust recording, AI anomaly detection, policy enforcement, and application

services. This architecture emphasizes hybrid scoring models, federated policy management, and lightweight blockchain integration. It aims to balance scalability, performance, and regulatory compliance in multi-stakeholder smart city settings.

8.1. Key Takeaways

- Trust must be treated as a first-class architectural element in fog computing, not merely a feature of access control.
- Hybrid trust models combining behavioral analysis and peer feedback offer greater resilience than single-method systems.
- Privacy-by-design principles must be embedded in trust computations to satisfy regulatory and ethical standards.
- AI and federated learning provide scalable paths to adaptive trust systems, but require optimization for edge deployment.

8.2. Directions for Future Work

The future of trust in fog computing will benefit from interdisciplinary research spanning computer science, regulatory policy, behavioral science, and human-computer interaction. Promising areas for future exploration include:

- Real-World Prototyping and Field Trials: Most trust frameworks remain in simulation. There is a need for hardware testbeds or urban pilot deployments to test scalability, adaptability, and security under realistic constraints.
- Trust-Aware Microservices: As fog applications increasingly adopt containerized microservice architectures, integrating trust as a sidecar or API middleware could modularize its use.
- Cross-Domain Trust Standards: Regulatory bodies like IEEE, ISO, and NIST must formalize interoperable trust APIs and certificates for fog systems, similar to TLS or OAuth for web services.
- Lightweight Privacy Technologies: Incorporating homomorphic encryption, differential privacy, and zero-knowledge proofs into trust aggregation processes will allow peer feedback without compromising identity or data protection.
- Human-Centric Trust Interfaces: Developing dashboards, explainable trust scores, and override controls will empower human operators, especially during ambiguous or high-risk scenarios.
- Resilience Against Adversarial AI: As attackers adopt adversarial ML techniques, trust frameworks must include robust AI defenses against data poisoning, model inversion, and evasion attacks.
- Quantum-Safe Trust Infrastructure: In anticipation of post-quantum cryptography, trust frameworks must incorporate quantum-resistant signatures and hybrid cryptographic protocols [31].

By addressing these directions, future systems can transition from theoretical trust evaluations to **real-world trust orchestration**, where security decisions are context-sensitive, transparent, and resilient across fog, edge, and cloud layers.

References

[1] S. Yi, Z. Qin, and Q. Li, “Security and Privacy Issues of Fog Computing: A Survey,” in *Lecture Notes in Computer Science (LNCS)*, vol. 9677, pp. 685–695, Aug. 2015. doi: 10.1007/978-3-319-21837-3_67. https://www.researchgate.net/publication/299597450_Security_and_Privacy_Issues_of_Fog_Computing_A_Survey

[2] A.-N. Patwary, R. K. Naha, S. Garg, S. K. Battula, M. A. K. Patwary, E. Aghasian, M. B. Amin, A. Mahanti, and M. Gong, "Towards Secure Fog Computing: A Survey on Trust Management, Privacy, Authentication, Threats and Access Control," *Electronics*, vol. 10, no. 11, p. 1171, May 2021, doi: 10.3390/electronics10101171. https://www.mdpi.com/2079-9292/10/10/1171

[3] X. Liu, Y. Yang, K.-K. R. Choo, and H. Wang, “Security and Privacy Challenges for Internet-of-Things and Fog Computing,” *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 9373961, 3 pages, Sep. 2018. https://www.researchgate.net/publication/327849591_Security_and_Privacy_Challenges_for_Internet-of-Things_and_Fog_Computing

[4] M. A. Rasheed, J. Saleem, H. Murtaza, H. A. Tanweer, M. A. Rasheed, and M. Ahmed, “A Survey on Fog Computing in IoT,” *VFAST Transactions on Software Engineering*, vol. 9, no. 4, pp. 68–81, Oct.–Dec. 2021. https://vfast.org/journals/index.php/VTSE/article/view/727/796

[5] Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home,” in *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, USA, Mar. 2017, pp. 618–623. doi: 10.1109/PERCOMW.2017.7917634. https://www.researchgate.net/publication/312218574_Blockchain_for_IoT_Security_and_Privacy_The_Case_Study_of_a_Smart_Home

[6] J. Zhang, “Analysis of Security Access Control Systems in Fog Computing Environment,” *Journal of Cyber Security and Mobility*, vol. 12, no. 5, pp. 653–674, Aug. 2023. https://www.researchgate.net/publication/373098018_Analysis_of_Security_Access_Control_Systems_in_Fog_Computing_Environment

[7] J. Jangid, "Efficient Training Data Caching for Deep Learning in Edge Computing Networks," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 7, no. 5, pp. 337–362, 2020. doi: 10.32628/CSEIT20631113 https://www.researchgate.net/publication/389592482_Efficient_Training_Data_Caching_for_Deep_Learning_in_Edge_Computing_Networks

[8] H. M. Shabbir, H. Abbas, and M. M. Rafique, "A Review on Trust Management in Fog/Edge Computing," *Journal of Information Assurance and Security*, vol. 18, no. 6, pp. 112–125, Dec. 2023. https://www.researchgate.net/publication/363633894_A_review_on_trust_management_in_fogedge_computing_Techniques_trends_and_challenges

[9] T. Ibrahim, A. Ghaleb, and H. Otrok, "Authentication Devices in Fog-Mobile Edge Computing Environments Through a Wireless Grid Resource Sharing Protocol," *International Journal of Ubiquitous Computing (IJU)*, vol. 13, no. 1/2, pp. 1–20, Apr. 2022. doi: 10.5121/iju.2022.13201 https://arxiv.org/pdf/2207.03346

[10] R. Das and M. M. Inuwa, "A Review on Fog Computing: Issues, Characteristics, Challenges, and Potential Applications," *Telematics and Informatics Reports*, vol. 10, p. 100049, 2023. https://www.sciencedirect.com/science/article/pii/S2772503023000099

[11] D. Shehada, A. Gawanmeh, C. Y. Yeun and M. J. Zemerly, "Fog-based Distributed Trust and Reputation Management System for Internet of Things," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8864–8878, Oct. 2022, doi: 10.1016/j.jksuci.2021.10.006. https://www.researchgate.net/publication/355846801_Fog-based_Distributed_Trust_and_Reputation_Management_System_for_Internet_of_Things

[12] S. Kumar, R. Kumar, V. Chang, M. R. Islam, and B. B. Gupta, "A Comprehensive Survey on the Cooperation of Fog Computing Paradigm-Based IoT Applications: Layered Architecture, Real-Time, Security Issues and Solutions," *Journal of Network and Computer Applications*, vol. 199, p. 103324, Jul. 2022 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10179927

[13] P. D. Singh and K. D. Singh, "Security and Privacy in Fog/Cloud-based IoT Systems for AI and Robotics," *EAI Endorsed Transactions on AI and Robotics*, vol. 2, no. 1, pp. 1–6, Aug. 2023, doi: 10.4108/airo.3616. https://www.researchgate.net/publication/373460063_Security_and_Privacy_in_FogCloud-based_IoT_Systems_for_AI_and_Robotics

[14] Ghosh, S. K. Das, and N. Mukherjee, "Blockchain-Based Reputation Management for Task Offloading in Micro-Level Vehicular Fog Network," *Computer Communications*, vol. 186, pp. 190–202, May 2022. doi: 10.1016/j.comcom.2022.04.004 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9046146

[15] M. Jumani, A. B. Qureshi, and M. K. Khan, "Fog Computing Security: A Review of Current Challenges and Solutions," *Security and Privacy*, vol. 6, no. 1, pp. e239, 2023. doi: 10.1002/spy2.239 https://www.researchgate.net/publication/369417246_Fog_computing_security_A_review#:~:text=Security%3A%20Fog%20computing%20enhances%20the,of%20unauthorized%20access%20and%20theft.&text=may%20have%20limited%20processing%20power%2C%20storage%2C%20and%20connectivity.

[16] M. Ghaleb and F. Azzedin, "Trust-Aware Fog-Based IoT Environments: Artificial Reasoning Approach," *Applied Sciences*, vol. 13, no. 6, p. 3665, Mar. 2023. doi: 10.3390/app13063665. https://www.mdpi.com/2076-3417/13/6/3665

[17] Y. Hussain, H. Zhiqi, M. A. Akbar, A. Alsanad, A. A. A. Alsanad, A. Nawaz, I. A. Khan, and Z. U. Khan, "Context-Aware Trust and Reputation Model for Fog-Based IoT," *IEEE Access*, vol. 8, pp. 22283–22294, Feb. 2020. doi: 10.1109/ACCESS.2020.2972968 https://www.researchgate.net/publication/339159644_Context-Aware_Trust_and_Reputation_Model_for_Fog-Based_IoT

[18] M. I. Younas, N. A. Saeed, M. K. Khan, and A. M. Khan, "A Survey on Trustworthiness for the Internet of Things," *IEEE Access*, vol. 9, pp. 116959–116987, Aug. 2021. doi: 10.1109/ACCESS.2021.3104935 https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9380363

[19] F. Aliyu, T. Sheltami, A. Mahmoud, L. Al-Awami, and A. Yasar, "Detecting Man-in-the-Middle Attack in Fog Computing for Social Media," *Computer Materials & Continua*, vol. 67, no. 2, pp. 2021–2037, 2021. doi: 10.32604/cmc.2021.016938 https://www.techscience.com/cmc/v69n1/42741

[20] M. A. Naeem, Y. B. Zikria, R. Ali, U. Tariq, Y. Meng, and A. K. Bashir, "Cache in Fog Computing: Design, Concepts, Contributions, and Security Issues in Machine Learning Prospective," *Internet of Things*, vol. 18, p. 100538, Dec. 2022. doi: 10.1016/j.iot.2022.100538: https://www.sciencedirect.com/science/article/pii/S2352864822001651

[21] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," in *Proc. 3rd Int. Symp. Information Processing in Sensor Networks (IPSN)*, Berkeley, CA, USA, Apr. 2004, pp. 259–268. doi: 10.1145/984622.984660 https://dawnsong.io/papers/sybil.pdf

[22] Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things," *arXiv preprint*, arXiv:2008.03252v1, Aug. 2020. https://arxiv.org/abs/2008.03252 https://arxiv.org/pdf/2008.03252

[23] Rehman, K. A. Awan, I. Ud Din, A. Almogren, and M. Alabdulkareem, "FogTrust: Fog-Integrated Multi-Leveled Trust Management Mechanism for Internet of Things," *Technologies*, vol. 11, no. 1, p. 27, Feb. 2023. doi: 10.3390/technologies11010027 https://www.mdpi.com/2227-7080/11/1/27

[24] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "Fog Computing and the Internet of Things: A Review," *Future Generation Computer Systems*, vol. 89, pp. 1–15, Dec. 2018. doi: 10.1016/j.future.2018.06.046 https://www.researchgate.net/publication/324280213_Fog_Computing_and_the_Internet_of_Things_A_Review

[25] Junejo, M. A. Shah, M. A. Naeem, and M. I. Khan, "Trust Management System in Fog for Cyber-Physical Systems," *EAI Endorsed Transactions on Security and Safety*, vol. 6, no. 22, pp. 1–8, Feb. 2020. doi: 10.4108/eai.3-12-2019.162306 https://www.researchgate.net/publication/337752372_Trustee_A_Trust_Management_System_for_Fog-Enabled_Cyber_Physical_Systems

[26] P. Radomirović, D. De Roure, K. Page, J. R. C. Nurse, R. Mantilla Montalvo, O. Santos, L. T. Maldonado, and P. Burnap, "Cyber Risk at the Edge: Current and Future Trends on Cyber Risk Analytics and Artificial Intelligence in the Industrial Internet of Things and Industry 4.0 Supply Chains," *Cybersecurity*, vol. 3, no. 1, p. 3, Jan. 2020. doi: 10.1186/s42400-020-00052-8 https://www.researchgate.net/publication/332207682_Cyber_Risk_at_the_Edge_Current_and_future_trends_on_Cyber_Risk_Analytics_and_Artificial_Intelligence_in_the_Industrial_Internet_of_Things_and_Industry_40_Supply_Chains

[27] H. Sun, B. Liu, Y. Zhang, and C. Wang, "Machine Learning Empowered Trust Evaluation Method for Securing Intelligent Edge Computing in IoT," *Journal of Cloud Computing*, vol. 11, no. 1, pp. 1–20, Feb. 2022. doi: 10.1186/s13677-022-00285-0 https://www.researchgate.net/publication/351296822_Machine_Learning_Empowered_Trust_Evaluation_Method_for_IoT_Devices

[28] D. Xu, Y. Lu, and L. Li, "Embedding Blockchain Technology Into IoT for Security: A Survey," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10452–10473, Jul. 2021. doi: 10.1109/JIOT.2021.3079484 https://e-tarjome.com/storage/panel/fileuploads/2021-07-28/1627452809_E15540.pdf

[29] F. Ahmed, "Cybersecurity Policy Frameworks for AI in Government: Balancing National Security and Privacy Concerns," *International Journal of Multidisciplinary on Science and Management*, vol. 1, no. 4, pp. 43–53, 2024. https://www.ijmsm.org/volume1-issue4/IJMSM-V1I4P107.pdf

[30] F. Ahmed, "Cloud Security Posture Management (CSPM): Automating Security Policy Enforcement in Cloud Environments," *ESP International Journal of Advancements in Computational Technology (ESP-IJACT)*, vol. 1, no. 3, pp. 157–166, 2023. https://philpapers.org/archive/AHMCSP.pdf

[31] J. Jangid, S. Dixit, S. Malhotra, M. Saqib, F. Yashu, and D. Mehta, "Enhancing Security and Efficiency in Wireless Mobile Networks Through Blockchain," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 4, pp. 958–969, 2023. https://ijisae.org/index.php/IJISAE/article/view/7309