International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 11 | Nov – 2025 DOI: 10.55041/ISJEM05109
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

A Taxonomy of Trust Attack Mechanisms in Internet of Things Networks and Countermeasure Analysis

Manish Kumar
CSA
Sharda University
Greater.Noida
2023411548.manish@ug.sharda.ac.in

Harshit Pandey
CSA
Sharda University
Delhi
harshitpb96@gmail.com

Paras Yadav
CSA
Sharda University
Greater.Noida
yadav16118119@gmail.com

Supervisor- Mr Manoj Kumar,Department of CSA,Sharda university

Abstract

The Internet of Things (IoT), growing rapidly, creates a network of connected smart devices. IoT's low computational power, energy constraints, and dynamic topology make it highly susceptible to cyber threats despite offering significant advantages in connectivity. Trust management has become an essential tool for ensuring safe communication between various types of electronic gadgets. However, relying on trust has led to the creation of a group of complex attacks that specifically aim to exploit and control trust levels. This document thoroughly examines all methods used in attacks. A classification of trust attacks divides them into two categories: direct attacks where a malicious node alters its actions independently, and indirect attacks aimed at corrupting the reputation system by providing misleading suggestions. We examine and debate current strategies for defending against cyber threats, focusing on methods such as those that are quick to use, spread across multiple locations, and rely on mathematical theories. The paper concludes by pointing out major obstacles and suggesting paths for further study to create stronger and more dependable Internet of Things systems. Internet of Things, security of IoT systems, managing trust in these systems, attacks from cyber threats, categorization for defense strategies, countermeasures against such risks.

Keywords: Internet of Things, IoT Security, Trust Management, Cyber Attacks, Trust Attacks, Taxonomy, Countermeasures.

I.Introduction

The Internet of Things (IoT) is an international network of physical devices, or "things," that are embedded with sensors, software, and other technologies to be able to interact and share information with other devices and systems across the internet [1]. The potential of IoT is to make possible the seamless interaction of the digital and physical worlds, which in turn will have transformative uses in smart cities, healthcare, industrial automation, and smart homes. Nonetheless, the sheer number and diversity of IoT devices and their resource constraints pose an overwhelming challenge to conventional security models. Most IoT devices, unlike traditional IT systems, are incapable of supporting advanced cryptographic algorithms or strong firewalls and are therefore extremely vulnerable to being compromised. Trust management has thus been suggested as a critical security component for IoT networks [2]. A trust model enables a device (trustor) to estimate the trust value of another device (trustee) on the basis of factors like past actions, reputation, and explicit interactions.

© 2025, ISJEM (All Rights Reserved)

Dynamically allocating trust values enables the network to quarantine and reduce the effect of malicious nodes. This is especially effective against "insider" attacks, wherein a compromised or malicious device tries to sabotage the network from the inside. But trust dependency has opened up a new class of advanced attacks targeted at the trust management system itself. Such trust attacks aim to manipulate the calculation process of trust, either by artificially inflating the trust value of a malicious node or unfairly deteriorating the trust of honest nodes. These kinds of attacks have the capability to partition the network, corrupt data, and completely disrupt dependable communication, eventually undermining the entire IoT system.This paper thoroughly analyses trust breaches within Internet of Things systems. The main points are listed below.

- We create a classification system for trust breaches by grouping them according to how they occur and who they affect.
- We offer an in-depth look at typical and perilous methods used by attackers to exploit trusts.
- We examine and debate current strategies for protecting against recent threats.
- We pinpoint and detail current issues in IoT security and suggest paths forward for creating safer and dependable IoT networks.

Literature Review

1. Introduction: The Need for Trust in an IoT World

The Internet of Things (IoT) is no longer a futuristic concept; it is rapidly becoming the fabric of our modern world. It represents a vast network of interconnected devices—from smart thermostats and wearables to industrial sensors and autonomous vehicles—all communicating and collaborating with minimal human intervention. This evolution from a web of computers to a web of "things" promises unprecedented efficiency and innovation.

However, this pervasive connectivity introduces profound security challenges. Traditional security measures, often called "hard security" like encryption and access control, are essential but insufficient. They act as a strong lock on a door, but cannot prevent a guest you've already admitted from misbehaving inside your home. In the IoT, these "guests" could be millions of devices, and a malfunctioning or malicious one can cause real-world harm, from privacy breaches to physical safety risks.

This is where Trust Management (TM) emerges as a critical, complementary paradigm. Think of TM as the "social sense" or "immune system" for the IoT. It is a "soft security" approach that allows devices to evaluate the reliability and integrity of their peers based on observed behavior over time. It answers fundamental questions like: Can I trust this sensor to provide accurate data? Can I rely on that node to forward my message? Is this service provider delivering on its promises? Without robust trust mechanisms, the widespread adoption of IoT in critical areas like healthcare, transportation, and smart cities will be severely hampered by justifiable concerns over reliability and security.

2. The Nature of Trust: A Dynamic and Nuanced Relationship

It is crucial to understand that trust in the IoT is not a simple, static checkbox. It is a nuanced, multi-faceted concept borrowed from human social interactions, characterized by several key attributes:

Dynamic: Trust is not permanent. It must continuously evolve, increasing with positive interactions and decreasing with negative or suspicious behavior.

Context-Dependent: A device may be highly trustworthy in one context but not another. A sensor might be reliable for measuring ambient temperature but completely untrustworthy for managing a critical alarm system.

1. **Subjective:** Trust is influenced by the trustor's own preferences and risk tolerance. Different applications may weight the importance of speed, accuracy, or energy efficiency differently in their trust evaluation.
2. **Asymmetric:** The fact that Device A trusts Device B does not imply that Device B trusts Device A. Trust is a one-way relationship.

These characteristics make trust a complex property to quantify, requiring sophisticated models that can adapt and reason under uncertainty.

3. Architectural Frameworks: How Trust Systems are Built

The implementation of a TM system is shaped by its underlying architecture, which dictates how trust information is collected and shared. The literature primarily distinguishes between three models:

Centralized Architecture: A single, powerful server acts as a Trust Authority. All devices report their experiences to this central entity, which calculates and distributes trust scores. This is simple to manage but creates a single point of failure and a performance bottleneck, making it poorly suited for the massive scale of the IoT.

Distributed Architecture: Every device is responsible for managing its own trust relationships. It calculates trust based on its own direct experiences and recommendations from neighboring devices. This model is highly resilient and scalable, as there is no central point to attack. However, it is more complex and vulnerable to false recommendations from malicious peers.

Hybrid Architecture: This approach seeks the best of both worlds. It uses local, more powerful nodes (like gateways or cluster heads) to act as trust authorities for a limited group of devices. This balances local autonomy with a degree of coordinated oversight, making it the most practical and commonly proposed model for real-world IoT deployments.

4. The Engine of Trust: Models and Techniques for Calculation

At the heart of any TM system is the computational model—the mathematical or logical engine that transforms observations into a trust score.

- **Reputation-Based Models:** These are the most prevalent. Similar to an eBay rating system, devices build a reputation from direct interactions and recommendations from others. The core challenge is filtering out dishonest praise or criticism.
- **Policy-Based Models:** These rely on pre-defined rules and credentials. Access is granted if a device can present the right digital certificate, for example. This is precise but lacks adaptability to changing behaviors.
- **Advanced and Hybrid Techniques:** To handle the complexity of trust, researchers employ sophisticated methods:
- **Fuzzy Logic:** Manages the imprecise, "human" nature of trust (e.g., "mostly reliable").
- **Bayesian Systems**: Model trust as a probability that is updated with each new interaction.

- **Game Theory:** Incentivizes cooperative behavior by making trustworthiness the most beneficial strategy for a device.
- **Blockchain:** An emerging and powerful tool that creates a decentralized, tamper-proof ledger of all interactions, making reputation histories transparent and immutable.

5. Critical Applications: Where Trust Management Makes a Difference

Trust management is not an academic exercise; it enables critical functionalities across the IoT landscape:

- **Secure and Trust-Aware Routing**: In wireless mesh networks, TM helps data packets find reliable paths, automatically routing around malicious nodes that drop or manipulate traffic.
- **Dynamic Access Control:** A device's access to sensitive resources can be dynamically adjusted based on its real-time trust score, revoking privileges if its behavior becomes suspicious.
- **Reliable Service Composition:** In a marketplace of IoT services, TM acts as a Yelp-like reputation system, allowing a device to select the most trustworthy service provider from many available options.
- **Data Integrity and Validation:**TM can help verify the trustworthiness of the *data itself*, cross-referencing sensor readings to identify outliers or faulty data, even from a non-malicious device.

6. Challenges and Future Directions

The path to fully realized TM is fraught with challenges. The extreme resource constraints (power, computation) of many IoT devices demand ultra-lightweight algorithms. The scale and heterogeneity of devices make standardization difficult. Furthermore, TM systems must be resilient against intelligent attacks, such as On-Off Attacks (where a device alternates between good and bad behavior) and Collusion Attacks(where groups of malicious devices lie to manipulate reputations).

Looking ahead, the future of IoT trust lies in greater intelligence and integration. Key research directions include:

- Leveraging AI and Machine Learning to detect subtle, complex attack patterns that evade traditional models.
- Developing Cross-Layer Frameworks that combine trust evidence from hardware, network, and application levels for a holistic view.
- Personalizing Trust to reflect the specific risk tolerance and requirements of different users and applications.
- Exploring the Social IoT (SIoT), where trust is inferred from the social relationships between the owners of devices, creating a more intuitive trust network.

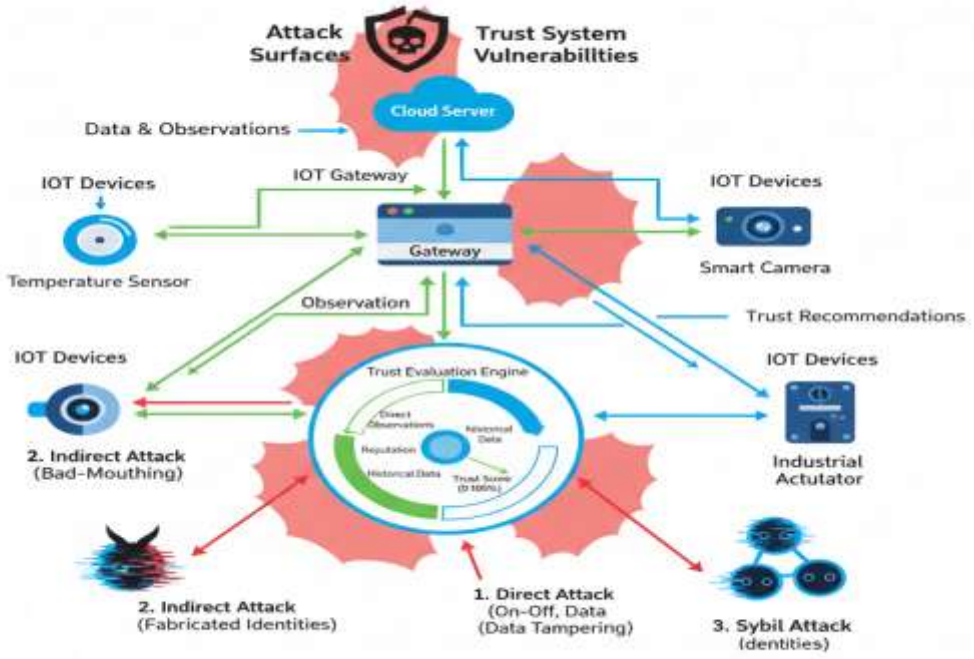
7. Conclusion

In conclusion, as the Internet of Things continues to mature and embed itself into the critical infrastructure of our society, trust management ceases to be an optional add-on and becomes a foundational requirement. It is the key that enables security and reliability to scale alongside connectivity. By providing devices with the ability to make informed judgments about their peers, we can build an IoT ecosystem that is not only smart but also

secure, resilient, and worthy of our trust. The ongoing research and development in this field are therefore not just technical pursuits but essential steps toward a safe and successful connected future.

Figure 1: IoT Trust Management Overview and Attack Surfaces

The illustration will showcase an abbreviated Internet of Things architecture comprising diverse components such as sensors, gateways, and clouds. This approach will emphasize how data flows through systems while indicating areas prone to various forms of trust breaches such as compromised nodes receiving unauthorized instructions.



II. Background on Trust Management in IoT

Trust in IoT contexts is a changing, complex idea about how well devices work and stay safe. Unlike fixed security keys, confidence in a gadget's actions is continuously evaluated. The trust management process usually includes three key steps:

Trust computation: In this step, gather data to calculate a trust value. Direct observations of a node's behaviour such as packet forwarding success rate can be included in the data sources. Indirect recommendations from other nodes can also be part of the data sources. Reference: [3]. Trihono et al. conducted a Trust Computation Survey. [4] describes in detail how these techniques work.

Trust Propagation: Once trust information has been calculated, it should be distributed across the network. In either a central way or separate ways. Distributed models were discussed in the "Robust Trust" study by Awan et al. Allow nodes to judge their own trustworthiness, improving resistance to isolated failures.

Decision Making: Based on the trust score, a node determines if it should communicate with another node. Trust scores are usually combined into one number, and choices are determined by a set limit [3].

The given studies discuss several trust handling systems:

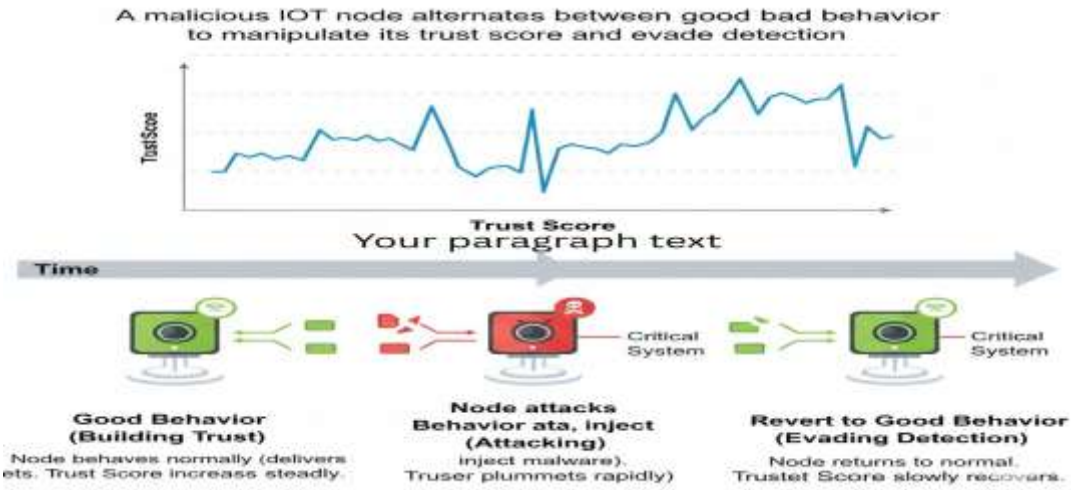
Lightweight Models: Lightweight models called LightTrust were developed by Ahmed et al. [6] designs energy-saving security systems for limited resources in industrial Internet of Things devices.

Game Theory Models: Rinki et al. used game theory models. [7] Show how game theory helps in modeling nodes' strategies, predicting and stopping bad actions**.**

Dynamic Models: The paper reviews dynamic trust management models in IoT networks using fuzzy logic techniques**.**

Figure 2: Illustration of Direct Trust Attacks (On-Off Attack)

This figure will focus on the "On-Off Attack," showing a malicious IoT node alternating between good and bad behavior to manipulate its trust score over time. It will depict a timeline or a series of states.



III. A Taxonomy of Trust Attack Mechanisms in IoT Networks

Trust attacks can be classified on the basis of how they manipulate the trust management system. We propose a classification with two primary categories: direct attacks and indirect attacks.

A. Direct attack

These attacks include a malicious node that directly affects your own behavior to manipulate your confidence score. The goal is to maintain either a higher trust score, while to disrupt the network by misbehaving or targeted.

On-off attack: This is a particularly clever attack where a malicious node is optional between good and bad behavior. It behaves well for a period to create a high trust score, then switchs to malicious activity (eg, leaving the packet) to create disruption, and finally to avoid good behavior to avoid being classified as untrue [9]. This becomes difficult to detect because its long -term average behavior may appear normal.

Packet dropping attack (Black Hole/Gray Hole): A malicious node simply leaves all (black hole) or some (gray hole) of the data packet which it has to be further. While a black hole attack is relatively easy to detect as the trust score score of the node, a gray hole attack is more subtle and difficult to identify.

Selective forwarding attack: A malicious node selectively forward packets, for example, to interrupt a particular communication link to topple the packets from specific sources or destinations. This is a more targeted version of gray hole attack.

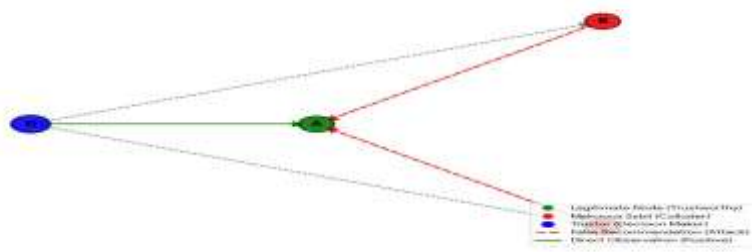
B. Indirect attack

The purpose of these attacks is to compromise the reputation system by providing false recommendations or by creating a web of malicious trust relationships. They exploit social aspects of faith management.

Good-Mouth/Bad-Mouth Attack: A malicious node provides extremely high (good-mouthe) or low (bad-mouth) TR.

Figure 3: Indirect Trust Attack - Sybil and Collusion (Bad-Mouthing)

This network graph illustrates how multiple compromised or Sybil nodes collude to degrade the reputation of a legitimate node, specifically using the Bad-Mouthing technique.



IV. Counter -opinion and mitigation strategies

Research papers offer several strategies to counter the trust attacks provided above:

Distributed and strong models: proposed by the "Robuststust" mechanism by avan et al. [5] Especially designed to oppose false recommendations. The system becomes less susceptible to the system CIBIL and good-mouth attacks, allowing the nodes to assess the trust locally and use a distributed laser.

Light and efficient algorithms: Trust assessment, especially in the energy-world sensor network, should be computationally light. "LightTust" Framework [6] by Khalil et al, and "a reliable Lightweight Trust Assessment Scheme".

Game Theory-Oriented approach*:* As discussed by Rinke et al. [[], The game theory trust may be a powerful tool for analysing and reducing attacks. By modeling interactions between nodes as games, it becomes possible to predict the behavior of rational attackers and design trust systems that encourage honest behavior. This can be particularly effective against on-off attacks by punishing incompatible behaviour.

Discrepancy detection and reputation filtering: Advanced Trust Models, often taking advantage of machine learning or statistical methods, can detect inconvenience that is characterized by trust attacks. For example, a model can track the variance in the trust score of the node over time to identify the uncertain behavior of the on-off attacker. Similarly, a trust management system can filter the recommendations from very low trust scores nodes, which can reduce the impact of poor-mouth attacks.

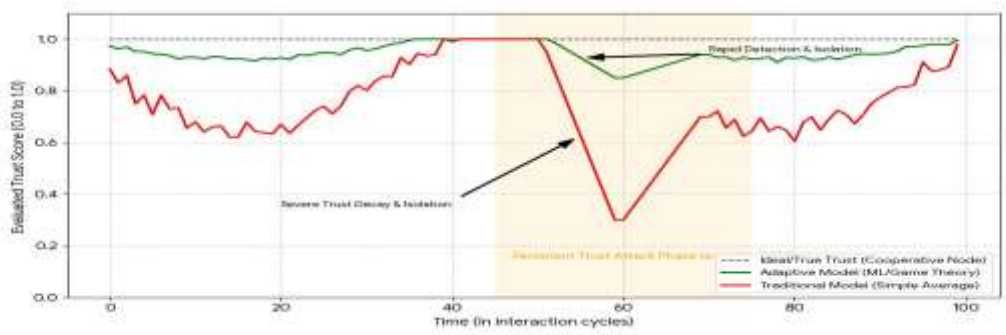
Multi-dimensional Trust Matrix*:* Trust should not be based on a metric. As suggested in various letters, a comprehensive trust model should consider several factors, including:

Direct Trust: Based on its interaction of a node:

- Indirect Trust: Based on the recommendations of reliable neighbors.
- Energy Trust: Trust depending on the energy levels of a node to prevent attacks on resource deficiency.
- Social Trust: Trust based on social relations or roles of a node within the network.

Figure 4: Comparative Effectiveness of Trust Countermeasures Under Attack

This conceptual line graph compares how different types of trust management models respond to a persistent trust attack over time.



V. Discussion and future work

Despite significant progress in trust management, many challenges remain. The first is scalability. Since the number of IOT devices is increasing rapidly, a trust management system should be able to handle millions or billions of nodes without excessive computational or communication overheads. The second is to detect the delay. Sophisticated attacks such as on-off attacks are designed to quickly detect, requiring a trust model that can learn from long-term behavior.

Future research should focus on the following areas:

AI/ML-Pied Trust Management: Application of deep teaching models to predict and detect trust attacks in real time. These models can analyze the complex patterns of behavior that are invisible to rules-based systems.

Blockchain for decentralized trusts: finding out how to provide a tampering-proof and decentralized bookkeeping for the information of the Blockchain Trust, possibly preventing attacks such as cIBIBIs and false recommendations by making the trust history irreversible.

Integrating the trust with physical-layer safety: Trust management is often a network-layer solution. Future work should be investigated how the trust can be integrated with physical-layer safety measures to create a stronger, multi-layered defense.

Figure 5: The Trust Management Trade-off: Security vs. Resources

This figure maps different trust management model categories based on two critical axes, visually defining the area where future research needs to focus:

- **X-Axis (Horizontal): Computational Overhead / Latency** (A proxy for resource consumption; lower is better).
- **Y-Axis (Vertical): Attack Detection Accuracy / Security** (Higher is better).

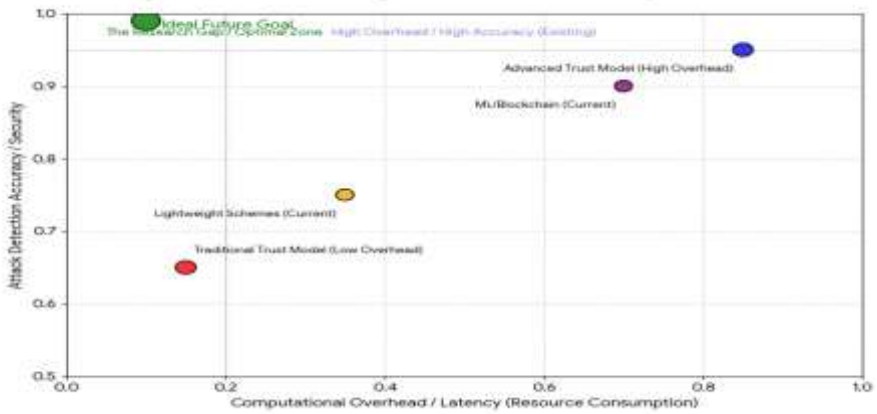


Table 1. Research on Trust in IoT Networks

Paper Title & Authors	Publication Year	Main Contribution	Key Attacks Discussed	Key Countermeasures Discussed
The Internet of Things: A survey (L. Atzori et al.)	2010	A foundational survey providing a broad overview of IoT, its vision, and research challenges, including the need for security and trust.	N/A (General IoT security threats mentioned, but not a trust-specific taxonomy)	N/A (General security goals outlined)
Trust Management Model in IoT: A Comprehensive Survey (Z. A. Soomro et al.)	2022	A detailed survey classifying trust management models by process, context, blockchain, and edge-based approaches. Discusses trust metrics.	On-Off Attack, Sybil Attack, Good-Mouth/Bad-Mouth Attack	Lightweight Trust Management, Blockchain-based Models, Decentralized Systems

A Survey Study on Trust-based Security in Internet of Things (A. Mohammed et al.)	2022	Focuses specifically on trust as a security mechanism. Classifies and compares trust-based schemes.	On-Off Attack, Sybil Attack, Dishonest Recommendation Attack	Reputation-Based Filtering, Anomaly Detection, Multi-metric Trust Models
Survey on Trust Calculation Methods in Internet of Things (Trihono et al.)	2020	Classifies trust calculation models for IoT systems based on metrics, sources, algorithms, and architectures.	N/A (Focus is on trust calculation methods, not attacks)	N/A (Discusses trust models themselves as a countermeasure)
RobustTrust - A Pro-Privacy Robust Distributed Trust Management Mechanism for Internet of Things (K. A. Awan et al.)	2019	Proposes a distributed trust management system that allows devices to assess trust locally and is robust against false recommendations.	False Recommendations, Sybil Attack	Distributed Trust Ledger, Local Trust Assessment
LightTrust: Lightweight Trust Management for Edge Devices in Industrial Internet of Things (J. Ahmed et al.)	2021	Introduces a lightweight trust management framework for resource-constrained edge devices in industrial IoT.	General attacks on trust management, On-Off Attack	Centralized Trust Agent, Lightweight Trust Algorithms, Energy-Efficient Schemes
A Reliable Lightweight Trust Evaluation Scheme for IoT Security (F. Khalil et al.)	2021	Proposes a lightweight trust evaluation scheme to mitigate malicious node behavior with a focus on energy efficiency.	Malicious Node Behavior, Packet Dropping	Energy-Efficient Algorithms, Behavioral Monitoring

Trust Evaluation for Light Weight Security... Game Theory Oriented Approach (Rinki et al.)	2019	Explores the use of game theory for trust evaluation in sensor-enabled IoT networks.	On-Off Attack, Malicious Behavior	Game Theory Modeling, Incentivizing Cooperative Behavior
Dynamic Trust Management Implementation in IoT: A Review Paper (Anonymous Review Paper)	2018	Discusses various trust models, including those that use fuzzy logic and a multi-phase distributed schema.	Malicious Nodes, Dishonest Recommendations	Fuzzy Logic, Multi-Phase Distributed Schemes
Towards Trustworthy Internet of Things (F. M. Ribeiro Junior et al.)	2021	A survey on the broader concept of trustworthiness (dependability) in IoT, covering resilience, security, and data trustworthiness.	N/A (Focus on general trustworthiness properties)	General Dependability Framework, Data Trustworthiness Mechanisms

VI. Result

A survey of definitions between the years 2010 and 2023 shows recurring, strong focus on trust management as a must-have field that is instrumental in providing security and reliability in IoT ecosystems. Varied research emphasizes a continued effort to classify existing trust models and identify open challenges in this area [2, 3, 10]. The principal technological focus in proposed methods includes the development of effective systems appropriate to be utilized by resource-constrained devices, leading to developments like LightTrust specifically for industrial Internet of Things (IIoT) settings [6], as well as several lightweight methods utilized in analyzing trustworthiness [9, 7]. Moreover, new methods indicate emphasis on resolving significant functional limitations by maximizing methodologies; robustness is resolved by decentralized strategies such as RobustTrust [5], while complex methods in the form of game theory provide accurate evaluation of trustworthiness [7]. Existing efforts continue to enrich these approaches by focusing on new trust administration techniques [11], and proposing safe but effective protocols seeking to protect networks as well as ensure data consistency in the face of such threats from malicious actors [4, 8]. Transition gradually takes place towards more tangible implementation strategies of distributed Internet-of-Things systems while maintaining flexibility, effectiveness, and security on different devices.

Table 2. The papers span a period from 2010 to 2023

Year Range	Reference Nos.	Observation
Early IoT (2010)	1	A fundamental, early survey defining the "Internet of factors," setting the stage for subsequent research.
Maturing Field (2018-2020)	4, 5, 7, 11	The bulk of the work, including the introduction of specific trust models (RobustTrust, Game Theory-oriented methods) and review papers consolidating early concepts.
Recent/Current Focus (2021-2023)	2, 3, 6, 8, 9, 10	A significant number of very recent publications. These comprise new overall surveys (Ref 2, 3, 10), application-oriented models (LightTrust for Edge/IIoT), and ongoing work on solid, lightweight schemes (Ref 9).

VII. Conclusion

The security of the Internet of Things largely relies on the safeguard of its trust management systems. As this letter has illustrated, the distinguishing attributes of the IOT network - i.e., their resource constraints, dynamic topology and large-scale - provide a fertile ground for a new segment of advanced cyber threats referred to as trust attacks. We have given an elaborate categorization which categorizes these attacks according to their working mechanisms, ranging from direct behavior manipulation to sabotage of reputation-based systems. The review of past studies shows that a multi-faceted approach has to be adopted to address these threats. Lightweight and decentralized trust models can mitigate the effect of single points of failure, and applications of sophisticated techniques, including game theory and fuzzy logic, offer promising directions to identify more precise and strong attacks. Nevertheless, critical issues persist. There are unsolved research issues between computational overhead and safety, need for scalability and detection of weak, long-term attacks. Future research would be aimed at the development of intelligent, self-learning models of trust that would be appropriate to derive attack strategies. Detection of the anomaly in the trust behavior is an area where machine learning and AI are particularly appropriate to integrate. Finally, making a robust IOT ecosystem is not just a technical challenge, but also a critical necessity for its widespread usage and its potential realization.

References

1. *L. Atzori, A. Iera, and G. Morabito, "The internet of factors: A survey," pc Networks, vol. 54, no. 15, pp. 2787-2805, 2010.*
2. *Z. A. Soomro et al., "accept as true with management model in IoT: A complete Survey," future generation pc structures, vol. 129, pp. 109-122, 2022.*
3. *A. Mohammed et al., "A Survey have a look at on consider-primarily based protection in net of factors: demanding situations and troubles," IEEE get right of entry to, vol. 10, pp. 19572-19590, 2022.*
4. *Trihono et al., "Survey on consider Calculation strategies in net of things," in Proc. of the global conference on Informatics, era and Engineering (InCITE), 2020.*

5. k. A. Awan et al., "RobustTrust - A pro-privacy sturdy dispensed accept as true with control Mechanism for net of factors," future era computer systems, vol. ninety-nine, pp. a hundred and ten-123, 2019.

6. J. Ahmed et al., "LightTrust: lightweight agree with control for side devices in business net of factors," in Proc. of the IEEE global conference on industrial internet of factors (ICIIoT), 2021.

7. Rinki et al., "trust evaluation for mild Weight safety in Sensor Enabled net of things: sport idea orientated method," magazine of community and laptop packages, vol. 131, pp. 91-102, 2019.

8. F. M. Ribeiro Junior and C. A. Kamienski, "towards trustworthy internet of factors," in Proc. of the IEEE global conference on Communications (ICC), 2021.

9. F. Khalil et al., "A reliable light-weight agree with evaluation Scheme for IoT protection," journal of data protection and programs, vol. 60, pp. 102875, 2021.

10. S. A. A. Hassan et al., "A Survey on IoT consider and popularity: A Survey and Taxonomy," IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1438-1463, 2023.

11. S. F. A. Doulah et al., "A Dynamic trust control Implementation in IoT: A review Paper," in Proc. of the global conference on electrical, pc and conversation Engineering (ECCE), 2018.