International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Trust Management Strategies in the Social Internet of Things: A Comprehensive Literature Review and Identification of Research Gaps

Shimaz Khan Shaik *[1], Sharifalillah Nordin [2], Mohamad Yusof Darus [3]

Submitted: 05/02/2024 **Revised**: 07/03/2024 **Accepted**: 18/03/2024

Abstract: This research paper presents a holistic study of the Trust Model in the context of the Social Internet of Things (SIoT) and its architectural components. It examines the importance of trust management in ensuring secure interactions among diverse nodes within SIoT networks. The paper researches various trust-related attacks that target the Trust Model and investigates the existing literature on mitigation techniques to counter these attacks effectively. Furthermore, the research analyzes the limitations of the current approaches, aiming to identify research gaps in trust management for SIoT. By evaluating the strengths and weaknesses of the existing work, this study lays the groundwork for future research directions in enhancing the Trust Model's resilience and adaptability in the rapidly evolving SIoT landscape. Through an in-depth analysis of trust, architecture components, attack scenarios, and mitigation strategies, this paper enhances comprehension of Trust Model dynamics in SIoT and offers valuable insights to guide further advancements in trust management and security for SIoT networks.

Keywords: *Trust Model, Social Internet of Things (SIoT), Architecture Components, Trust-related Attacks, Mitigation Techniques, Security, Research Gaps, Future Research Directions.*

1. Introduction

The IoT, a critical technology, connects a vast number of devices with processing, sensing, and actuating capabilities, enabling diverse applications in domains like home automation and healthcare[1]. IoT encompasses a wide array of objects, from self-driving cars to smartphones [2]. It involves connecting devices to collect and share data, generating "big data" analyzed for valuable insights [3][4]. However, growth brings challenges like connectivity, power consumption, interoperability, computational complexity, storage complexity, security, and trust issues [1]. Security is a critical concern in the IoT landscape, leading to privacy and economic concerns [2]. Securing communication among IoT devices is crucial before further deployment. Our society exhibits heterogeneity, dynamism, and complexity, with social connections forming groups based on factors like common interests, locations, and needs. Translating this idea of social networks into the Internet of Things (IoT) can effectively tackle challenges within the IoT ecosystem. The amalgamation of social features into the IoT has created a new concept referred to as the “Social Internet of Things (SIoT)”. SIoT involves establishing a “social network” that encompasses smart objects, services, or a blend of both. This concept is intended to fulfil the necessities of users, software developers, and designers[5][6]. Also, nodes offer and consume various services, allowing interaction with potential malicious nodes. Trust plays a vital role in ensuring secure and reliable information exchange between nodes[7]. It involves the trustor's willingness to rely on a trustee's promises, irrespective of their capability to observe or control the trustee, even with potential

1 Research Scholar, 2 Senior Lecturer, 3 Associate Professor College of Computing, Informatics, and Mathematics, Universiti Teknologi MARA, Malaysia
** Corresponding Author Email: shimazshimaz@gmail.com*

negative consequences[8]. Trust is characterized as the trustor's belief that the person or entity in the position of trustee will fulfil trusted goals as expected. Social relationships between owners and devices influence trust computation, with nodes considering direct experiences, social connections, and other factors to classify benevolent and malevolent nodes. The trust management model comprises various components and Trust features[9]. Node behaviour, feedback, social relationships, and other factors influence feature computation, and aggregating these features determines the node's trust value. Trust models in IoT security can be vulnerable to various security attacks [10]. When nodes are exposed to these attacks, they may provide false ratings for services or discriminate against certain nodes. Trust management becomes critical to ensure credible communication between nodes and the delivery of certified services with guaranteed security. To ensure an efficient trust model we need efficient detection and mitigation mechanisms for trust-related attacks [11]. Although significant contributions have been made in this area, there are still identified shortcomings [12] that must be addressed to enhance the trust model's resilience against such attacks. This research aims to address and overcome the challenges of current trust models within the realm of Social IoT. This study conducts a comprehensive literature review to examine the current challenges associated with trust management models aimed at ensuring the security of SIoT networks. The limited research in this area motivates the search for effective solutions to enhance the security of SIoT networks. The review specifically focuses on identifying and understanding various trust-related attacks that can compromise the reliability of SIoT systems, shedding light on the challenges faced in this domain. Overall, this research paper provides a valuable contribution by offering a comprehensive study of the architecture of the IoT "Trust model" and shedding light on the challenges and potential solutions to ensure secure and reliable IoT systems. The rest of the paper is organized as follows: 2:Taxonomy of IoT trust, 3: Related Works, 4: Discussion 5: Research Gaps, 6. Conclusion.

2. Taxonomy of IoT Trust

2.1 Social IoT

The IoT refers to intelligent objects incorporated with capabilities for sensing, computing, networking, actuation, allowing data collection and exchange. IoT is a key technology in smart cities, smart cars, advanced power grid systems, and healthcare. Social relationships exist in our heterogeneous society, forming groups founded on common goods, influence, and needs. The incorporation of "social networks" into IoT has led to the emergence of the SIoT concept [5][6].

*2.*2 Trust Management in IoT Security

In a distributed IoT network, the existence of malicious nodes introduces security risks, and depending merely on cryptographic algorithms or basic security controls may not be adequate to address some attacks. Therefore, Ensuring security in IoT necessitates trust management, which includes encouraging positive conduct, forecasting node actions to avert engagements with malicious nodes, and evaluating trust through historical behaviour and ratings provided by other nodes. Trust can be computed based on social and QoS attributes such as friendship, cooperativeness, connectivity, reliability, and good behaviour of a node[13]. Authors may offer varying definitions of trust, but the main focus of trust management is to enhance security and aid the process of decision-making. "Trust is the willingness to rely on another party, expecting them to act in a way that is important to the trustor" [14]. "Trust is also associated with the confident anticipation that one's weaknesses will not be exploited in an online risk situation" [15]. Trust Management is crucial for enhancing IoT security, and incorporating social attributes can further improve trust models. It consists of various components. These components work together to establish and maintain trust among IoT devices and networks. The vital elements of a typical "Trust Model" are enumerated in the following sub-sections.

2.3 Trust Composition

This defines what components have to be considered for trust computation. The components that are part of the "Trust Model" are classified into QOS-based and social-based.

QoS-based trust

In this model [16][17], an IoT device's trust value is calculated from its quality of service. Different metrics which are used to measure this model of trust are response time, reliability, interoperability, power consumption, error rates, availability rates, scalability

etc.

Social-based Trust.

Social-based trust in the "Social Internet of Things (SIoT) " refers to the incorporation of social notions and relationships into the trust management mechanisms of IoT systems. In this context, trust is not solely determined by technical aspects but is influenced by social interactions and relationships among entities within the IoT network[5][6]. These relationships are "Parent-OR", "Owner-OR", "Guardian-OR", "Social-OR", "Sibling-OR", "Guest-OR", "Service-OR", and "CoLocation-OR". Social-based trust considers factors such as direct experiences, feedback, and social connections between devices and users to assess the reliability and credibility of interactions. This approach recognizes that in a social context, individuals and devices may form communities or networks based on shared interests, influence, or other social factors. By incorporating social elements into trust computation, SIoT intends to enhance the overall security and reliability of IoT systems, considering not only technical aspects but also the dynamics of social relationships within the network.

2.4 Trust aggregation

During the trust aggregation phase, the features or attribute values derived in the trust composition phase are brought together. Various techniques, including " weighted sum, belief theory, Bayesian inference (with belief discounting), fuzzy logic, machine and deep learning, and regression analysis" [12], are employed to aggregate these derived values in the trust composition process.

2.5 Trust Update

Trust updates can be classified into event and time-driven types. Event-driven: In this scheme, an event or transaction would trigger the update of trust data in a node. Time-driven: in this scheme, trust observations are collected, aggregated & updated, periodically.

2.6 IoT Trust Placement Strategy or Trust Propagation

Centralized Trust

In this method, the trust will be directed through a central node or Trust Authority (TA), which is accessible to all other nodes within its designated domain. "The Trust Authority (TA) is responsible for overseeing diverse facets of trust information management, encompassing tasks such as trust negotiation, calculation, decision-making, and potentially assisting users by providing the necessary initial information required for trust computation" [18][19].

Distributed Trust

In this kind of trust, IoT nodes independently exchange the trust values among themselves without a centralized head unit. This can be classified into Direct and Indirect trusts [10], [21], [22].

2.7 Trust information collection

Direct Trust

A node observes a neighbour node directly and infers the trust evaluation based on its interaction as depicted in **Figure 1**, the neighbour's social behaviour, or the neighbour's attitude[20]. When there is no direct interaction between them then there is no trust value computed. Also, it computes the trust value on the neighbour node, locally and aggregates it with the learnt value from direct interaction to compute the final trust value[20].

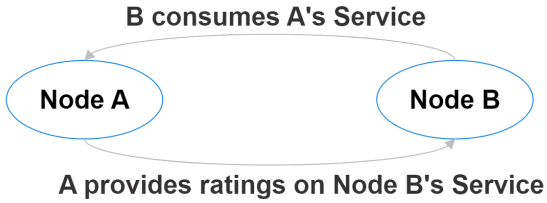

Fig 1 Direct Trust

Indirect trust

It refers to recommendations from third-party nodes. For example, as depicted in **Figure 2**, device, A computes the trust score of device, B from the endorsements of third-party nodes while node, A has no history of any transactions with node, B, before[9].

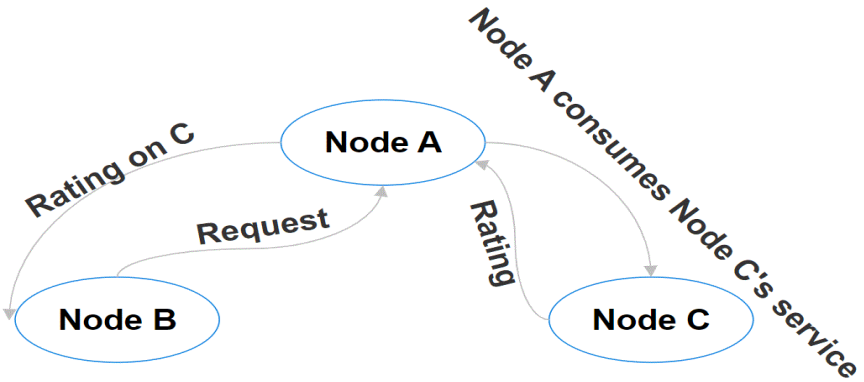

Fig 2. Indirect Trust

2.8 Characteristics of a Trust

Table -1 highlights key characteristics of trust [21][22] in the context of an IoT network. Trust is subjective, varying from one node's viewpoint to another, and can be either objectively measured or context-dependent. It is asymmetric, where trust may not be reciprocated between nodes. Trust is dynamic and can change over time, while transitive trust can exist among a set of nodes. Additionally, full trust is rare, as nodes typically exhibit varying levels of trust towards each other. Understanding these trust properties is crucial for designing secure and reliable IoT systems.

Table 1: Characteristics of Trust

Trust is subjective	The trust factor is subjective and varies depending on the trustor's viewpoint. For instance, device A might trust device B, whereas device C might decide to distrust B.
Trust is Objective	In the context of computational trust, trust factors can be assessed and tracked based on QoS.
Trust is Asymmetric	Trust does not exist bi-directional. For example, node A may trust B while B doesn't trust A.
Trust is Dynamic	Trust validity can be limited to a particular timeframe. For instance, node A may have trust in node B during period T1, whereas trust may not be present during a different period, T2.
Trust is Context Dependent	The trust values may differ significantly contextually. For example, node A may trust another node B in specific context C1 while it doesn't trust another context C2
There is no full trust	In most situations, a device's trust in another device is not complete
Trust is Transitive	Among the set of nodes in an IoT network, this property may exist as follows : o A trust B o B trust C o A Trust C

2.9 Trust-Related Attacks

There would be malevolent and benevolent nodes in the Social IoT or IoT network. The malevolent nodes try to attack the functionality of the IoT network by providing bad services and poor feedback scores for the benevolent nodes. The main attacks[12][9][23] that affect the Trust models in IoT security are given in **Table 2**.

Table 2: Trust-related attacks

Attack Name	Description
"Malicious with Everyone (ME)"	This is the most straightforward attack, and it serves as a benchmark for testing TMSs. A malicious node engages in malicious behaviour toward everyone, resulting in consistently poor suggestions and services, irrespective of the requester.
"Self-promotional attacks (SPA)"	Malicious nodes emphasize their importance by providing positive recommendation scores for themselves, aiming to be selected as service providers. However, they later provide poor services.
"Bad Mouthing Attack(BMA)"	Negative recommendations from malicious actors affect the standing of benevolent devices, diminishing their likelihood of being selected as service providers.
"Ballot stuffing attacks (BSA)"	Providing positive recommendations to enhance the reputations of misbehaving nodes raises the probability of them getting nominated as service providers.
"Whitewashing attack(WA)"	A malicious device can leave and join again in the network to eliminate its negative reputation.
"Discriminatory attacks (DA)"	A dishonest node could target individuals with weak social ties or those who are not friends, exploiting human behavior that tends to favor interactions with friends in social IoT systems.
Opportunistic Service Attack(OSA)	A deceitful node might provide exceptional service when it perceives a chance to enhance its reputation, particularly if it believes its standing is diminishing due to substandard service. When having a favorable reputation, it can collaboratively engage with other malicious nodes to execute tactics such as vote-stuffing and badmouthing.

3. Related Works

The history of "Trust management" in the IoT is given in the following section. The literature is currently extensive as a result of the numerous scholars who have studied this issue in recent years. We don't plan to cover all the studies that have been published; instead, we aim to highlight the models that the literature has found to be the most useful. The Literature review on related works is categorized into different categories as depicted in **Figure 3**.

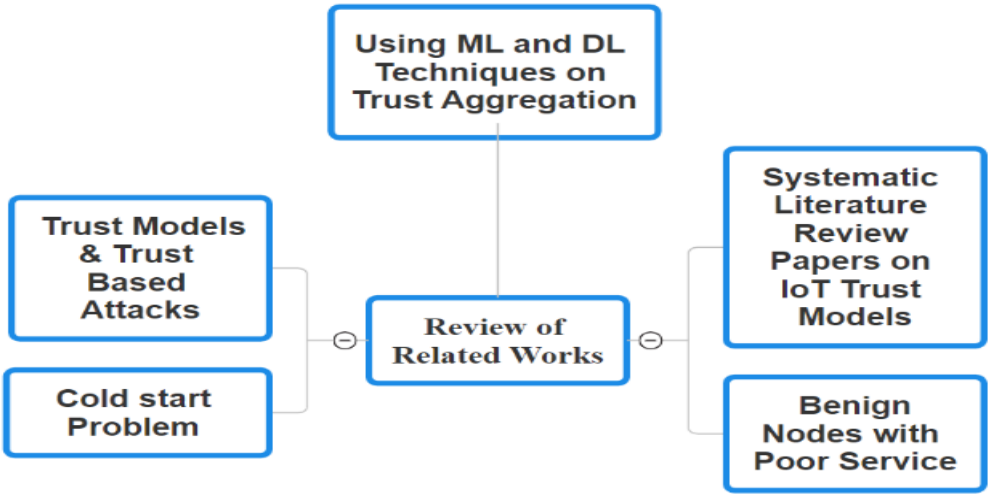

Fig 3: Categories of Related Works

3.1 Related Works on Trust Models and Trust-based Attacks.

The following section enumerates the related works based on Trust Models and Trust-based attacks. An efficient trust model is realized by (1) selecting the right features or attributes and composing efficient trust values for them and (2) efficient trust aggregation technique which shows resilience against trust-related attacks [7].

The paper [24] introduced a "Trust management approach based on a fuzzy reputation for the Internet of Things (IoT)". Nevertheless, their method focuses solely on detecting a particular IoT setting involving sensors and " (QoS)" trust indicators (forwarding/transfer ratio and energy usage, overlooking the crucial aspect of social interaction in social IoT systems

In their paper [19] the authors suggest subjective and objective "Trust Management" techniques for the SIoT. They consider features like centrality, object attributes, and various opinions over time. Trust aggregation uses a weighted sum approach. However, the paper notes the limitation of using centrality based on well-known friends to detect malicious nodes and highlights challenges in determining trust levels for newly connected nodes.

The trust management model [23] presents a method for managing trust in the SIoT. "Trust is calculated between objects through Direct Observations, Indirect Recommendations, Centrality, Energy, and Service ratings, employing a weighted sum for trust aggregation". While the model addresses on-off attacks, it has limitations in handling Sybil attacks, as discussed by the authors [13].

Distributed trust management scheme (DDTMS) is proposed in the paper [25] with a significant focus on identifying and mitigating on-off attacks (OOA) in the IoT. Doesn't mitigate other trust-related attacks. It uses the weighted sum for trust aggregation and the reward and punishment features for trust aggregation.

The study by the authors [26] identifies and safeguards against malicious behaviour in nodes, specifically targeting potential On-Off attacks in a multiservice Internet of Things. The proposed "Trust Management" approach utilizes direct information, transaction amounts, and node positions to establish trust, employing a weighted sum for trust aggregation.

The work [27] " implements a trust evaluation system in ad hoc networks for securing ad hoc routing and assisting malicious node detection". The attributes used for the trust composition are action trust, recommendation trust and forgetting factor. The probability statistics techniques are used for the trust aggregation and no explicit trust attack detection methods are discussed.

The paper [28] offers a trust evaluation module and implements authorization using artificial constraints. It uses the fuzzy-based evaluation matrix to compute the trust score based on predetermined policies.

The article [29] "suggests an adaptive Trust Management approach for service composition

applications in SOA-based IoT systems". Introducing a collaborative filtering system, it selects input based on similarity ratings tied to associations with friends, acquaintances, and communities. Addressing attacks by hostile nodes, "an adaptive filtering method dynamically blends direct and indirect trust to improve the accuracy in terms of time and bias". Privacy concerns arise from the need for devices to disclose friends' and location information. Challenges like the cold start problem and additional trust-related attacks are acknowledged.

The author [30] proposes a new technique that detects malevolent devices based on BMA, BSA, DA and SPA behaviour. The solution to the cold start problem and other trust-related attacks was not addressed. Multi-Layer Perceptron is used for trust aggregation. Features such as reputation, honesty, provider quality, similarity, rating frequency and direct experience are used.

The paper [31] provides a " Trust Management " scheme which decentralized and based on machine learning. It uses three novel parameters: " the goodness, usefulness score, and perseverance score". The suggested model has been tested against every sort of attack, except the SPA and SA. Unfortunately, no solution to the cold start issue, and it has not addressed all the attacks specific to the trust models.

The authors [32] propose "DATM", "a discriminative-aware trust management framework for SIoT service provisioning". This technique uses object ratings and a data mining model to compare service query contexts with past contexts. Trust convergence, determined with the weighted K-NN machine-learning technique, considers social similarity, energy level, and timestamp attributes. The framework identifies nodes causing attacks but lacks a solution for a new beginning node without transactions.

The paper [18] presents "IoT-HiTrust, a 3-tier hierarchical trust-based service management protocol for large-scale mobile cloud IoT systems". This protocol allows IoT clients to assess and submit subjective service trust scores. The approach mitigates various attacks but does not cover trust convergence upon node joining. Instead, it relies on features like direct and indirect rating, COI similarity, friends similarity, and social contact similarity, utilizing a weighted sum for trust aggregation.

Li, Song, and Zeng [33] introduce RealAlert, a secure sensing strategy for the Internet of Things. This policy-based approach assesses data and IoT device reliability using reporting history and context. Trust aggregation employs the Dampster Shafer theory of evidence (DST), countering BMA, BSA, and On-off attacks by identifying unusual network activity.

According to [34] an effective trust management system should have the following features: (1) Resistance to attack; (2) Overcoming the resource constraint ; (3) Avoiding failure with a centralized server ; (4) Overcoming data sparsity and cold start issue.

3.2 Related Works on Cold Start Problem

The "cold start issue" in the context of IoT Trust Models refers to a challenge that arises when a new device or node joins the network. In the initial stages, when the device has no prior history or interactions within the network, establishing trust becomes a complex task and the following section enumerates the related works on the cold start problem.

The paper [31]proposes a federated learning strategy to solve the cold-start issue. By keeping user data on their devices, privacy concerns are mitigated through distributed training. The method employs a dual deep Q learning scheduling strategy to calculate trust ratings for potential recommenders, aiding in the selection of optimal candidates based on trust and energy levels.

The paper [30] introduces a model for a trust-based system for SIoT, aiming to identify reliable service providers for each requestor while minimizing exposure to malicious nodes. It establishes a social network among requestor nodes using a flexible bipartite graph, creating a trust model based on node centrality and similarity metrics. The approach identifies trustworthy nodes, tackles data sparsity and cold start issues, and extracts latent information from SIoT nodes through matrix factorization

The study [32]presents a unique "Trust and Reputation model" for IoT, using "distributed probabilistic neural networks" to differentiate between reliable and malevolent devices. "It addresses the cold start issue by foreseeing ratings for newly connected devices over time". With distributed processing, it eliminates a single point of failure for improved availability. The model accommodates various IoT device types, providing different protection levels based on data sensitivity. Traditional collaborative filtering techniques in recommendation systems may yield

inaccurate results in cases where the closest neighbour hasn't assessed the anticipated item, contributing to issues like cold start and data sparsity.

The paper [33]proposes an advanced recommendation algorithm that boosts accuracy by incorporating users' social and trust ties. Integrating trust relationships based on familiarity and user reputation generates a trust score, and using social relationships and user preferences calculates a similarity score. The final prediction score is accurately determined by fusing the similarity and trust associations. This approach improves recommendation accuracy and addresses the drawbacks of traditional collaborative filtering techniques.

The paper [34] proposes TIRec, a lightweight trust inference model for IoT service recommendations. It integrates a weighted centrality measure to withstand attacks in choosing a trust path and computation algorithm. The model incorporates rating, direct trust, and indirect trust in a matrix factorization framework to forecast ratings, considering both trustee and trustor influence. This is the first attempt to incorporate a trust inference algorithm into trust-based recommendation systems

In article [35] , a trust-aware recommender system is introduced for social IoT applications. Trusted data is utilized to combat issues like opinion spam and enhance system accuracy. The method transforms trust measurements into a directional, weighted trust network, using a user-item rating matrix to create an implicit trust network. It aims to maximize trust with minimal social connection information, acknowledging the context sensitivity of social link information quantity and structure.

Paper [36] proposes two recommendation models tackling complete and incomplete cold start challenges for new items. Integrating collaborative filtering (CF) and deep learning neural networks, the models incorporate content features into the CF model, timeSVD++. Evaluated on a large Netflix dataset, results show effective performance, suggesting applicability to diverse recommender systems in social networking and online commerce.

The publication [37] introduces an SIoT architecture with a personalized recommendation mechanism to enhance service composition and discovery. Using the knowledge-desire-intention model, the recommender engine resolves the cold start issue early in the suggestion generation process, outperforming existing approaches with up to a 28% higher F-score in experiments and benchmarks on multiple datasets.

Paper [38] tackles the cold-start user issue in recommendation systems by introducing UIThybrid, a Hybrid Collaborative Filtering Recommendation technique integrating user trust into CF-based methods. The system strikes a balance between recommendation robustness, accuracy, and diversity, as evidenced by real-world trials on the Epinions dataset, showcasing UIThybrid's viability and effectiveness.

3.3 Distinguishing Benign Poor service from Malicious Nodes

The network nodes could be well-intentioned but may provide suboptimal service due to technical issues. While these nodes with inadequate service might be labelled as malicious in current literature, such misclassification could impact the precision of IoT Trust computation within the IoT Trust model.

Despite the development of intricate trust mechanisms to prevent unauthorized data alterations and detect felonious activity, the author [39] points out two critical aspects that remain inadequately addressed. Firstly, nodes in a network may provide inaccurate services intentionally or unintentionally. Secondly, requester nodes may struggle to assess the accuracy of the services they receive in terms of quality. The author argues that a trust system should consider service evaluation errors and distinguish attackers from poorly performing objects. The simulation results suggest that such situations do not necessitate sophisticated trust algorithms.

3.4 Related Works Using DL Techniques on IoT Trust

In this section, we examine research papers on the application of “Machine Learning and Deep Learning techniques” in the Trust Aggregation phase of IoT Trust computation. The studies highlight innovative approaches, emphasizing their impact on improving accuracy and efficiency in trust aggregation within the IoT.

The author [40] tackles security and trust issues in “Vehicle Ad Hoc Networks (VANETs) for the Internet of Vehicles (IoV)”. Their approach involves classifying cars as trustworthy or untrustworthy using machine learning techniques. Using a real IoT dataset, they compute a feature matrix for three parameters and employ machine-learning methods for vehicle classification. Simulation results show that mean

parametric score-based classification outperforms feature-based classification in accuracy.

A study [41] recommends "using trust as a metric to enhance security and reliability in Federated Learning (FL), a privacy-preserving machine learning paradigm". The proposed decentralized FL algorithm, based on a mathematical framework for trust computation in multi-agent systems, proves effective in addressing security and privacy challenges, including data poisoning attacks, in decentralized FL scenarios.

A new deep learning-based trust evaluation model is proposed using a "Multi-Layer Perceptron (MLP)" [26]. This approach can detect the type of attacks performed by malevolent nodes and isolate them from the network, achieving a more reliable atmosphere. Experimentation with accurate data shows promising results for the proposed system.

This paper [42] discusses a new TM model that "leverages Machine Learning (ML) techniques to detect and prevent malicious attacks by learning trust features derived from malicious nodes' behaviour descriptions". The study highlights the effectiveness of the proposed model by presenting the results of experiments with simulated datasets based on accurate data.

The proposed model [43] (DSL-STM) includes multidimensional metrics to describe SIoT entities' behaviour, aggregated using Machine Learning to classify users and detect and counter-attack types. "A hybrid propagation method is suggested to spread trust values in the network while preserving scalability and dynamism".

This study [44] proposes a "discriminative-aware trust management (DATM) system". DATM, utilizing entity ratings, employs a data mining algorithm that compares a service request's context with past queries, utilizing a weighted-kNN method to predict trust value. Variables like social similarity, service significance, and provider energy are considered. Simulations validate DATM's ability to detect self-erving behaviors and thwart trust-related threats, ensuring reliable services in the SIoT network.

This research[45] introduces a distinctive approach for identifying and eliminating attacks from hostile nodes in the network, known as the "Multi-hop Convolutional Neural Network with an attention mechanism (MH-CNN-AM)". Performance comparisons with existing methods are conducted based on metrics such as accuracy, precision, recall, F1-score, and MAE.

The paper [46] presents "a hybrid trust framework for Social IoT (SIoT), where IoT devices with social and behavioural attributes collaborate to deliver low-latency services and applications". The proposed framework employs "Probabilistic Neighborhood Overlap (P-NO)" to estimate tie strengths between nodes in a social graph created by human and machine social networks. This hybrid framework incorporates dynamic and static approaches for trust management, balancing resource overheads and benefiting from the higher accuracy of an active approach.

This study [47] proposes a "trust management model for IoT devices and services, combining the Long Short-Term Memory (LSTM) algorithm and the Simple Multi-Attribute Rating System (SMART)". SMART determines trust values, while LSTM identifies behavioural changes based on trust thresholds.

4. Discussion

4.1 Cold Start Issue

In this section, we examine the research papers on the cold start problem that addresses the nodes with no transaction history and newly joined in the network and these kinds of literature are summarized in **Table 3** such as matrix factorization, federated learning, social relationship and user preference calculations, two-way trust recommendation, asymmetric implicit trust network, collaborative filtering, deep learning, and hybrid collaborative filtering to mitigate the cold start issue in IoT.

No	Literature	Method used
1	[40]	Matrix Factorization Model
2	[41]	Federated learning-based approach
3	[42]	characteristics and learns over time

4	[43]	A recommendation system with bidirectional trust, known as TT-SVD, is introduced in AI-enabled IoT systems
5	[59]	In calculating the similarity score, factors such as social connections and user preferences are considered.
6	[44]	matrix factorization model
7	[45]	By employing a user-item rating matrix, the trust propagation metrics are transformed into a directed and weighted trust network within an asymmetric implicit trust network.
8	[46]	Collaborative Filtering and Deep Learning 2
9	[47]	Based Recommendation
10	[48]	knowledge–desire–intention model
11	[60]	The trust degree is computed, and prediction is made using multilayer perceptron (MLP) and generalized matrix factorization (GMF) with trust information
12	[49]	Hybrid Collaborative Filtering Recommendation approach with User-Item-Trust Records (UIThybrid),

4.2 Trust Aggregation Techniques

This section discusses the works of literature on trust aggregation techniques and it is summarized in **Table 4**. The techniques used in the studies include dynamic mathematical formula, weighted sum, weighted K-nearest neighbour (K-NN), Dempster-Shafer theory of evidence (DST), multi-layer perceptron (MLP), Bayesian technique, fuzzy evaluation matrix, and iSVM machine learning algorithms.The studies were conducted by different authors and published in different years, ranging from 2015 to 2023. The table gives an overview of the research studies and the techniques used in them, which can be useful for researchers looking for references and ideas for their studies. Trust aggregation is an important issue in the IoT, as it involves combining trust values from multiple sources to make decisions about the trustworthiness of devices and data. The techniques listed in the table can help to address this issue by providing different approaches for aggregating trust values, such as using mathematical formulas, machine learning algorithms, or fuzzy logic.

Table 4: Trust Aggregation techniques in existing works

No	Trust Aggregation Techniques	Literature
1	Dynamic Mathematical formula	[7]
2	Weighted Sum	[13] [10] [18] [19] [25] [27]
4	Weighted K-NN	[44]
6	Dempster-Shafer Theory of evidence (DST)	[24]
9	Multi Layer Perceptron	[26]
11	Bayesian technique	[28]
12	Fuzzy Evaluation Matrix	[29]
13	iSVM Machine Learning Algorithms	[48]

4.3 Features Used in the Existing Works

IoT Trust composition is the process of combining trust evaluations of multiple IoT devices or components to create a composite trust value. This process involves several attributes that contribute to the trustworthiness of an IoT device or component. Many different attributes have been proposed in the literature study as described in **Table 5**, including centrality, object characteristics/capabilities, cooperativeness, honesty, friendliness/social similarity, COI similarity, location similarity, amount of transactions, recommendations, direct observations,

long-term opinion, short-term opinion, energy consumption, punishment score, policy-based, reputation, quality of provider, perseverance score, and timestamp. However different literature uses different attributes in their work.

Table 5 : Features/ Attributes Used in Existing Works

No	Literature	Centrality	Object Characteristics/capabilities	Cooperativeness	Honesty	Friendliness /Social	COI similarity	Location Similarity	Amount of Transactions	Recommendations	Direct Observations	Long Term opinion	Short Term Opinion	Energy Consumption	Punishment score	Policy-based	Reputation	Quality of Provider	Perseverance Score	Timestamp
1	[7]	×	×	✓	✓	✓	✓	✓	×	✓	✓	×	×	×	×	×	×	×	×	×
2	[13]	×	×	✓	×	×	✓	×	×	×	✓	×	×	✓	×	×	×	×	×	×
3	[10]	✓	×	✓	×	×	✓	×	×	✓	✓	×	×	✓	×	×	×	×	×	×
4	[44]	×	×	×	×	✓	×	×	×	×	×	×	×	✓	×	×	×	×	×	✓
5	[18]	×	×	×	×	✓	✓	✓	×	✓	✓	×	×	×	×	×	×	×	×	×
6	[24]	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
7	[19]	✓	✓	×	×	×	×	×	×	✓	✓	✓	✓	×	×	×	✓	✓	×	×
8	[25]	×	×	×	×	×	×	×	×	×	✓	×	×	×	✓	×	×	×	×	×
9	[26]	×	×	×	✓	×	×	×	✓	×	✓	×	×	×	×	×	✓	✓	×	×
10	[27]	×	×	×	×	×	×	✓	✓	×	✓	×	×	×	✓	×	×	×	×	×
11	[28]	×	×	✓	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×
12	[29]	×	×	×	×	×	×	×	×	×	×	×	×	×	×	✓	×	×	×	×
13	[48]	×	✓	×	×	✓	×	×	×	✓	×	✓	✓	×	×	×	×	×	✓	×
14	[30]	✓	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×	×

4.4 Mitigation and Detection of Trust-Related Attacks

Table 6 lists various literature on trust attacks, which are attacks designed to manipulate trust relationships in networks. The table includes information on the presence of different types of attacks, such as "BSA (Ballot Stuffing Attack), BMA (Bad Mouthing Attack), DA (Discretionary Attack), OSA (Opportunistic Service Attack), SPA (Self-Promoting Attack), OOA (On-Off Attack), WA (Whitewash Attack), and SA (Sybil Attack)". The table also includes information on whether the literature discusses trust attacks or not. In addition, the table shows the presence or absence of trust metrics, such as trust evaluation methods or trust models. Overall, the table provides an overview of different literature on trust attacks and their focus on various aspects of trust metrics and trust attacks.

Table 6: Literature Review on Trust-Related Attacks										
		Attack Mitigation								Node Ranking
No	Literature	BSA	BMA	DA	OSA	SPA	OOA	WA	SA	
1	[7]	✓	✓	✓	×	✓	×	✓	×	×
2	[13]	×	×	×	×	×	×	×	✓	×
3	[10]	×	×	×	×	×	✓	×	×	×
4	[44]	✓	✓	×	✓	✓	×	×	×	×
5	[18]	✓	✓	✓	×	✓	×	×	×	✓
6	[24]	✓	✓	×	×	×	✓	×	×	×
7	[19]	×	×	✓	×	✓	✓	×	×	×
8	[25]	×	×	×	×	×	✓	×	×	×
9	[26]	✓	✓	✓	×	✓	×	×	×	×
10	[27]	×	×	×	×	×	✓	×	×	×
11	[28]	×	×	×	×	×	×	×	×	×
12	[29]	×	×	×	×	×	×	×	×	×
13	[30]	✓	✓	×	✓	✓	×	✓	×	×

5. Research Gaps

This section summarizes the research gap in the studied literature papers and is given in **Table 7**. Social Internet of Things (IoT) systems, also denoted as Social IoT, represent a novel integration of social networking and IoT technologies. These systems enable social interactions, collaborations, and user sharing, creating new opportunities for connecting people and devices to work together towards common goals. However, this integration also introduces significant challenges in establishing trust among users and devices within these systems. Trust is crucial in any IoT system, as it forms the foundation for users to rely on the system's functionality and share sensitive data. Many trust models are designed to establish trust between nodes, with a focus on social and Quality of Service (QoS) aspects. Nonetheless, certain attacks specifically target these trust models [12][9][23]. This study examines the limits of existing trust models in Social IoT and explores the necessity for new models that can incorporate social factors.

Table 7: Research Gaps Identified

No.	Research Gap Identified
1	Only a subset of attacks have been identified or mitigated in the existing literature
2	Due to variations in features considered and the weights assigned to each feature depending on the attack type, the weighted mean may not detect all attacks.
3	Most works propose trust models for the general IoT architecture without considering the social attributes
4	Sometimes, a service-providing node may have benevolent intentions but cannot offer a satisfactory service due to errors or malfunctions. Similarly, a benevolent node may not be able to accurately evaluate a service provider due to a lack of information about the service offered. Still, as per the existing trust models, these nodes are considered malicious nodes
5	When a node joins the network as a new node, this scheme fails to detect the malicious nodes in the beginning stage.[Cold start Issue]

6. Conclusion

In our research, we have conducted a thorough review of previous works related to the SIoT and its Trust Model. Our report covers a comprehensive analysis of SIoT, delving into its background research and the Trust Model it incorporates. We have outlined the various components of the Trust Model and discussed potential Trust-related attacks that could disrupt SIoT's Trust Model. Furthermore, we have conducted a literature review to examine the various techniques used for Trust composition and aggregation. In this research, we extensively analysed the existing system and highlighted its limitations and weaknesses in terms of Trust composition and aggregation. We have also scrutinized current literature and synthesized our findings, with a particular focus on addressing the "cold start" issue and distinguishing between benevolent but poor service nodes and malicious nodes. Additionally, our study explores the application of various Machine Learning (ML) and Deep Learning (DL) techniques in Trust aggregation. Lastly, we have investigated the weaknesses in the existing literature related to solving these issues. In summary, our report offers a comprehensive analysis of the Social IoT and its Trust Model, along with extensive research to identify weaknesses and limitations in the current system. The literature review would help the researchers to identify the research gaps and contribute novel orks in this domain to strengthen IoT security.

References

[1] K. Balasubramanian, *Building blocks for the internet of things*, vol. 9. 2014.

[2] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," *Proc. - 2015 IEEE World Congr. Serv. Serv. 2015*, pp. 21–28, 2015, doi: 10.1109/SERVICES.2015.12.

[3] "IoT," 2016. https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/ (accessed Feb. 11, 2020).

[4] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep learning for IoT big data and streaming analytics: A survey," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 4, pp. 2923–2960, 2018, doi: 10.1109/COMST.2018.2844341.

[5] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343–357, 2015, doi: 10.1109/ACCESS.2015.2416657.

[6] A. Khelloufi *et al.*, "A Social-Relationships-Based Service Recommendation System for SIoT Devices," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1859–1870, 2021, doi: 10.1109/JIOT.2020.3016659.

[7] I. R. Chen, F. Bao, and J. Guo, "Trust-Based Service Management for Social Internet of Things Systems," *IEEE Trans. Dependable Secur. Comput.*, vol. 13, no. 6, pp. 684–696, 2016, doi: 10.1109/TDSC.2015.2420552.

[8] Z. M. Aljazzaf, M. A. M. Capretz, and M. Perry, "Trust-based Service-Oriented Architecture," 2016.

[9] W. Najib, S. Sulistyo, and Widyawan, "Survey on trust calculation methods in internet of things," *Procedia Comput. Sci.*, vol. 161, pp. 1300–1307, 2019, doi: 10.1016/j.procs.2019.11.245.

[10] A. M. Kowshalya and M. L. Valarmathi, "Trust Management in the Social Internet of Things," *Wirel. Pers. Commun.*, vol. 96, no. 2, pp. 2681–2691, 2017, doi: 10.1007/s11277-017-4319-8.

[11] W. Abdelghani, C. A. Zayani, I. Amous, and F. Sèdes, "Trust Evaluation Model for Attack Detection in Social Internet of Things," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11391 LNCS, no. 18, pp. 48–64, 2019, doi: 10.1007/978-3-030-12143-3_5.

[12] M. S. Roopa, S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions," *Comput. Commun.*, vol. 139, no. September 2018, pp. 32–57, 2019, doi: 10.1016/j.comcom.2019.03.009.

[13] A. Meena Kowshalya and M. L. Valarmathi, "Dynamic trust management for secure communications in social internet of things (SIoT)," *Sadhana - Acad. Proc. Eng. Sci.*, vol. 43, no. 9, 2018, doi: 10.1007/s12046-018-0885-z.

[14] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An Integrative Model of Organizational

Trust Author (s): Roger C . Mayer , James H . Davis and F . David Schoorman Published by : Academy of Management Stable URL : http://www.jstor.com/stable/258792 REFERENCES Linked references are available on JSTOR f," *Acad. Manag. Rev.*, vol. 20, no. 3, pp. 709–734, 1995.

[15] C. L. Corritore, B. Kracher, and S. Wiedenbeck, "On-line trust: Concepts, evolving themes, a model," *Int. J. Hum. Comput. Stud.*, vol. 58, no. 6, pp. 737–758, 2003, doi: 10.1016/S1071-5819(03)00041-7.

[16] W. Viriyasitavat, L. Da Xu, Z. Bi, D. Hoonsopon, and N. Charoenruk, "Managing QoS of Internet-of-Things Services Using Blockchain," *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 6, pp. 1357–1368, 2019, doi: 10.1109/TCSS.2019.2919667.

[17] M. S. · G. B. · A. K. Tripathi1, "QoS-Aware Selection of IoT-Based Service.pdf." 2020.

[18] I. R. Chen, J. Guo, D. C. Wang, J. J. P. Tsai, H. Al-Hamadi, and I. You, "Trust-Based Service Management for Mobile Cloud IoT Systems," *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 1, pp. 246–263, 2019, doi: 10.1109/TNSM.2018.2886379.

[19] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, 2014, doi: 10.1109/TKDE.2013.105.

[20] N. B. Truong and G. M. Lee, "A Survey on Trust Computation in the Internet of Things," no. April 2017, 2016.

[21] M. S. Tyrone Grandison, " A Survey of Trust in Internet Applications," *IEEE Commun. Surv. Tutorials, Fourth Quart.*, pp. 1–30, 2000.

[22] I. Pranata, G. Skinner, and R. Athauda, "A holistic review on trust and reputation management systems for digital environments," *Int J Comput Inf Technol*, vol. 01, no. 01, pp. 44–53, 2012, [Online]. Available: http://ijcit.com/archives/volume1/issue1/Paper010106.pdf.

[23] A. M. Kowshalya and M. L. Valarmathi, "Trust Management in the Social Internet of Things," *Wirel. Pers. Commun.*, vol. 96, no. 2, pp. 2681–2691, 2017, doi: 10.1007/s11277-017-4319-8.

[24] W. Li, H. Song, and F. Zeng, "Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 716–723, 2018, doi: 10.1109/JIOT.2017.2720635.

[25] S. W. A. Hamdani, A. W. Khan, N. Iltaf, J. I. Bangash, Y. A. Bangash, and A. Khan, "Dynamic distributed trust management scheme for the Internet of Things," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 29, no. 2, pp. 796–815, 2021, doi: 10.3906/ELK-2003-5.

[26] M. M. B, W. Abdelghani, and I. Amous, "Deep Learning for Trust-Related Attacks," vol. 1, pp. 389–404, 2020, doi: 10.1007/978-3-030-34986-8.

[27] C. V. L. Mendoza and J. H. Kleinschmidt, "Mitigating on-off attacks in the internet of things using a distributed trust management scheme," *Int. J. Distrib. Sens. Networks*, vol. 2015, 2015, doi: 10.1155/2015/859731.

[28] F. Bao, I. R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based internet of things systems," *Proc. - 2013 11th Int. Symp. Auton. Decentralized Syst. ISADS 2013*, 2013, doi: 10.1109/ISADS.2013.6513398.

[29] J. Wang, H. Wang, H. Zhang, and N. Cao, "Trust and Attribute-Based Dynamic Access Control Model for Internet of Things," *Proc. - 2017 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2017*, vol. 2018-Janua, pp. 342–345, 2017, doi: 10.1109/CyberC.2017.47.

[30] S. Aalibagi, H. Mahyar, A. Movaghar, and H. E. Stanley, "A Matrix Factorization Model for Hellinger-Based Trust Management in Social Internet of Things," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 4, pp. 2274–2285, 2022, doi: 10.1109/TDSC.2021.3052953.

[31] O. A. Wahab, G. Rjoub, J. Bentahar, and R. Cohen, "Federated against the cold: A trust-based federated learning approach to counter the cold start problem in recommendation systems," *Inf. Sci. (Ny).*, vol. 601, pp. 189–206, Jul. 2022, doi: 10.1016/J.INS.2022.04.027.

[32] S. Asiri and A. Miri, "An IoT trust and reputation model based on recommender systems,"

2016 14th Annu. Conf. Privacy, Secur. Trust. PST 2016, pp. 561–568, 2016, doi: 10.1109/PST.2016.7907017.

[33] C. Ju, J. Wang, and C. Xu, "A novel application recommendation method combining social relationship and trust relationship for future internet of things," *Multimed. Tools Appl.*, vol. 78, no. 21, pp. 29867–29880, 2019, doi: 10.1007/s11042-018-6604-2.

[34] B. Cai, X. Li, W. Kong, J. Yuan, and S. Yu, "A Reliable and Lightweight Trust Inference Model for Service Recommendation in SIoT," *IEEE Internet Things J.*, vol. 9, no. 13, pp. 10988–11003, 2022, doi: 10.1109/JIOT.2021.3125347.

[35] J. Son, W. Choi, and S. M. Choi, "Trust information network in social Internet of things using trust-aware recommender systems," *Int. J. Distrib. Sens. Networks*, vol. 16, no. 4, 2020, doi: 10.1177/1550147720908773.

[36] J. Wei, J. He, K. Chen, Y. Zhou, and Z. Tang, "Collaborative filtering and deep learning based recommendation system for cold start items," *Expert Syst. Appl.*, vol. 69, pp. 1339–1351, 2017, doi: 10.1016/j.eswa.2016.09.040.

[37] G. X. Lye, W. K. Cheng, T. B. Tan, C. W. Hung, and Y. L. Chen, "Creating personalized recommendations in a smart community by performing user trajectory analysis through social internet of things deployment," *Sensors (Switzerland)*, vol. 20, no. 7, pp. 1–28, 2020, doi: 10.3390/s20072098.

[38] F. Wang *et al.*, "With User-Item-Trust Records," pp. 1–11, 2021.

[39] C. Marche and M. Nitti, "Can We Trust Trust Management Systems?," *IoT*, vol. 3, no. 2, pp. 262–272, 2022, doi: 10.3390/iot3020015.

[40] S. A. Siddiqui, A. Mahmood, W. E. Zhang, and Q. Z. Sheng, "Machine learning based trust model for misbehaviour detection in internet-of-vehicles," *Commun. Comput. Inf. Sci.*, vol. 1142 CCIS, pp. 512 – 520, 2019, doi: 10.1007/978-3-030-36808-1_56.

[41] A. Gholami, N. Torkzaban, and J. S. Baras, "Trusted Decentralized Federated Learning," 2022, doi: 10.1109/CCNC49033.2022.9700624.

[42] R. Magdich, H. Jemal, C. Nakti, and M. Ben Ayed, "An efficient Trust Related Attack Detection Model based on Machine Learning for Social Internet of Things," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 2021, pp. 1465–1470, doi: 10.1109/IWCMC51323.2021.9498808.

[43] W. Abdelghani, I. Amous, C. A. Zayani, F. Sèdes, and G. Roman-Jimenez, "Dynamic and scalable multi-level trust management model for Social Internet of Things," *J. Supercomput.*, vol. 78, no. 6, pp. 8137–8193, 2022, doi: 10.1007/s11227-021-04205-5.

[44] B. Jafarian, N. Yazdani, and M. Sayad Haghighi, "Discrimination-aware trust management for social internet of things," *Comput. Networks*, vol. 178, p. 107254, 2020, doi: 10.1016/j.comnet.2020.107254.

[45] R. Mohan Das *et al.*, "A novel deep learning-based approach for detecting attacks in social IoT," *Soft Comput.*, vol. 1, 2023, doi: 10.1007/s00500-023-08389-1.

[46] N. Narang and S. Kar, "A hybrid trust management framework for a multi-service social IoT network," *Comput. Commun.*, vol. 171, pp. 61–79, 2021, doi: https://doi.org/10.1016/j.comcom.2021.02.015.

[47] Y. Alghofaili and M. A. Rassam, "A Trust Management Model for IoT Devices and Services Based," 2022.

[48] C. Marche and M. Nitti, "Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 3, pp. 3297–3308, 2021, doi: 10.1109/TNSM.2020.3046906.