

A Review on Efficient Trust Computational and Evaluation Based on Machine Learning

Anil Kumar, Abhay Bhatia, Sunil Kumar



Abstract: These days, machine learning (ML) models are used across many complex fields, including bioinformatics, medicine, and other disciplines. Their black-box nature, however, may make it difficult to understand and trust the outcomes they provide. As a result, there is now a greater need for trustworthy visualisation tools to promote confidence in machine learning models. This topic has gained popularity in the visualisation community over the past few decades. To offer an overview of current research on the subject, as well as the frontiers of that study. The Internet of Things (IoT) enables billions of objects, in both physical and virtual contexts, to intelligently communicate with one another. Smartphones, for example, have evolved into valuable personal assistants and an integral part of people's daily lives and work. Machine learning, such as reinforcement learning and deep learning, is increasingly commonly used in IoT to improve performance and efficiency. Machine learning, on the other hand, has several flaws that could jeopardise the security, trust, and privacy of IoT environments. One of the most serious threats is adversarial learning, in which attackers try to trick the learning algorithm with carefully crafted training examples, leading to incorrect outputs. This Special Issue will feature cutting-edge research from academia and industry, with a focus on debates over the security, trust, and privacy issues in machine learning-based IoT.

Keywords: ML, Internet of Things, Trust Evaluation Methods, Trust Management System (TMS).

Nomenclature:

ILP: Integer Linear Programming

TMS: Trust Management System

ML: Machine Learning

P2P: Peer-To-Peer

TMs: Trust Models

DTM: Data-Oriented Trust Models

ETM: Entity-Oriented Trust Models

HTM: Hybrid Trust Models

HMI: Human-Machine Interaction

M2M: Machine-To-Machine

I. INTRODUCTION

Trust assessment is the process of figuring out how much you can trust someone based on how they act and what other trustworthy people do. It has been widely used as a decision-making tool across a range of fields. A trust assessment in a sensor network that identifies "rogue nodes" could help ensure the network is safe. When users of a social network use trust assessment, it makes it easier for them to make friends, reduces the risks associated with social activities, and improves the overall quality of social networking. When studying e-commerce, researchers often use trust assessment to help them choose which services to study. In a multi-agent system, trust evaluation ensures that automated agents can communicate safely and that automation works more effectively. Trust assessment is helpful in peer-to-peer (P2P) networking in several ways, such as finding objects that interact with each other, sharing resources with friendly peers, and protecting against malicious peers. Service requesters can use trust assessments to help them choose exemplary services from among many applicants. Given this, it is best to follow a research-based approach when conducting a trust assessment.

There are now several surveys that rate trust. This article provides an overview of the trust and reputation system used in online transactions, describes how to assess trustworthiness, and presents current trust management strategies and trust assessment methods for the Internet of Things (IoT). Trust assessment strategies for managing services for the Internet of Things were examined. Research on assessing the trustworthiness of web services provided an overview of several approaches to evaluating the trustworthiness of open multi-agent systems. It examined methods for determining whether an online transaction is trustworthy. Here are some ways to determine whether a website is reliable. In their most recent paper [14], they provided an overview of the various approaches to evaluating trust in cross-cloud alliances. Although the above literature offers a summary of approaches to assessing trust across multiple situations, it lacks a review of machine-learning-based trust assessment techniques.

Most traditional ways to measure trust are based on the amount of contact between a trustee and a trust, both direct and indirect. On the other hand, conventional ways of judging trust don't work if the person giving the trust and the person receiving it have never spoken before. But sometimes the data used to judge trust is only part of the story, and the evaluation method misses other essential facts. This makes a big difference in the accuracy of trust evaluations. On the other hand, the vast majority

Manuscript received on 24 October 2025 | First Revised Manuscript received on 28 October 2025 | Second Revised Manuscript received on 02 November 2025 | Manuscript Accepted on 15 November 2025 | Manuscript published on 30 November 2025.

*Correspondence Author(s)

Dr. Anil Kumar*, Associate Professor, Department of Computer Science & Engineering, Roorkee Institute of Technology, Roorkee (Uttarakhand), India. Email ID: chauhananil01@gmail.com, ORCID ID: [0000-0002-8918-3004](https://orcid.org/0000-0002-8918-3004)

Dr. Abhay Bhatia, Associate Professor, Department of Computer Science & Engineering, Roorkee Institute of Technology, Roorkee (Uttarakhand), India. Email ID: dhawan.abhay009@gmail.com, ORCID ID: [0000-0001-7220-692X](https://orcid.org/0000-0001-7220-692X)

Dr. Sunil Kumar, Professor, Department of Information Technology, Ajay Kumar Garg Engineering College, Ghaziabad (U.P.), India. Email ID: sunilymca2k5@gmail.com, ORCID ID: [0000-0001-5444-8175](https://orcid.org/0000-0001-5444-8175)

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open-access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

of traditional ways to measure trust combine different aspects of trust, account for weighting, and perform other calculations as needed. But figuring out the weights is hard, which makes it hard to judge things correctly. To address these problems, several experts have suggested using machine learning to improve the accuracy and robustness of trust evaluations.

Due to the rapid growth of internet services, social networking, and mobile communications, the amount of information used to judge a person's level of trust is bound to increase. Over the last few years, "big data" has become a topic of growing interest among academics and businesspeople. It looks different in many ways, including, but not limited to, speed, volume, value, variety, and truthfulness (5V). Big data is complex, multidimensional, and constantly evolving. This makes it hard to do a trust assessment in a real, chaotic, and brilliant environment. Big data is often used in large-scale distributed computing scenarios such as social networking, ubiquitous computing, peer-to-peer networking, and grid computing. Grid computing and peer-to-peer networking are two other examples. Because there is a lot of data and it is hard to understand how it is organised, traditional ways of assessing trust don't work well for computing trust values that can be evaluated using oversized data methods. Machine learning is one of the most important and widely used methods for

handling large amounts of data—the Characteristics of Trust. - The transdisciplinary concept of trust is difficult to describe. At its core, trust may be seen as a belief or a judgment. According to [13], it is an entity's subjective expectations about the future behaviour of other entities. The concept of "trust" is understood differently by different scholars. Although there are many definitions of trust across domains, the following characteristics of trust are universal: subjectivity, dynamism, context-awareness, partial transitivity, temporal decay, asymmetry, and measurability. Methods used in the past to evaluate trust are known as trust evaluation methods. The process of assessing trust using characteristics that impact trust is called trust evaluation. There is not one single approach that can be used to determine trustworthiness across all program parameters. The majority of conventional trust evaluation methodologies focus on trust-related characteristics during the trust assessment. The following are some models that may be used for evaluation; however, this list is not exhaustive: Models based on the mean with subjective Bayesian inference logic (weighted), a theory attributed to Dempster and Shafer. Examples of fuzzy logic include cloud models, game theory, fuzzy cognitive maps, information entropy models, and fuzzy logic itself.

Table I: Traditional Trust Evaluation Methods

	Advantages	Disadvantages
Bayesian Inference	The approach is straightforward and uses Bayesian inference to determine probabilities to express trust value.	Erroneously contrasting the unpredictability of chance with the subjectivity and uncertainty of trust.
Dempster-Shafer Theory	Having a good representation of uncertainty is sufficient; knowing the a priori probability is not necessary.	The data have to be completely separate from one another, and the notion of synthetic rules is flawed.
Fuzzy Logic	A practical approach to the murky issue of trust.	Formulating regulations and assigning membership responsibilities might prove challenging.
Subjective Logic	Include the subjective aspect, and make trust reasoning and complete computation easier.	Building operators is a challenging endeavour.
Entropy-based model	When conveying the unpredictability of trust relationships, information entropy is a valuable tool.	Inadequate assessment of the issues that might impact one's ability to trust.
Game Theory	The theory of games is quite comprehensive, but it also accounts for the degree of information. This brings the theory's outcomes very close to actual events.	It is not easy to devise the guidelines for playing the game.
Cloud-based	It describes the uncertainty of trust and completely incorporates ambiguity and randomness.	Cloud theory is frequently used in trust combination and transfer calculations. Using it to determine trustworthiness based on trust evidence remains challenging.

Table 1 outlines the benefits and drawbacks of several traditional approaches to evaluating a company's trustworthiness [12]. Although these approaches can evaluate trust, they also impose rigorous constraints on the use of formal mathematics in the assessment process. It may be challenging to put the models into practice at times. The selection of trust-related traits and the development of rules governing their use significantly affect the reliability of trust assessments. For the most part, static data analysis (such as exploratory and confirmatory factor analysis [4]) and literature reviews are used in prior work to justify. When it comes to selecting trust impact factors and building rules, it lacks intelligence and dynamic assistance.

A During the trust evaluation process, several different existing approaches use linear aggregation to combine the results of multiple trust-impact attributes. These application areas include multi-agent systems, social networks, service environments, and ad-hoc networks. Based on the assessment of conventional trust evaluation techniques in

the aforementioned application scenarios, typical trust evaluation methods are no longer acceptable when prior information is inadequate. This was determined by looking at the scenarios. Conveying trust through a linear combination of elements such as experience, knowledge, recommendations, and so on can be challenging when one lacks theoretical or practical guidance. As a direct consequence, the reliability of trust assessments may be called into question.

A. The Benefits of Machine Learning in the Process of Trust Assessment

The preceding explanation of conventional techniques for trust assessment makes it abundantly clear that incorporating machine learning into the trust evaluation process offers numerous benefits that are hard to dispute. To begin, a machine-learning-based trust assessment can overcome the

"cold start" and "zero knowledge" challenges associated with previous methodologies. Traditional techniques for trust assessment use both direct and indirect information from prior interactions and recommendations to compute trust levels. However, when the trustee is inexperienced, this information is not readily accessible, rendering typical processes ineffective. In this scenario, trust assessment based on machine learning may develop a trust model by adding additional trust-related feature data. This model can then be used. In the meantime, many traditional approaches to measuring trust rely on a linear combination of direct and indirect trust values to represent trust. The weights used for the combination, however, might be challenging to determine in many real-world situations. The precision of trust assessments may be affected by this technique, and it is believed that their accuracy can be improved using machine learning.

Second, using machine learning to process large amounts of data to establish trustworthiness may yield credible discoveries. Big data increases the volume of readily accessible data for trust assessment, thereby improving the accuracy of the evaluation [15]. Due to the massive amount of data and complex data structures, traditional trust evaluation methods become cumbersome and difficult to use in large-scale networking scenarios, such as social networks. As a result, traditional trust evaluation methods often yield inaccurate results. On the other hand, the use of machine learning as a basic approach to the processing of large amounts of data comes with its own set of benefits. It explains that, as a consequence, when dealing with vast amounts of data, machine learning is manifestly more suitable for trust assessment than the methodologies that preceded it.

Third, when evaluating reliability from an artificial intelligence perspective, machine learning can be beneficial. Machine learning, which is the kind of artificial intelligence that sees the most widespread use, investigates how computers can be programmed to behave in ways analogous to those of humans [20]. It does so by fashioning a model from preexisting data for further computation (or experience). This approach is consistent with how humans think. Human beings' subjective actions determine trust. As a result, machine learning may be used to perform trust assessments.

Fourth, the technique of assigning trust ratings based on machine learning is straightforward to understand. It is common knowledge that the most basic steps in applying machine learning to the issue of trust assessment are: the process as a whole may be broken down into three stages: data preparation, model selection, and model determination. Specifically, the following should be done: In data preparation, useful features are extracted from raw data that may contain missing values, repeated values, noise, and high dimensions using data cleaning, data fusion, feature selection, and other approaches. Then, we must choose, from the wide variety of machine learning algorithms now available, the most effective and suitable learning approach to construct a trust assessment model. In conclusion, the model's performance is sensitive to parameter configuration, as the method often requires parameter specification. As a result, the parameters need to be adjusted after the technique

is selected, and the ones that yield the best results should be chosen to create the final model. The process of human decision-making is modelled after machine learning-based trust assessment, meaning choices are made based on past experiences. This method is easy both to execute and to understand.

In other contexts, machine learning may be used to assess levels of trust.

In this part, we investigate research on trust assessment using machine learning across a variety of settings, including ubiquitous computing, grid computing, and peer-to-peer networking.

II. MACHINE LEARNING FOR DIRECT TRUST EVALUATIONS

The models that are based on either/or choices. In a ubiquitous setting, [22] offered a model for dynamic trust assessments. The trust model incorporates several variables, including prior probability, trust level, historical contact history, temporal impact, and peer endorsement. An algorithm from NBC was picked for the trust determination, and then it was applied twice. When making the initial decision to use NBC, only past information about the service provider was considered. When it is not possible to reach a decision, the facts from the suggestions are used to conclude. The subjectivity of this technique is supported by substantial evidence. Although the simulation tests demonstrated that it was capable of making dynamic judgments, they did not prove that it was successful. This model may perform dynamic trust evaluation if it is aware of the context. Data privacy and protection against potential threats, however, were not among the considerations. In addition, the computational cost was not accounted for [24].

In their research, [16] proposed using a random forest-based linear discriminant analysis model to assess the credibility of individuals who took part in crowdsourcing. The plan is divided into the following five stages. Before constructing a multidimensional reputation index system, data must be gathered and preprocessed. During the second step, the data are narrowed down, and during the third step, they are standardised. In the fourth step, you will choose a subset of characteristics and model them using machine learning. At the fifth step, the model's reliability is examined for accuracy. Several experiments were conducted using data from the zbj.com platform to evaluate its reputation. These experiments used a variety of dimensionality reduction strategies and machine learning techniques in combination. The research culminates in an improvement of 0.928 percentage points in accuracy when linear discriminant analysis is combined with random forests. The four data indicators that go into determining one's reputation are their initial reputation dimension, their penalty reputation dimension, their assessment data indicator, and their transaction data indicator. There is not a single one that is not open to personal interpretation. The strategy does not take into account the existing circumstances. Both the offensive and defensive measures used to protect privacy were neglected. The concept of computing

overhead is not mentioned anywhere in this paper.

III. TRUST EVALUATION

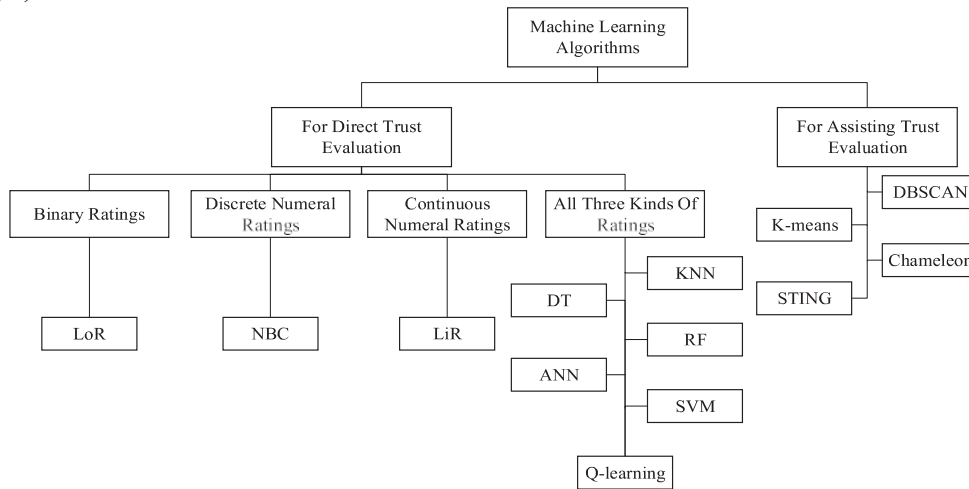
The Characteristics of a Trustworthy Person: Fundamentally, trust is a belief or judgment, which is a challenging concept to define across *disciplines*. It is an entity's subjective expectation of future behaviour from other entities. Various academics define the term "trust" differently. Although different domains have distinct definitions of trust, the aspects of trust that are constant are subjectivity, dynamism, context-awareness, imperfect transitivity, temporal decay, asymmetry, and measurability.

A. Benefits of Machine Learning for Trust Evaluation

Using machine learning to measure trust has numerous clear advantages, as we've shown in our review of

traditional trust evaluation methodologies thus far. Preliminary findings indicate that applying machine learning-based trust assessments can overcome the "cold start" and "zero knowledge" challenges associated with traditional trust evaluations.

Traditional trust evaluation strategies use data from previous direct and indirect interactions to calculate trust ratings. Due to a lack of experience, standard tactics are ineffective when used by a new trustee. When utilising machine learning to evaluate trust, you can build a trust model by adding more trust-related feature data. As a result, many traditional trust evaluation processes use a linear blend of direct and indirect trust values, with weights that are difficult to define. This method affects the accuracy of the trust assessment, which could be improved with machine learning [18].



[Fig.1: Machine Learning Methods are Classified According to Their Roles in Trust Evaluation and Evaluation Granularity]

Second, when it comes to judging trust, large-scale data processing employing machine learning may yield reliable results. Large-scale data sets enable more precise trust assessments. Large-scale networking scenarios, such as social networks, require the use of complex data structures and thorough trust evaluation techniques, which can lead to erroneous conclusions. Machine learning, on the other hand, provides substantial advantages when working with massive volumes of data. As a result, machine learning surpasses traditional trust evaluation approaches when dealing with large amounts of data.

Regarding the third issue, in machine learning and artificial intelligence, it becomes much easier to assess trust. Machine learning, the most common form of artificial intelligence, examines how computers can imitate human behaviour. It generates a model based on previously obtained data for future computations (or experiences). This approach is comparable to the way most people think. Humans rely on their own views to assess trustworthiness. As a result, machine learning could be used to determine whether or not someone is trustworthy. To put it another way, machine learning provides a simple, effective way to measure trust. Machine learning can undeniably help with the problem of evaluating trustworthiness. The process includes preprocessing data, selecting models, and choosing the final models. Details are as follows: Preprocessing recovers usable features from missing values, repetitive values, noise, and enormous dimensions by employing

techniques such as data cleaning and data fusion [19]. This is the first step in the process of converting raw data into usable qualities. The next step is to choose the best machine learning method for building a model to judge trustworthiness among the many available options. The model's performance may vary widely depending on how the algorithm's parameters are adjusted, as there are many variables to consider. This means that after selecting a method, the parameters must be fine-tuned before selecting the best-performing ones for the final model. Trust is quantified in the same way that human decision-making is modelled using machine learning. This is a straightforward and easy-to-understand method.

IV. RELATED WORK

[1] Machine learning (ML) services are being employed in a variety of mission-critical human-facing domains, so it is essential to maintain the integrity and trustworthiness of ML models. In this paper, we examine a model in which cloud service providers receive massive amounts of data from devices with limited resources to build machine learning-based prediction models. These models are then sent back to the devices with limited resources to be executed locally, using the devices' limited resources and intermittent Internet connections. Our proposed solution includes an intelligent polynomial-time heuristic that maximises the

trustworthiness of machine learning models. This is accomplished by selecting and switching between a subset of machine learning models from a larger superset. This is done to maximise trustworthiness while staying within the given reconfiguration budget/rate and reducing cloud communication overhead. To evaluate how well our proposed heuristic works, we will use two case studies. In the first step of this process, we analyse Industrial Internet of Things (IIoT) services. To estimate the remaining serviceable life of an engine, we use a proxy dataset derived from a simulation of turbofan engine degradation. In this specific instance, the data we have acquired show that the trust levels of the chosen models are 0.49% to 3.17% lower than those produced using integer linear programming (ILP). Second, we consider innovative city services and use a simulated dataset for experimental transportation to forecast the number of automobiles in this scenario. The chosen model has a trust level that is between 0.7 and 2.53 percentage points lower than the ILP results. In addition, we demonstrate that our proposed heuristic produces an ideal competitive ratio when used as a polynomial-time approximation method.

Together, Upul Jaya Singhe and his associates [2], the Internet of Things has made it much simpler to get access to a massive quantity of private data about the items that are participating in each ecosystem. This raises a variety of concerns, ranging from difficulties with data management to the potential for bias in data analytics over sensitive information such as locations, interests, and behaviours. These threats may be grouped into several categories. In response to these concerns, the idea of trust has been proposed as an essential component that may help both people and services overcome perceptions of risk and uncertainty before reaching any conclusions. This is done before any evaluations are made. Establishing confidence in a cyber world, on the other hand, may be a challenging process due to the numerous significant factors arising from cyber-physical systems. As a consequence, it is of utmost importance to have an intelligent trust computation model that provides accurate, understandable trust values to potential actors. As a direct consequence, the authors of this paper offer a paradigm for quantifying trust. After that, a numerical representation of each person's trustworthiness is constructed using this methodology. In addition, a novel approach based on machine learning principles has been developed to categorise the extracted trust characteristics and combine them into a final trust value for judgment. In conclusion, a simulation is used to evaluate the effectiveness of our methodology. According to the findings, our strategy outperforms other data-aggregation methods.

Subhash Sagar et al. [3], The Internet of Things (IoT) refers to a network that is now expanding to include billions of networked physical objects. These objects include a wide variety of sensors, smartphones, and embedded devices. When deployed in the real world, these physical gadgets, also known as smart objects, gather crucial information from their environments. The idea of the Internet of Things (IoT) has recently been extended to include social networking features, giving rise to the exciting new paradigm of the "Social Internet of Things" (SIoT). In the SIoT, devices act as independent agents, capable of intelligently sharing

information and locating new services through social interactions with their owners. The development of trustworthy connections between physical objects and the mitigation of risks associated with decision-making both need a foundation of trust. To develop a computational model of trust for extracting individual trust qualities in an SIoT setting, this work aims to do so. In addition, a machine-learning-based method is used to compile all trust attributes into a single entity, enabling the calculation of an aggregate trust score. According to the simulations, the proposed trust-based paradigm successfully separates trustworthy nodes from untrustworthy nodes within the network.

Wei Ma et al. [4] Malicious or damaged Internet of Things (IoT) devices pose substantial threats to the Internet of Things ecosystem due to its rapid expansion. To overcome this problem, trust has been recognised as an essential component of an effective security strategy for detecting abnormal devices in IoT networks. Nevertheless, evaluating trust in IoT devices is challenging because trust is a degree of confidence in a variety of trust traits, each of which is difficult to define individually. This makes trust difficult to measure. As a result of this study, a machine-learning-based trust assessment technique has been proposed. A deep learning technique is used to integrate trust components of network QoS (Quality of Service) to construct a behavioural model for a specific IoT device. This approach also fully accounts for the time-dependent characteristics of network behaviour. Trust may also be evaluated as continuous numerical values if the evaluation is used to determine the degree of similarity between actual network activities and the behaviours the behavioural model predicts. Trust values are applied both to determine whether a device can be trusted and to inform decision-making. In conclusion, tests are conducted to demonstrate that the recommended technique is successful, and the results of these experiments are given.

Vijender Busi Reddy et al. [5] over the internet, every item connected to the Internet of Things (IoT) is reachable, tractable, and accessible. To be useful, Internet of Things (IoT) devices need to work together and exchange information. Due to the openness, anonymity, and dynamism inherent to IoT networks, a malicious device can gain access to the network and cause disruption. Trust models have been proposed to detect malicious objects and enhance network reliability. The use of recommendations in trust computation serves as the basis for trust models. As a direct consequence, trust models are vulnerable to attacks based on collaboration and unfavourable publicity. In this study, we propose a similarity model as a preventive measure against badmouthing and collusion attacks. We also show that the recommended technique effectively reduces the influence of hostile recommendations on trust computation.

According to Rzan Tarig Frahat et al. [6], "IoT trust management" is a security solution that establishes trust between IoT entities before initiating interactions with other anonymous devices. This is done to prevent potential security breaches. In addition to the fog node technique,

new research published in the academic literature often uses a Blockchain-based trust management model for IoT. This is done to circumvent the limitations imposed by the Internet of Things' resources. In fact, Blockchain has solved many of the issues present in centralised systems. Despite this, it is still not the method of choice for handling the enormous amounts of data generated by the Internet of Things, as it has constraints such as latency, network overhead, and scalability issues. As a result, we identify critical features to consider when constructing scalable models. Additionally, we present a fully distributed trust management model for IoT that scales to large systems while simultaneously addressing the limitations imposed by Blockchain. Our model was constructed using an innovative method called Holocaine. This method addresses many security concerns, including detecting inappropriate actions, maintaining data integrity, and ensuring availability.

In the work of Mohammed Bahutair and colleagues [7] on crowd-sourced Internet of Things services, they introduce the concept of adaptive trust. Adaptive trust is a usage-based measure of a service's trustworthiness, determined by how users use it. The innovative four-stage paradigm is used to conduct the trust analysis for the dynamic service. The evaluation is based on how the service is used. In the first step, an algorithm attempts to predict multiple trust factors that determine the overall trustworthiness of an Internet of Things service. In the second step, the trust factors are used to construct a service-to-factor model. This model forecasts a service's trustworthiness for each trust component. At the third step, a use-to-factor model is developed. This model establishes the relative significance of each element within a specific usage scenario. In the last step, the two models are combined to provide a trust value appropriate for a given use case. To validate the proposed approach, a series of experiments using actual data were conducted.

Ayesha Altaf et al [8] The Internet of Things (IoT) is a technology that converts the real world into a digital network. The Internet of Things poses a challenging new data security dilemma. As a result, trust is an essential component of IoT device security. The Trust Management System (TMS) is designed to reduce the likelihood that communicative parties will make mistakes in their interactions. One approach to building trust may be to have users directly contact servers, depending on their experiences across a range of settings. This body of work aims to provide a context-based trust management system that relies on users' first-hand experiences while connected to servers across a range of settings. The Naive Bayesian classification method is used in this technique. The direct user experiences determined by context are filtered and classified, then used in a trust formation process to develop and update trust over time. The proposed protocol was validated using datasets from online services, and the results indicate that establishing trust based on contextual knowledge is a promising strategy.

Syeda Mariam Muzammal et al. [9] Attackers can quickly penetrate data channels due to the massive quantity of data collection and exchange that occurs between devices connected to the Internet of Things (IoT), as well as the minimal IoT security that is currently available to secure data transmission. In Internet of Things networks, the IPv6

Routing Protocol has become the standard routing protocol for Low Power and Lossy Networks (RPL). In IoT applications, RPL offers very little security against numerous risks, both unique to RPL and inherited from WSN. In addition, the memory, processing, and power of the currently available Internet and routing security solutions are severely limited, making it impossible for Internet of Things devices to operate as intended. Approaches based on machine learning, intrusion detection systems, and trust have all been proposed as potential mitigation strategies for the security of Internet of Things networks and routing. In current trust-based techniques, node mobility is either not addressed at all or addressed inadequately for mobile sink nodes. This is particularly true for security against RPL attacks. This article presents SMTrust, a conceptual architecture for ensuring the safety of routing protocols in the Internet of Things, grounded in mobility-based trust metrics. The strategy presented aims to protect against widespread RPL attacks, such as Black Hole, Grey Hole, Rank, and Version Number attacks. We anticipate that SM Trust will give superior network performance when compared to current trust models such as DCTM-RPL and SecTrust-RPL. This improvement will include greater attack detection accuracy, greater mobility, and increased scalability. Our approach is distinctive compared to other models because it accounts for the mobility of both sensor nodes and sink nodes. This aspect was not taken into account by different models. Because of this feature, it is suitable for deployment in a mobile Internet of Things environment. The proposed architecture of SM Trust, as a secure routing protocol, ensures privacy, integrity, and availability among sensor nodes during routing in IoT networks when implemented in RPL. This is accomplished using a hashing algorithm.

Besfort Shala et al. [10] For the Internet of Things (IoT) ecosystem to function correctly, it is essential that trust be established across its many autonomous entities. In this context, recent research argues that integrating blockchain technology with trust assessment tools is a viable option. [Citation needed] However, each of these Internet of Things technologies comes with its own unique set of limitations, which are explored further in this paper. First, this study examines several alternatives to blockchain-based trust mechanisms and discusses the pros and cons of applying them to decentralised Internet of Things communities. After that, an optimal trust model is proposed using a trust-based weighting mechanism with multiple layers of adaptation. Several other trust-metric parameters and the mathematical models that accompany them for assessing trust are also presented. In addition, by using control loops and smart contracts, this book proposes a fresh approach to the incentive mechanisms used in the IoT marketplace. As a direct consequence, people feel inspired to continue developing their positive behaviours. In conclusion, the suggested trust model is trustworthy. The outcomes of experiments conducted across a range of situations demonstrate that the proposed strategy is more resistant to a variety of attacks than the current approaches.

Ahmad Khalil et al., [11] In the newly developing

technological age known as "the Internet of Things," people, machines, and things all connect and the world around them through the internet (IoT). In this context, trust is essential to the growth of Internet of Things services and is a significant factor in the initiative's success. IoT services and apps may, in some cases, use data related to their users' privacy. As a result, people need to trust the organisations to which they are transferring their personal information. In this study, we present a methodology that utilises a Fuzzy Logic model to assess the security trust level of IoT nodes based on several input characteristics, including Device Physical Security, Device Security Level, and Device Ownership Trust. This methodology was developed for this study. The proposed Fuzzy Logic model has an output that calculates a trust level for each node in the network. To collect information that may be crucial and that concerns privacy protection, the best node (or nodes) in terms of trust level are selected based on the user-set threshold. Users of Internet of Things services can now choose trustworthy nodes (with a trust level above the threshold) to collect their data.

VANET (Vehicular Ad-hoc Network) is a vital transportation technology developed by Farhan Ahmad and his colleagues [21]. It enables vehicles to share sensitive information (such as warnings about steep curves and the presence of black ice) in real time with one another and with surrounding infrastructure, helping prevent accidents and making the driving experience more pleasant. To achieve these goals, VANET must operate in a safe environment where information is genuine, trustworthy, and shared across the network's many components. On the other hand, a VANET is susceptible to a wide range of attacks that may lead to the dissemination of tainted or misleading information throughout the many nodes that make up the network. Introducing trust across vehicle nodes is one technique for building a safe, trustworthy network. Multiple Trust Models (TMs) for VANETs are currently being developed to achieve this goal. These TMs may be broken down into the following three categories: entity-oriented Trust Models (ETM), data-oriented Trust Models (DTM), and hybrid Trust Models (HTM). The trustworthiness of the information (data), the vehicle (entity), or both may be determined in several different ways by these TMs. Within the scope of this paper, a comparison of the three TMs is presented [23]. In addition, we evaluate these TMs based on several other trust, security, and quality-of-service factors. According to the simulation results, each of these TMs has deficiencies in end-to-end latency, event detection probability, and false-positive rate. This work may serve as a template for researchers to follow in designing future VANET TMs that are not only effective but also efficient.

Yasir Hussain et al., [13] Trust and reputation are fundamental concepts in any communication, whether it be human-to-human (H2H), human-machine interaction (HMI), or machine-to-machine (M2M) (M2M). Cloud computing and the Internet of Things (IoT) deliver new capabilities but also pose a plethora of security and privacy challenges that must be addressed. It is necessary to consider a range of security concerns as a fundamental component of the Internet of Things (IoT). These concerns include determining whether a user can be trusted and identifying

malicious users. In addition, fog computing, also known as edge computing, is redefining Cloud-based IoT by delivering Cloud services at the network edge. This may help address security, privacy, and trust issues. In this research, we provide a context-aware trust assessment model for the purpose of determining whether or not a user in a fog-based Internet of Things system can be trusted (FIoT). The recommended approach uses a context-aware, multi-source trust-and-reputation-based assessment system to evaluate a user's trustworthiness accurately. In addition, we use a context-aware feedback and feedback crawler system that supports objective, efficient, and dependable trust assessment. We also provide a monitor mode for harmful or untrustworthy users, which helps monitor a user's behaviour and determine whether the person can be trusted. The proposed method employs several configurable parameters that can be fine-tuned to meet the system's needs. The simulations and results show that our process for determining a user's trustworthiness is both practical and reliable.

V. CONCLUSIONS

This article provides an in-depth discussion of the various machine learning-based trust evaluation systems that are currently available on the market. To begin, we discussed the fundamental notions that underpin both machine learning and trust, as well as the benefits of using machine learning to assess trust. During this interim period, [17] we investigated the benefits and drawbacks of more conventional approaches to trust rankings using machine learning methodologies. To find out how to evaluate the effectiveness of a trust assessment technique that is based on machine learning, we first investigated the criteria that should be satisfied by an effective method of trust evaluation. Because of this, we were able to determine the requirements for establishing the quality of a trust assessment approach that was based on machine learning. We have categorised the current approaches to assessing reliability into a wide variety of subcategories based on how they are intended to be used, the role machine learning algorithms play in determining reliability, and the level of specificity of the evaluation. We took a detailed look at each methodology and weighed its benefits and drawbacks against the assessment criteria we were given. The investigation's findings indicate that the location under consideration is still in the early phases of development. The most significant issues still requiring resolution have been compiled into a list for reference. Last but not least, to encourage individuals to contribute further resources and undertake additional study, we offered potential avenues for future exploration. This article provides an in-depth discussion of the various machine learning-based trust evaluation systems that are currently available on the market. To begin, we discussed the fundamental notions that underpin both machine learning and trust, as well as the benefits of using machine learning to assess trust. During this interim period, we investigated the benefits and drawbacks of more conventional approaches to trust ranking using machine

learning methodologies. To find out how to evaluate the effectiveness of a trust assessment technique that is based on machine learning, we first investigated the criteria that should be satisfied by an effective method of trust evaluation. Because of this, we were able to determine the requirements for establishing the quality of a trust assessment approach that was based on machine learning. We have categorised the current approaches to assessing reliability into a wide variety of subcategories based on how they are intended to be used, the role machine learning algorithms play in determining reliability, and the level of specificity of the evaluation. We took a detailed look at each methodology and weighed its benefits and drawbacks against the assessment criteria we were given. The investigation's findings indicate that the location under consideration is still in the early stages of development.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Basheer Qolomany; Ihab Mohammed; Ala Al-Fuqaha; Mohsen Guizani; Junaid Qadir Trust-Based Cloud Machine Learning Model Selection for Industrial IoT and Smart City Services IEEE Internet of Things Journal Year: 2021 | Volume: 8, Issue: 4 | Journal Article | Publisher: IEEE DOI: <https://doi.org/10.1109/JIOT.2020.3022323>
2. Upul Jayasinghe; Gyu Myoung Lee; Tai-Won Um; Qi Shi Machine Learning Based Trust Computational Model for IoT Services IEEE Transactions on Sustainable Computing Year: 2019 | Volume: 4, Issue: 1 | Journal Article | Publisher: IEEE DOI: <https://doi.org/10.1109/TSUSC.2018.2839623>
3. Subhash Sagar; Adnan Mahmood; Quan Z. Sheng; Wei Emma Zhang. Trust Computational Heuristic for Social Internet of Things: A Machine Learning-based Approach. ICC 2020 - 2020 IEEE International Conference on Communications (ICC) Year: 2020 | Conference Paper | Publisher: IEEE DOI: <https://doi.org/10.1109/ICC40277.2020.9148767>
4. Wei Ma; Xing Wang; Mingsheng Hu; Qinglei Zhou Machine Learning Empowered Trust Evaluation Method for IoT Devices IEEE Access Year: 2021 | Volume: 9 | Journal Article | Publisher: IEEE DOI: <https://doi.org/10.1109/ACCESS.2021.3076118>
5. Vijender Busi Reddy; Atul Negi; S Venkataraman; V Raghu Venkataraman A Similarity-based Trust Model to Mitigate Badmouthing Attacks in Internet of Things (IoT) 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) Year: 2019 | Conference Paper | Publisher: IEEE DOI: <https://doi.org/10.1109/WF-IoT.2019.8767170>
6. Rzan Tarig Frahat; Muhammed Mostafa Monowar; Seyed M Buhari Secure and Scalable Trust Management Model for IoT P2P Network 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS) Year: 2019 | Conference Paper | Publisher: IEEE DOI: <https://doi.org/10.1109/CAIS.2019.8769467>
7. Mohammed Bahutair; Athman Bougettaya; Azadeh Ghari Neiat Adaptive Trust: Usage-Based Trust in Crowdsourced IoT Services 2019 IEEE International Conference on Web Services (ICWS) Year: 2019 | Conference Paper | Publisher: IEEE DOI: <https://doi.org/10.1109/ICWS.2019.00038>
8. Ayesha Altaf; Haider Abbas; Faiza Iqbal Context-Based Trust Formation Using Direct User-Experience in the Internet of Things(IoT) 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom) Year: 2019 | Conference Paper | Publisher: IEEE DOI: <https://doi.org/10.1109/CloudCom.%202019.00072>
9. Syeda Mariam Muzammal; Raja Kumar Murugesan; Noor Zaman Jhanjhi; Low Tang Jung SMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoT Applications 2020 International Conference on Computational Intelligence (ICCI) Year: 2020 | Conference Paper | Publisher: IEEE DOI: <https://doi.org/10.1109/ICCI51257.2020.9247818>
10. Besfort Shala; Ulrich Trick; Armin Lehmann; Bogdan Ghita; Stavros Shiaeles Blockchain and Trust for Secure, End-User-Based and Decentralized IoT Service Provision IEEE Access Year: 2020 | Volume: 8 | Journal Article | Publisher: IEEE DOI: <https://doi.org/10.1109/ACCESS.2020.3005541>
11. Ahmad Khalil; Nader Mbarek; Olivier Togni Fuzzy Logic Based Security Trust Evaluation for IoT Environments 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA) Year: 2019 | Conference Paper | Publisher: IEEE DOI: <https://doi.org/10.1109/AICCSA47632.2019.9035294>
12. Farhan Ahmad; Asma Adnane; Fatih Kurugollu; Rasheed Hussain A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks 2019 Wireless Days (WD) Year: 2019 | Conference Paper | Publisher: IEEE DOI: <https://doi.org/10.1109/WD.2019.8734204>
13. Yasir Hussain; Huang Zhiqiu; Muhammad Azeem Akbar; Ahmed Alsanad; Abeer Abdul-Aziz Alsanad; Asif Nawaz; Izhar Ahmed Khan; Zaheer Ullah Khan Context-Aware Trust and Reputation Model for Fog-Based IoT IEEE Access Year: 2020 | Volume: 8 | Journal Article | Publisher: IEEE DOI: <https://doi.org/10.1109/ACCESS.2020.2972968>
14. L. Liu and H. Jia, "Trust Evaluation via Large-Scale Complex Service-Oriented Online Social Networks," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 11, pp. 1402-1412, Nov. 2015, DOI: <https://doi.org/10.1109/TSMC.2015.2406858>.
15. Wang, Jingwen, Xuyang Jing, Zheng Yan, Yulong Fu, Witold Pedrycz, and Laurence T. Yang. "A survey on trust evaluation based on machine learning." *ACM Computing Surveys (CSUR)* 53, no. 5 (2020): 1-36. DOI: <https://doi.org/10.1145/3408292>.
16. Huang, Yanrong, and Min Chen. "Improve reputation evaluation of crowdsourcing participants using multidimensional index and machine learning techniques." *IEEE Access* 7 (2019): 118055-118067. <https://ieeexplore.ieee.org/document/8787738>
17. Shushu Liu, Lifang Zhang, and Zheng Yan. 2018. Predict pairwise trust based on machine learning in online social networks: A survey. *IEEE Access* 6 (2018), 51297-51318. DOI: <https://doi.org/10.1109/ACCESS.2018.2869699>.
18. Jorge López and Stephane Maag. 2015. Towards a generic trust management framework using a machine-learning-based trust model. In *Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA - Volume 01 (TRUSTCOM'15)*. IEEE Computer Society, Washington, DC, 1343-1348. DOI: <https://doi.org/10.1109/Trustcom.2015.528>.
19. Chengying Mao and Rongru Lin. 2016. QoS trust rate prediction for web services using PSO-based neural network. In the 2016 International Conference on Advanced Cloud and Big Data (CBD). 68-74. DOI: <https://doi.org/10.1109/CBD.2016.022>.
20. Chengying Mao, Rongru Lin, Changfu Xu, and Qiang He. 2017. Towards a trust prediction framework for cloud services based on PSO-driven neural network. *IEEE Access* 5 (2017), 2187-2199. DOI: <https://doi.org/10.1109/ACCESS.2017.2654378>.
21. Muhammad Mohsin Mehdi, Imran Raza, and Syed Asad Hussain. 2017. A game theory-based trust model for vehicular ad hoc networks (VANETs). *Computer Networks* 121, C (July 2017), 152-172. DOI: <https://doi.org/10.1016/j.comnet.2017.04.024>.
22. Kumar, Aditya, Karan Singh, and Satvik Vats. "Trust evaluation-based machine learning for WSNs." In *2023, the 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1430-1436. IEEE, 2023. <https://ieeexplore.ieee.org/document/10112390>
23. Bhatia, Abhay, Anil Kumar, Arpit Jain, Adesh Kumar, Chaman Verma, Zoltan Illes,

Ioan Aschilean, and Maria Simona Raboaca. "Networked control system with MANET communication and AODV routing." *Heliyon* 8, no. 11 (2022). DOI: <https://doi.org/10.1016/j.heliyon.2022.e11678>

24. Kumar, Anil, Abhay Bhatia, Arun Kashyap, and Manish Kumar. "LSTM network: a deep learning approach and applications." In *Advanced Applications of NLP and Deep Learning in Social Media Data*, pp. 130-150. IGI Global, 2023. DOI: <http://doi.org/10.4018/9781-6684-6909-5.ch007>.

AUTHOR'S PROFILE



Dr. Anil Kumar is presently associated with Roorkee Institute of Technology (RIT), Roorkee, Haridwar, Uttarakhand, as an Associate Professor in the Department of Computer Science and Engineering. He has 19+ years of academic experience and has worked with various reputable engineering institutions. He has completed his B. Tech in Information Technology from AKTU (formerly UPTU), M. Tech in Computer Science and Engineering and PhD specialising in Natural Language Processing. He is currently an active member of IEEE and has reviewed several journal articles. He has a distinguished record of research papers and book chapters with more than 20 publications in Scopus, IEEE and SCI journals. He has authored books titled "Essential Interpersonal Skills for Engineers", "Mastering Data Structures: A Practical Approach" and "Practical Approach to Machine Learning with TensorFlow". He also has six book chapters in his bucket, and his research areas include Natural Language Processing, Neural Networks, Machine Learning, and Image Processing.



Dr. Abhay Bhatia is an accomplished academician and researcher, serving as an Associate Professor in the Department of Computer Science and Engineering at Roorkee Institute of Technology, Uttarakhand. With over 13 years of teaching and research experience, he holds a B.Tech. and M.Tech. in Computer Science and a PhD in Wireless Sensor Networks. An active IEEE member, he has published over 34 papers, authored 11 book chapters, and filed seven patents. His authored books include Fundamentals of IoT and Practical Approach to Machine Learning with TensorFlow. His research interests include Artificial Intelligence, Machine Learning, and Wireless Sensor Networks.



Dr. Sunil Kumar, pursued a Bachelor of Technology in Computer Science & Engineering from B.I.E.T., Jhansi, affiliated to Bundelkhand University, Jhansi, Uttar Pradesh, and a Master of Technology in Computer Science & Engineering from Y.M.C.A. Institute of Engineering affiliated to Maharshi Dayanand University, Rohtak, Haryana, and Ph.D. in Computer Science & Engineering from I. K. Gujral Punjab Technical University, Kapurthala, Punjab. He has worked in many reputed institutes. He is currently a Professor in the Department of Information Technology at Ajay Kumar Garg Engineering College, Ghaziabad, Uttar Pradesh. He has published more than 45+ research papers in reputed international journals and conferences. He has reviewed many research papers in journals and conferences. He has guided various B.Tech. and M.Tech. Students. His research interests lie in Computer Networks, Wireless Networks, Cryptography & Network Security, and Machine Learning.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.